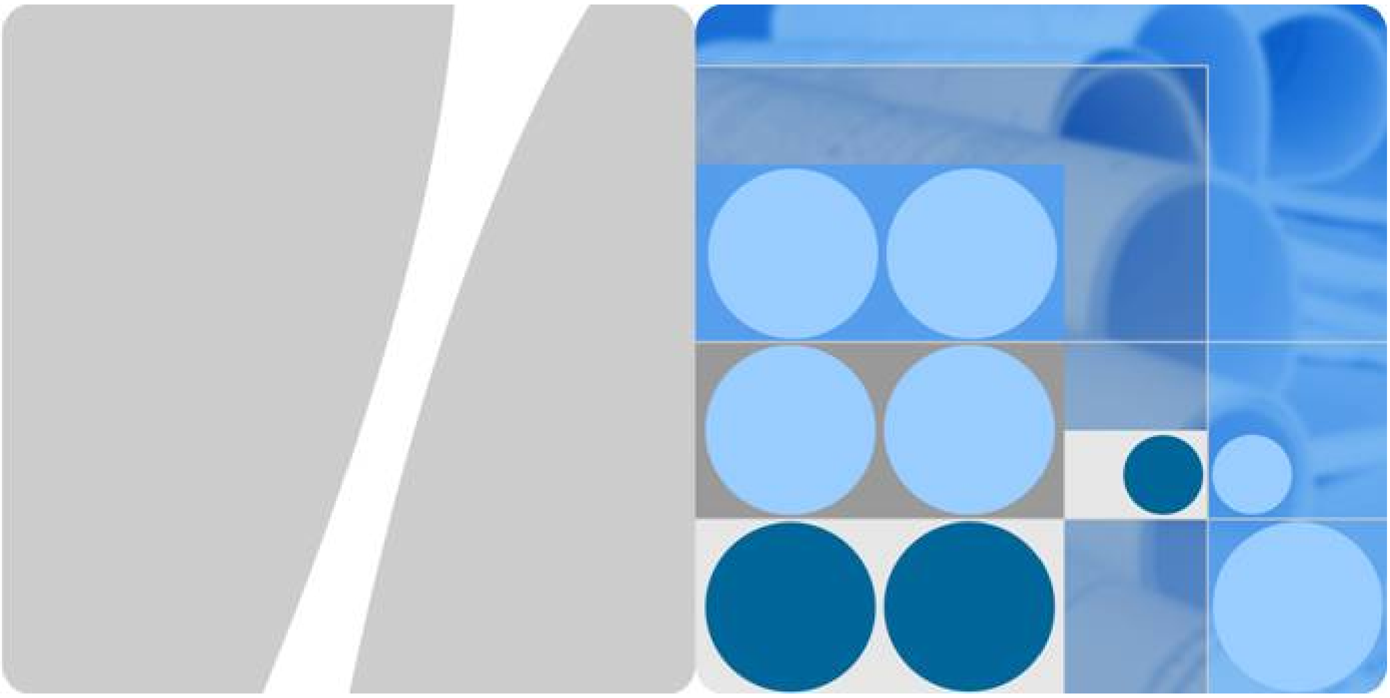


SmartAX MA5600T/MA5603T Multi-service Access Module

V800R011C00

Commissioning and Configuration Guide

Issue	04
Date	2012-09-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

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

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

This document is intended for:

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

Symbol Conventions

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

Symbol	Description
⚠ DANGER	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 that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
🔑 TIP	Indicates a tip that may help you solve a problem or save your time.

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

Command Conventions

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

GUI Conventions

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

Update History

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

Updates in Issue 04 (2012-09-20)

This is the forth release. Compared with issue 03 (2012-07-30) of V800R011C00, this issue has the following changes.

Type	Change
Modify	The chapter **14.9 Configuring ETH OAM**.

Updates in Issue 03 (2012-07-30)

This is the third release. Compared with issue 02 (2012-06-05) of V800R011C00, this issue has the following changes.

Type	Change
Modify	● **20 Example: Configuring VPLS**. ● **10.7 Configuring the R2 Service**. ● **Adding an SIP Interface**. ● **17.3.5 Example: Configuring the P2P ISDN BRA Service**. ● **17.3.6 Example: Configuring the P2P ISDN BRA Service (Based on the SIP Protocol)**. ● **17.3.7 Example: Configuring the P2MP ISDN BRA Service**. ● **17.3.8 Example: Configuring the P2MP ISDN BRA Service(Based on the SIP Protocol)** . ● **17.3.4 Example: Configuring the VoIP Service (H.248-based and SIP-based)**. ● **17.3.10 Example: Configuring the ISDN PRA Service (Based on the SIP Protocol)**. ● **18.3.6 Configuring TDM E1/T1 Private Line Service**. ● **4.8 (Optional) Configuring the VDSL2 Vectoring Function**.

Updates in Issue 02 (2012-06-05)

This is the second release. Compared with issue 01 (2012-04-30) of V800R011C00, this issue has the following changes.

Type	Change
New	● **8.2.8 (Optional) Configuring the Maximum Number of Programs That Can Be Watched by the Multicast User**. ● **8.2.9 (Optional) Configuring the Maximum Rate for Sending IGMP Packets**. ● **9.10 (Optional) Configuring the Maximum Number of Programs That Can Be Watched by the Multicast User**. ● **9.11 (Optional) Configuring the Maximum Rate for Sending IGMP Packets**.

Type	Change
Modify	● 8.2 Configuring the Multicast Service on a Single NE. ● 8.2.2 Configuring the Multicast VLAN and the Multicast Program. ● 8.2.3 Configuring a Multicast User. ● 9.3 Configuring the Multicast VLAN and the Multicast Program. ● 9.5 Configuring a Multicast User.

Updates in Issue 01 (2012-04-30)

This is the first release. Compared with issue 02 (2012-03-30) of V800R010C00, this issue has the following changes.

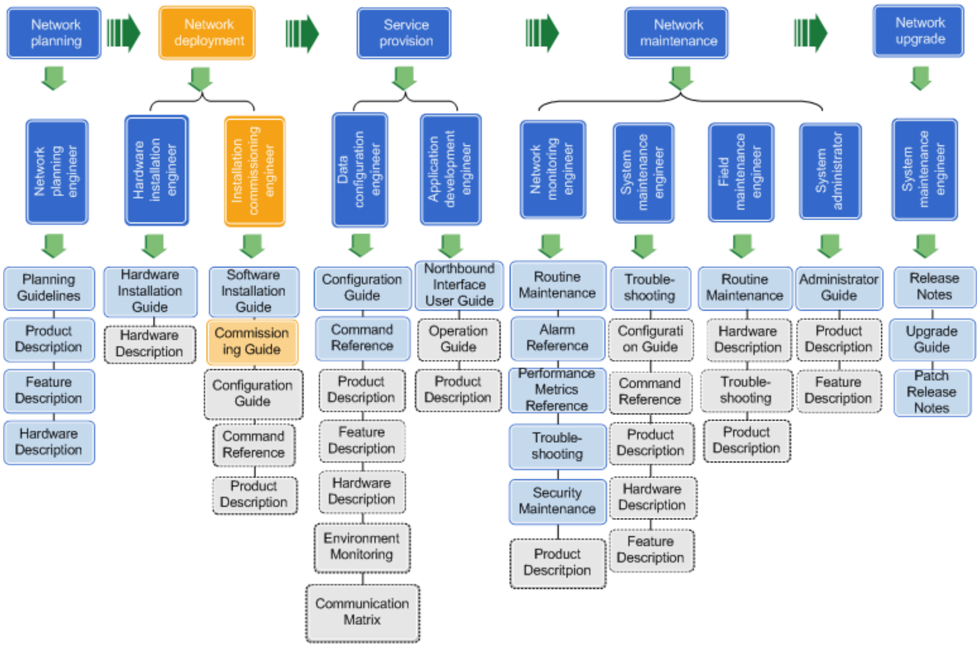
Type	Change
New	● 1.3.14 Enabling the ONT Automatic Discovery function. ● 2.6.1 Creating a VLAN. ● 2.6.2 Configuring the VLAN attribute. ● 2.6.3 Configuring the VLAN S+C forwarding policy. ● Configuring Queue-based Rate Limit. ● 4.8 (Optional) Configuring the VDSL2 Vectoring Function. ● 10.2.3 (Optional) Configuring the Centrex. ● 10.2.4 (Optional) Configuring Line Hunting. ● 10.2.5 (Optional) Configuring Digitmap for SIP Interfaces . ● 10.7 Configuring the R2 Service. ● 13 Configuring VPLS MP2MP Intercommunication. ● 20 Example: Configuring VPLS. ● 22 Appendix: Common Configuration Operations.
Modify	● Login Through the Local Serial Port. ● Login Through Telnet (Outband Management). ● Login Through Telnet (Inband Management). ● Login Through SSH (Outband Management). ● Login Through SSH (Inband Management). ● 1.3.6 Checking the Software State. ● 8.2.5 (Optional) Configuring Multicast Preview. ● 8.2.7 (Optional) Configuring the Multicast Logging Function. ● 9.7 (Optional) Configuring Multicast Preview. ● 9.9 (Optional) Configuring the Multicast Logging Function. ● 14.1 Configuring Ethernet Link Aggregation.

Contents

1 Commissioning

About This Chapter

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



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

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

1.3 Stand-Alone Commissioning
After the hardware installation, a stand-alone MA5600T/MA5603T should be commissioned to ensure that the stand-alone MA5600T/MA5603T works in the normal state. The following recommended commissioning tasks and sequences are for reference only. Different offices have

different conditions; therefore, it is recommended that customers, with the assistance of Huawei engineers, modify commissioning tasks according to actual requirements.

1.4 Interconnection Commissioning

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

1.5 Maintenance and Management Commissioning

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

1.6 Supplementary Information

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

1.1 Commissioning Introduction

The topic describes the commissioning definition and procedure.

1.1.1 Commissioning Definition

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

1.1.2 Commissioning Procedure

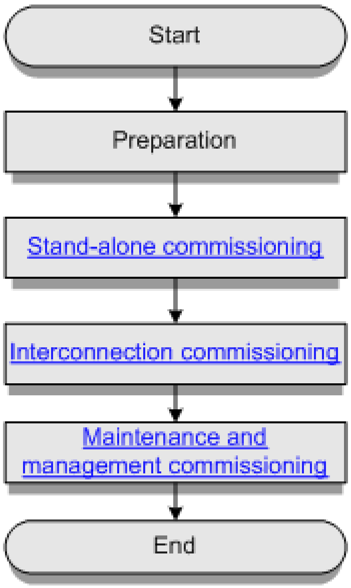
This topic describes the procedure for commissioning the device.

Flowchart

Perform the commissioning according to the flowchart.

Figure 1-1 shows the commissioning procedure.

Figure 1-1 Commissioning procedure


Start
Preparation
Stand-alone commissioning
Interconnection commissioning
Maintenance and management commissioning
End

Commissioning Item

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

Commissioning Preparations

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

Stand-Alone Commissioning

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

Interconnection Commissioning

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

Maintenance and Management Commissioning

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

1.2 Commissioning Preparations

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

1.2.1 Checking Hardware

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

Context

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

Table 1-1 Hardware checklist

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

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

1.2.2 Preparing Software

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

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

Table 1-2 Software checklist

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

1.2.3 Preparing Tools

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

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

Table 1-3 Tool checklist

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

1.2.4 Planning Data

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

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

Table 1-4 Data checklist

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

NOTE

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

1.3 Stand-Alone Commissioning

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

1.3.1 Checking the Settings of DIP Switches

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

Context

NOTE

Only the MA5600T supports this operation.

Checking the Settings of DIP Switches on the ESC Board

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

Prerequisites

The device must be powered off.

Description of DIP Switches

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

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

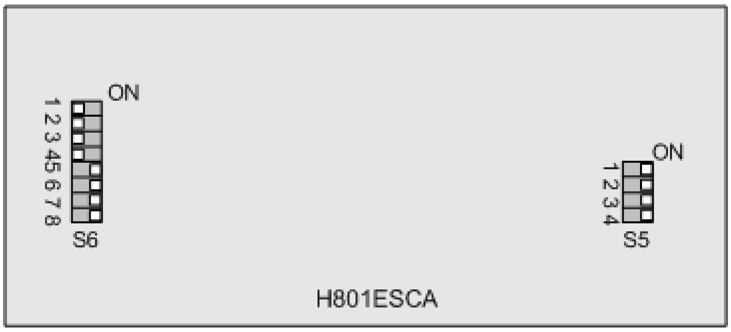


Table 1-5 describes the usage of DIP switches S5 and S6.

Table 1-5 Usage of the DIP switches

Electric Switch	Usage
S5-1	Used to set the external sensor type of JTA1-JTA4. For detailed information, see **Table 1-6**. ● ON: The external sensors are of the current type. ● OFF: The external sensors are of the voltage type.
S5-2	
S5-3	
S5-4	

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

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

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

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

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

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

S6-5	S6-4	S6-3	S6-2	S6-1	Address Value of Sub-nodes
0	0	0	0	0	00000 (0)

S6-5	S6-4	S6-3	S6-2	S6-1	Address Value of Sub-nodes
0	0	0	0	1	00001(1)
0	0	0	1	0	00010(2)
0	0	0	1	1	00011(3)
0	0	1	0	0	00100(4)
0	0	1	0	1	00101(5)
0	0	1	1	0	00110(6)
0	0	1	1	1	00111(7)
0	1	0	0	0	01000(8)
0	1	0	0	1	01001(9)
0	1	0	1	0	01010(10)
0	1	0	1	1	01011(11)
0	1	1	0	0	01100(12)
0	1	1	0	1	01101(13)
0	1	1	1	0	01110(14)
0	1	1	1	1	01111(15) (default)
1	0	0	0	0	10000(16)
1	0	0	0	1	10001(17)
1	0	0	1	0	10010(18)
1	0	0	1	1	10011(19)
1	0	1	0	0	10100(20)
1	0	1	0	1	10101(21)
1	0	1	1	0	10110(22)
1	0	1	1	1	10111(23)
1	1	0	0	0	11000(24)
1	1	0	0	1	11001(25)
1	1	0	1	0	11010(26)
1	1	0	1	1	11011(27)
1	1	1	0	0	11100(28)

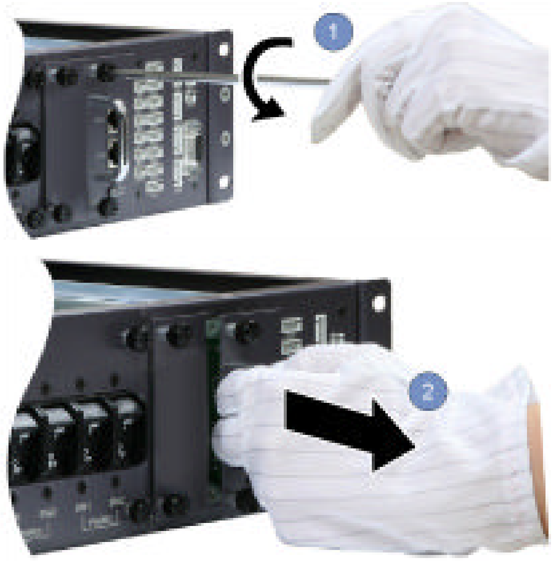
S6-5	S6-4	S6-3	S6-2	S6-1	Address Value of Sub-nodes
1	1	1	0	1	11101(29)
1	1	1	1	0	11110(30) is used by the ESC board, and the H801ESC board cannot be set to this value.
1	1	1	1	1	11111(31)

Procedure

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

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

Figure 1-3 Removing the ESC board

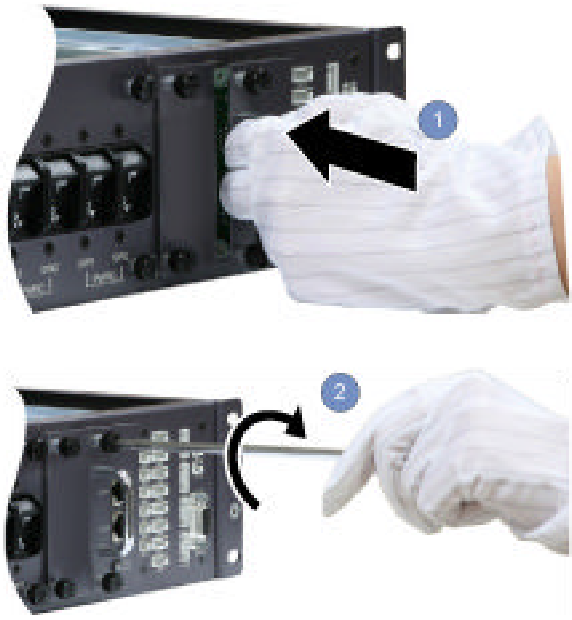


Step 3 Hold the ejector lever of the front panel and remove the ESC board from the PDU, as shown in (2) of **Figure 1-3**.

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

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

Figure 1-4 Inserting the ESC board



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

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

----End

Result

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

Checking the Settings of DIP Switches on the Fan Monitoring Board

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

Prerequisites

The device must be powered off.

Description of DIP Switches

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

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

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

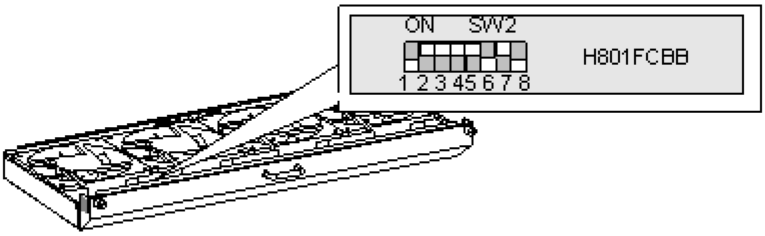


Figure 1-6 Layout of the DIP switches (in default settings) of the 19-inch fan tray

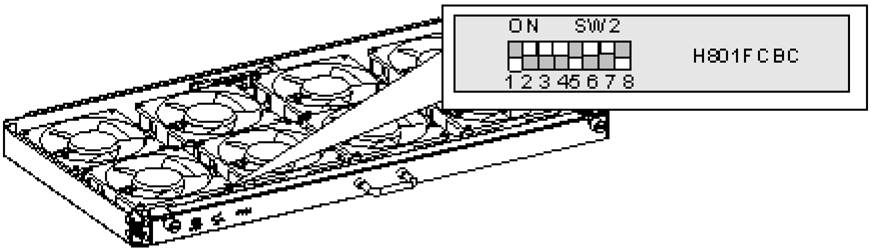


Table 1-8 lists the usage of the SW2.

Table 1-8 usage of the SW2

DIP Switch	Usage
SW2-1	Used to set the sub-node address. This value must correspond with the configured sub-node address of the fan in the system and cannot be identical to the address value of the ESC sub-node. Such restrictions ensure that the fan tray can communicate with the control board. For detailed information, see **Table 1-9**. ● ON: The mapping address bit is 0. ● OFF: The mapping address bit is 1.
SW2-2	
SW2-3	
SW2-4	Used to set the baud rate of the communication between the fan tray and the control board. ● ON: The baud rate is 19200 bit/s (default). ● OFF: The baud rate is 9600 bit/s.
SW2-5	Used to set the number of fans. This value must correspond with the system data configuration. For detailed information, see **Table 1-10**.
SW2-6	
SW2-7	Used to set the fan speed adjustment mode. This value must correspond with the system data configuration. For detailed information, see **Table 1-11**.
SW2-8	

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

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

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

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

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

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

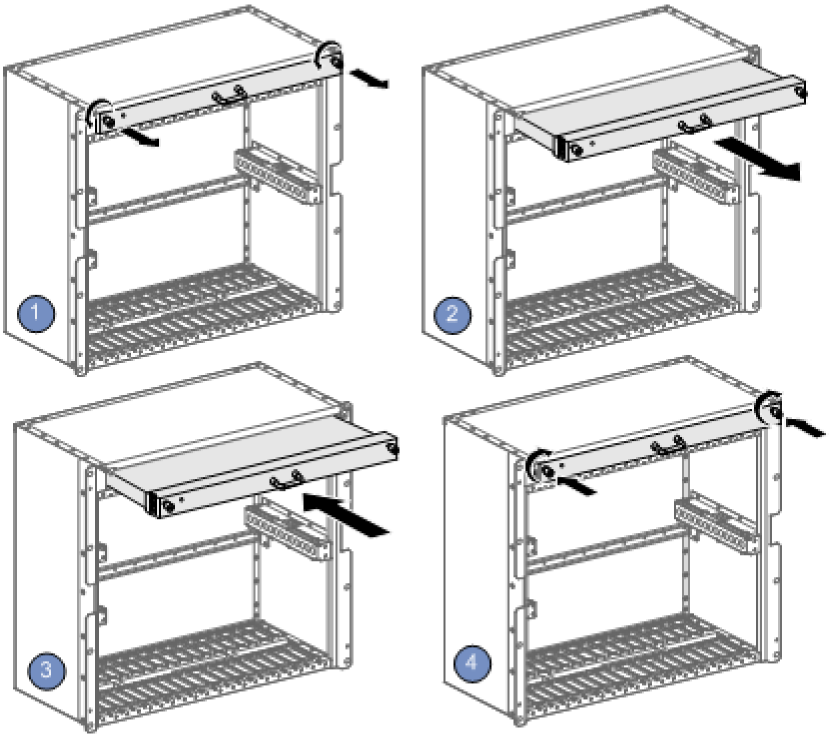
SW2-8	SW2-7	Speed Adjustment Mode	Speed Adjustment Policy	Remarks
ON	ON	Measure the temperature at the air intake vent (reserved)	Policy 1 ● If the temperature is lower than 25°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 25°C to 35°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 35°C, the fans rotate at full speed.	-

SW2-8	SW2-7	Speed Adjustment Mode	Speed Adjustment Policy	Remarks
ON	OFF	Measure the temperature at the air exhaust vent	Policy 2 ● If the temperature is lower than 55°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 55°C to 65°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 65°C, the fans rotate at the full speed.	-
OFF	ON	Measure the temperature at the air intake vent	Policy 3 ● If the temperature is lower than 30°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 30°C to 50°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 50°C, the fans rotate at full speed.	The ESTI and the 19-inch fan trays support only policy 3. Therefore, only this setting can be adopted.
OFF	OFF	Stop fan rotating and measure the temperature at the air intake vent	Policy 4 ● If the temperature is lower than 15°C, the fans stop rotating. ● If the temperature ranges from 15°C to 45°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 45°C to 65°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 65°C, the fans rotate at full speed.	-

Procedure

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

Figure 1-7 Removing/Inserting the fan tray



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

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

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

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

----End

Result

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

1.3.2 Powering On the Device

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

Prerequisites

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

Context

⚠ **CAUTION**

Inserting or removing boards is prohibited during startup.

Procedure

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

----End

Result

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

1.3.3 Commissioning the Power Supply System

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

Checking the Power Supply of the DC PDU

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

Prerequisites

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

Procedure

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

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

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

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

----End

Result

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

Checking the Power Supply of the Power Board

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

Prerequisites

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

Context

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

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

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

Procedure

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

Step 2 Turn on the switch again.

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

----End

Result

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

1.3.4 Configuring the Maintenance Terminal

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

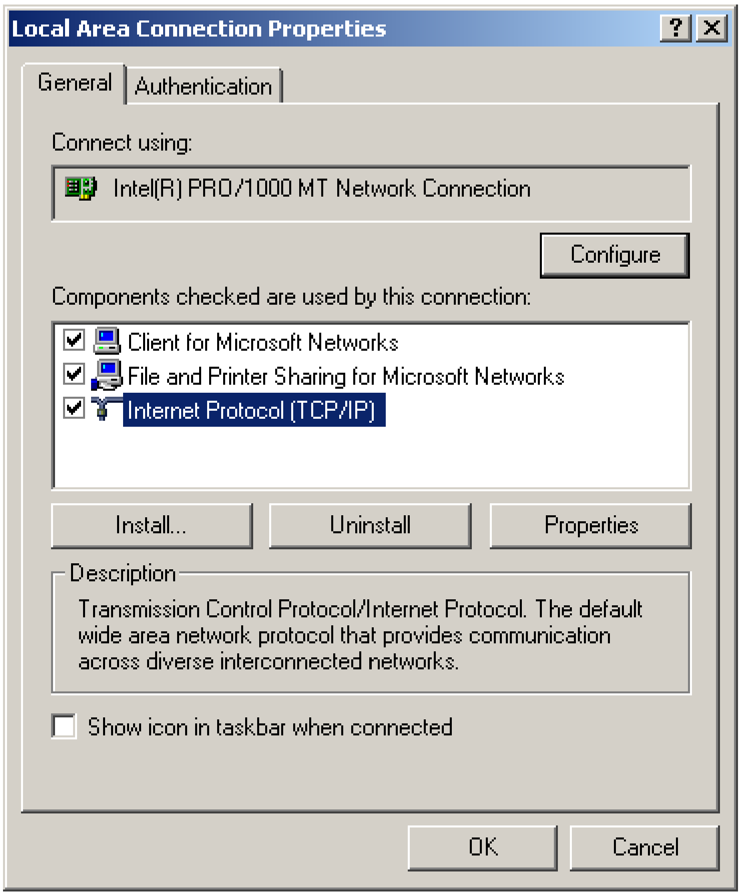
Context

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

Procedure

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

Figure 1-8 Configure the local area connection properties



Local Area Connection Properties

Connect using:
Intel(R) PRO/1000 MT Network Connection

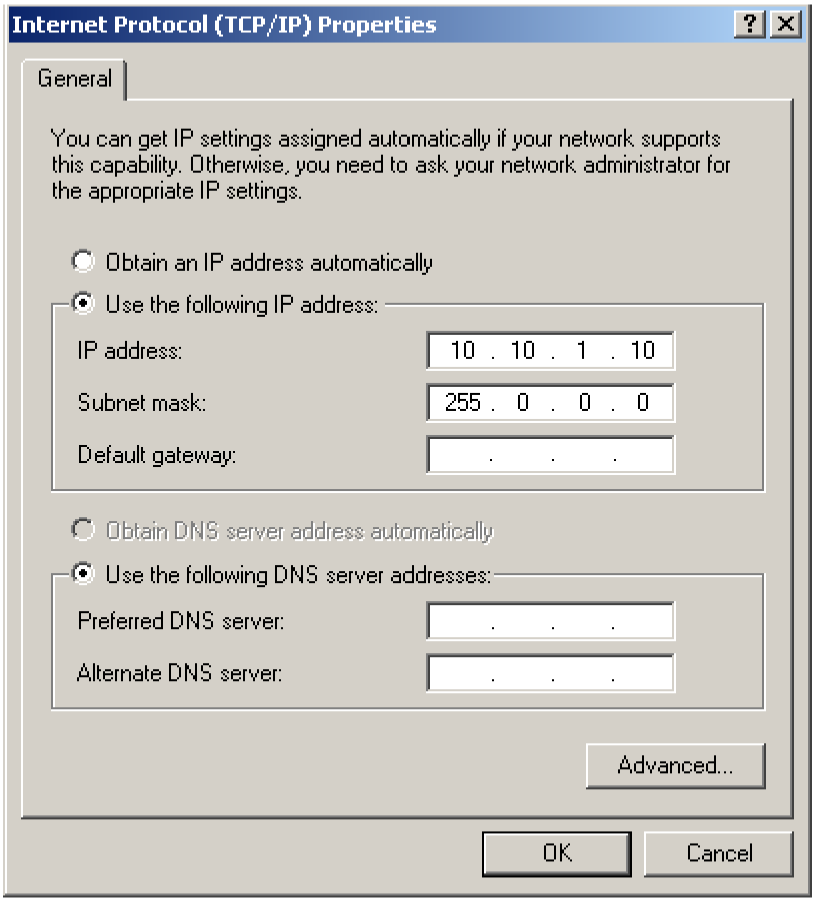
Components checked are used by this connection:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

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

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



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 1 . 10

Subnet mask: 255 . 0 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

NOTE

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

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

----End

Result

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

NOTE

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

1.3.5 Logging In to the System

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

Login Through the Local Serial Port

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

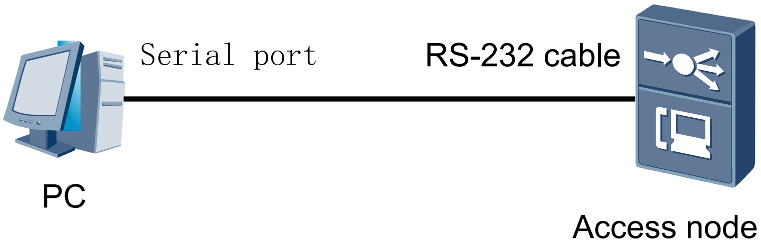
Prerequisites

- A maintenance terminal (generally a laptop configured with a HyperTerminal application) must be available.
- An RS-232 serial port cable (one end with an RJ-45 connector and the other end with a DB-9 or DB-25 female connector) must be available.

Networking

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

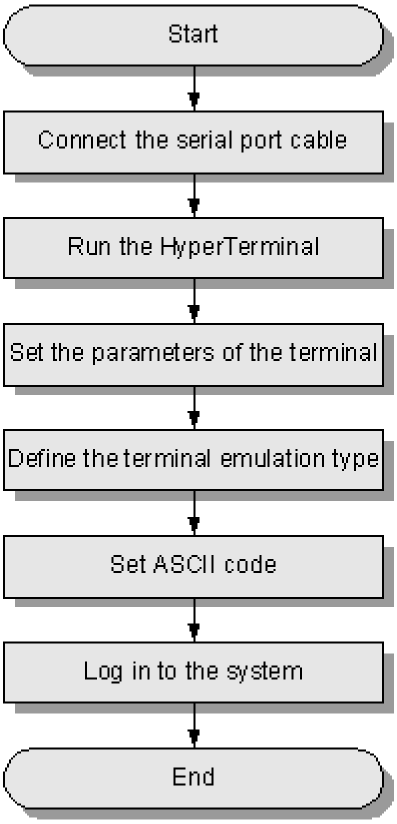
Figure 1-10 Logging in to the MA5600T/MA5603T through the local serial port



Flowchart

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

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


Start
Connect the serial port cable
Run the HyperTerminal
Set the parameters of the terminal
Define the terminal emulation type
Set ASCII code
Log in to the system
End

Procedure

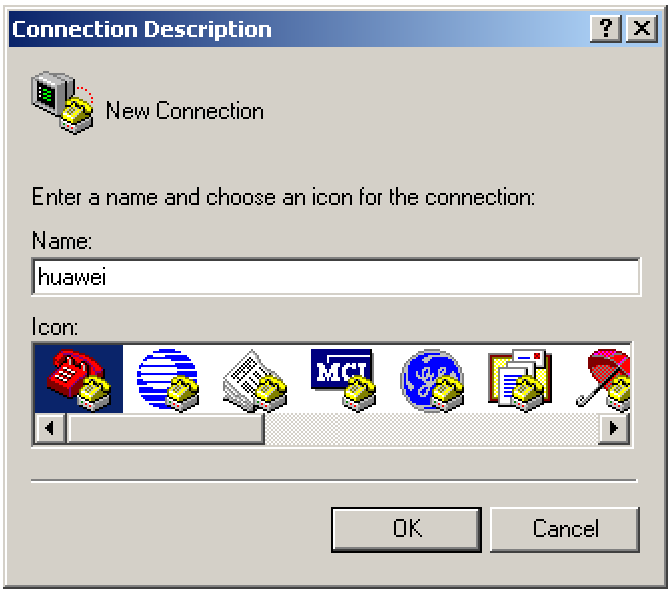
Step 1 Connect the serial port cable.

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

Step 2 Set the HyperTerminal communication parameters.

1. Set up a connection.

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



Connection Description

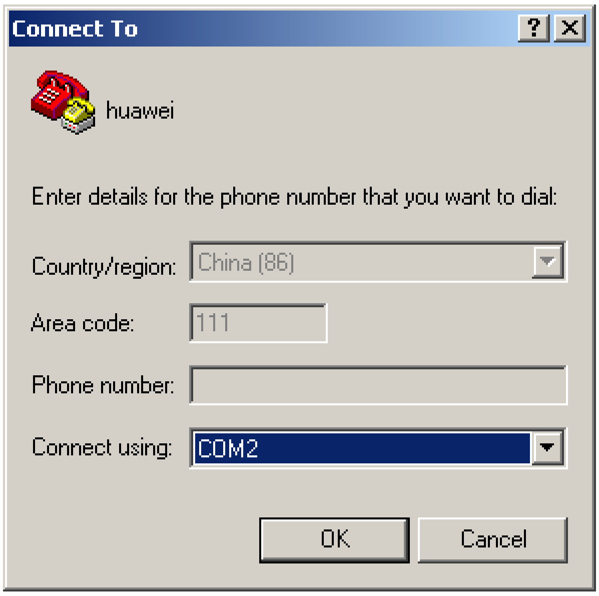
New Connection

Enter a name and choose an icon for the connection:

Name: huawei

2. Set the serial port.

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



Connect To

huawei

Enter details for the phone number that you want to dial:

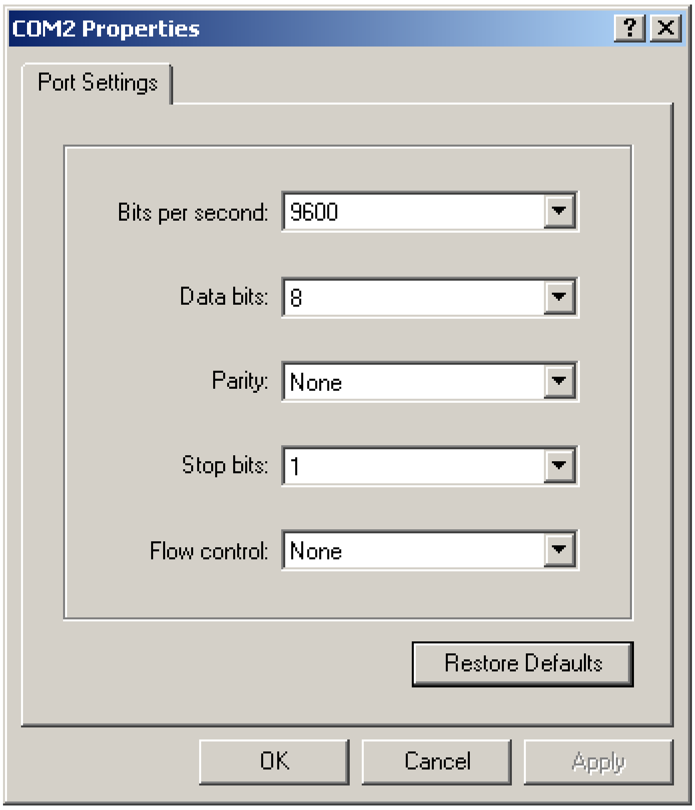
Country/region: China (86)

Area code: 111

Phone number:

Connect using: COM2

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



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

NOTE

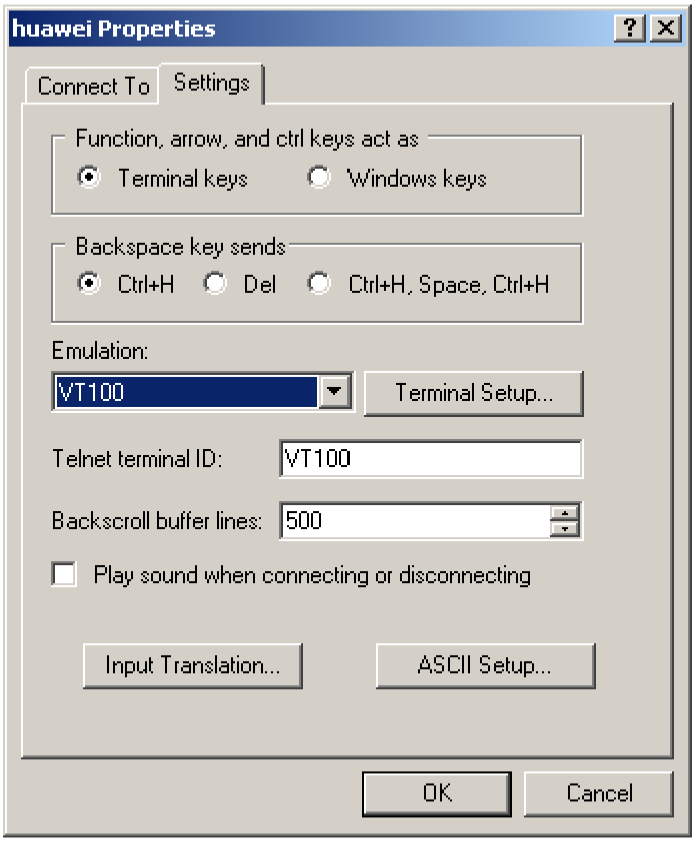
- The baud rate of the HyperTerminal must be the same as the baud rate of the serial port on the MA5600T/MA5603T. By default, the baud rate of the serial port is 9600 bit/s.
- If illegible characters are displayed on the HyperTerminal interface after you log in to the system, it is generally because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

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

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

1. Set the emulation type of the HyperTerminal.

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



huawei Properties

Connect To | Settings

Function, arrow, and ctrl keys act as
● Terminal keys ○ Windows keys

Backspace key sends
● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

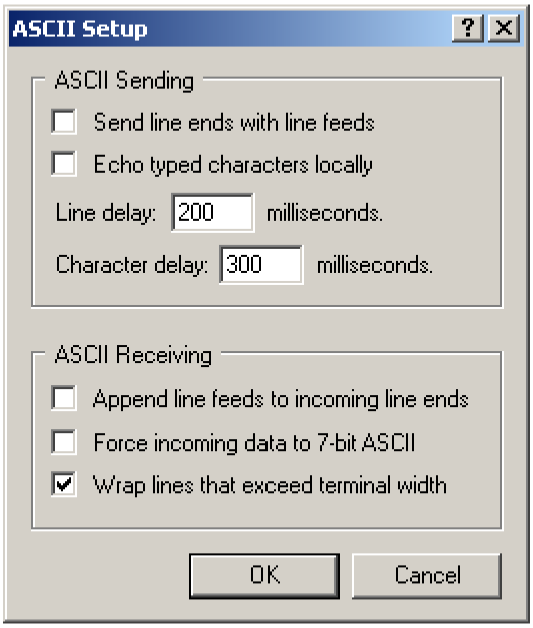
Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

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

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



ASCII Setup

ASCII Sending
□ Send line ends with line feeds
□ Echo typed characters locally
Line delay: 200 milliseconds.
Character delay: 300 milliseconds.

ASCII Receiving
□ Append line feeds to incoming line ends
□ Force incoming data to 7-bit ASCII
☑ Wrap lines that exceed terminal width

NOTE

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

----End

Result

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

NOTE

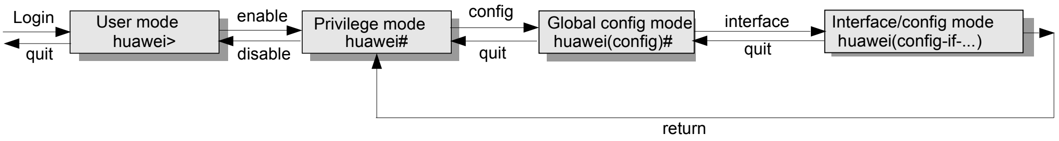
To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

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

Follow-up Procedure

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

Figure 1-12



Login Through Telnet (Outband Management)

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

Prerequisites

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

NOTE

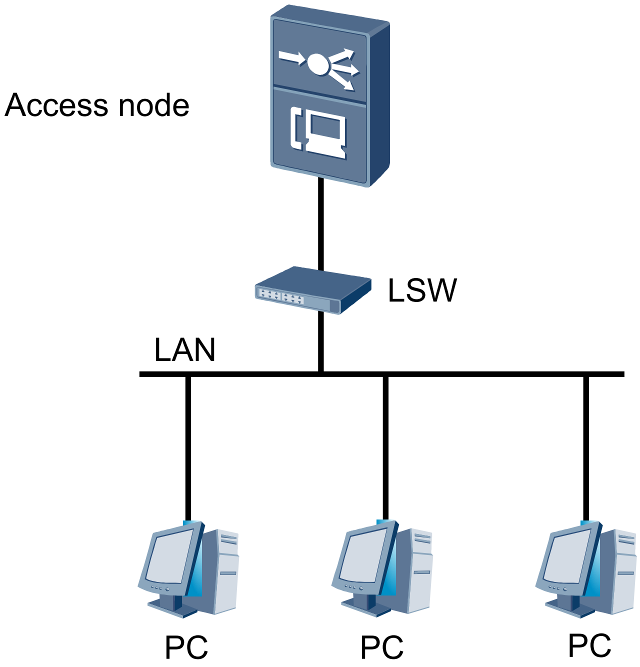
The default IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

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

Networking

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

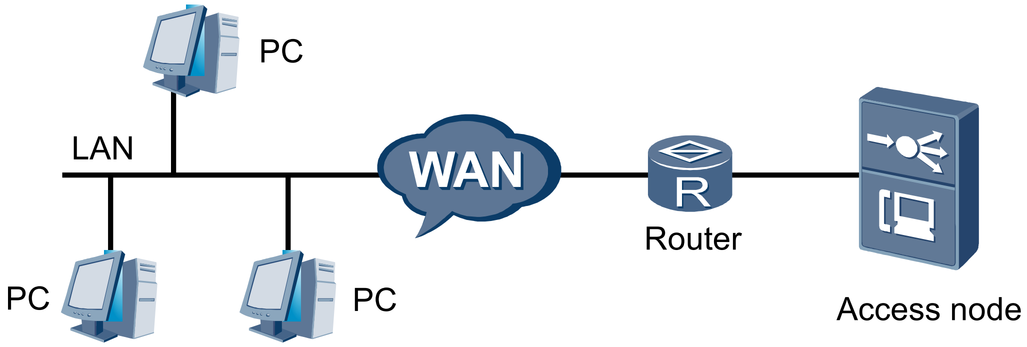
Figure 1-13 Example network for outband management through telnet in a LAN



NOTE

The MA5600T/MA5603T is connected to the LAN using the straight using cable, and the IP address of the maintenance Ethernet port of the MA5600T/MA5603T is in the same network segment as the IP address of the maintenance terminal. Alternatively, the Ethernet port of the maintenance terminal can be directly connected to the maintenance Ethernet port of the MA5600T/MA5603T to manage the MA5600T/MA5603T in the outband management mode. In such a condition, a crossover cable must be used.

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



Data Plan

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

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

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

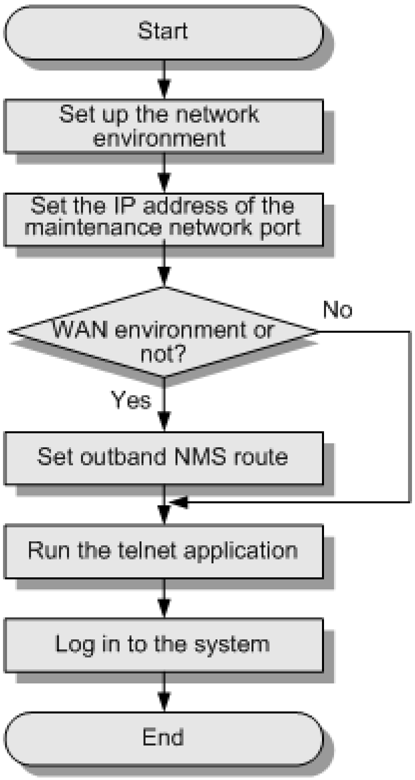
Table 1-13 Data plan for the outband management through telnet in a WAN

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

Flowchart

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

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


Start
Set up the network environment
Set the IP address of the maintenance network port
WAN environment or not?
No
Yes
Set outband NMS route
Run the telnet application
Log in to the system
End

Procedure

Step 1 Set up the network environment.

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

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

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

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

Step 3 Add a route for the outband management.

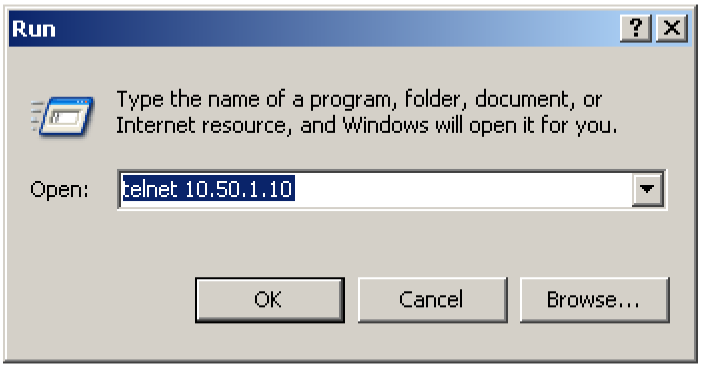
- If the network environment is set up as shown in Figure 1-13, you need not add a route.
- If the network environment is set up as shown in Figure 1-14, run the **ip route-static** command to add a route from the maintenance Ethernet port of the MA5600T/MA5603T to the maintenance terminal.

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

Step 4 Run the telnet application.

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

Figure 1-16 Running the telnet application



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 10.50.1.10

Step 5 Log in to the system.

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

```
>>:root
>>:admin

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

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

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

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

----End

Result

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

NOTE

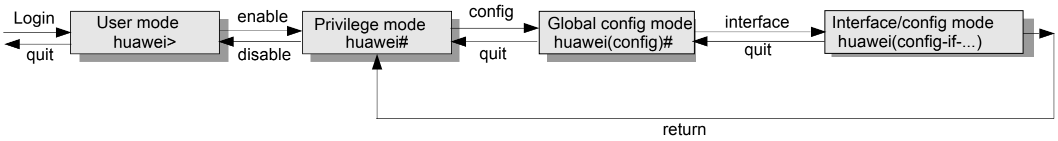
To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

Follow-up Procedure

- You can run the **idle-timeout** command to set the terminal timeout time. if you do not input commands within the specified timeout time, the system disconnects the terminal. By default, the terminal timeout time is set to 5 minutes. If you do not run any commands within 5 minutes, the system disconnects with the terminal. To perform any operation, you must have to log in to the system again.

- In the commissioning procedure, you must use the command, It is recommended that you know well the command modes first.**Figure 1-17** shows how to switch command modes.

Figure 1-17



Login Through Telnet (Inband Management)

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

Prerequisites

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

NOTE

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

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

Networking

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

NOTE

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

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

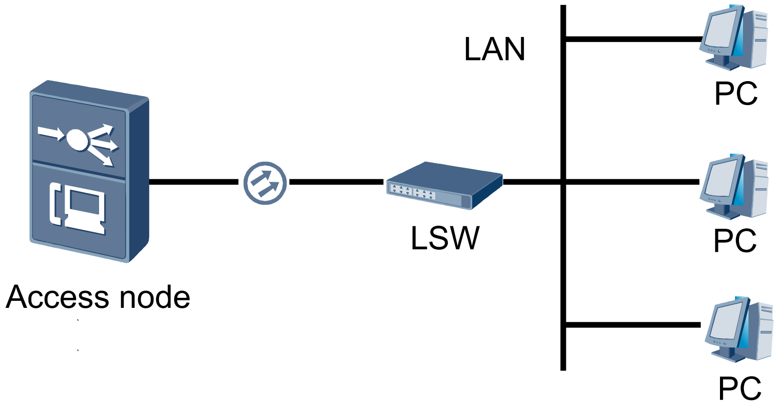
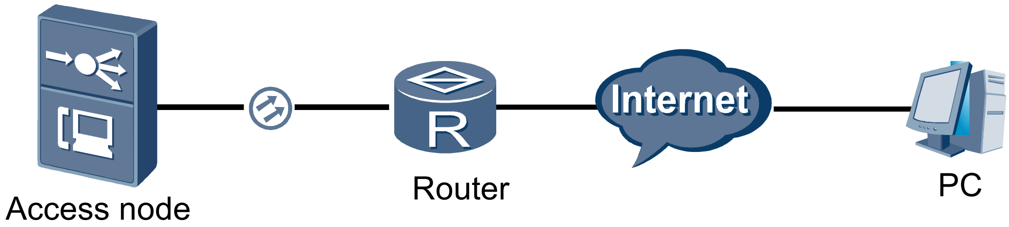


Figure 1-19 Example network for inband management through telnet in a WAN



Data Plan

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

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

Item	Data
Upstream port of the MA5600T/MA5603T	● VLAN ID: 30 ● Port: 0/19/0 ● IP address: 10.50.1.10/24
Maintenance terminal	IP address: 10.50.1.20/24 (in the same subnet as the IP address of the maintenance Ethernet port)

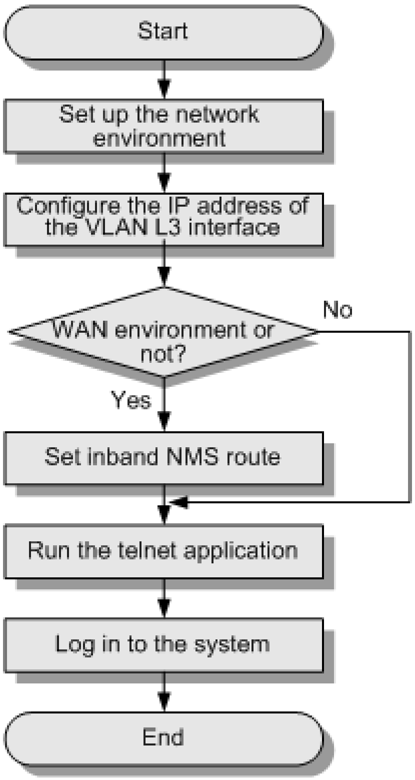
Table 1-15 Data plan for the inband management through telnet in a WAN

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

Flowchart

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

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


Start
Set up the network environment
Configure the IP address of the VLAN L3 interface
WAN environment or not?
No
Yes
Set inband NMS route
Run the telnet application
Log in to the system
End

Procedure

Step 1 Set up the network environment.

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

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

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

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

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

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

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

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

NOTE

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

Step 3 Add a route for the inband management.

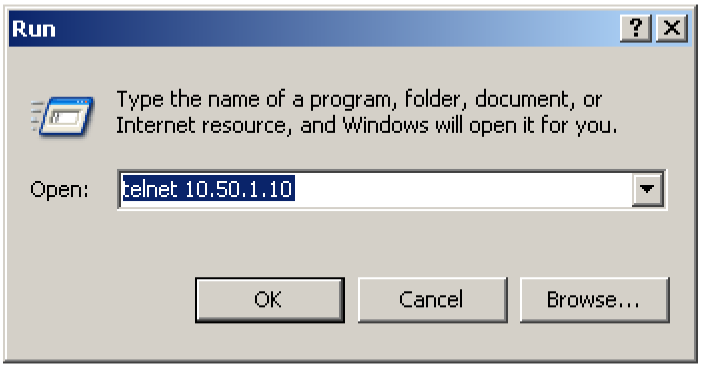
- If the network environment is set up as shown in **Figure 1-18**, you need not add a route.
- If the network environment is set up as shown in **Figure 1-19**, run the **ip route-static** command to add a route from the maintenance Ethernet port of the MA5600T/MA5603T to the maintenance terminal.

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

Step 4 Run the telnet application.

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

Figure 1-21 Running the telnet application



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 10.50.1.10

Step 5 Log in to the system.

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

```
>>:root
```

```
>>:admin

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

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

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

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

Parameter	Description
All user fail login information	Indicates the information about failed login of all users, which can be viewed only by user root or security administrator.
Access Type	Indicates the access type of the login.
IP-Address	Indicates the IP address of the login.
Time	Indicates the time of the login.
Login Times	Indicates the login times.

----End

Result

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

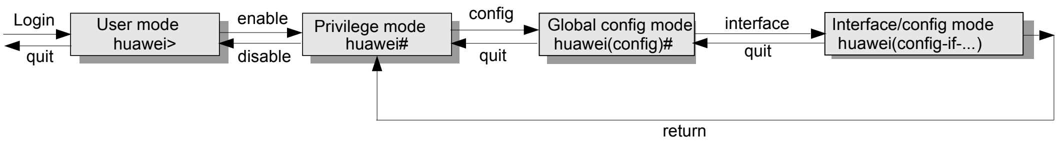
NOTE

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

Follow-up Procedure

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

Figure 1-22



Login Through SSH (Outband Management)

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

Prerequisites

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

NOTE

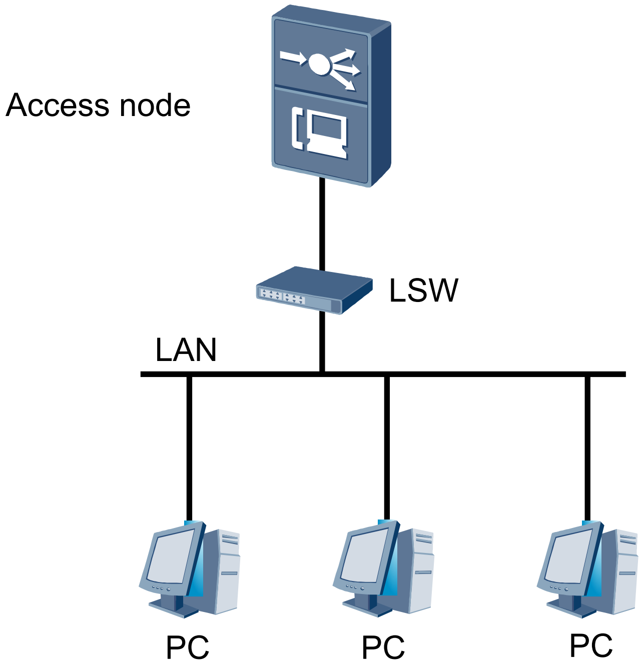
The default IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

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

Networking

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

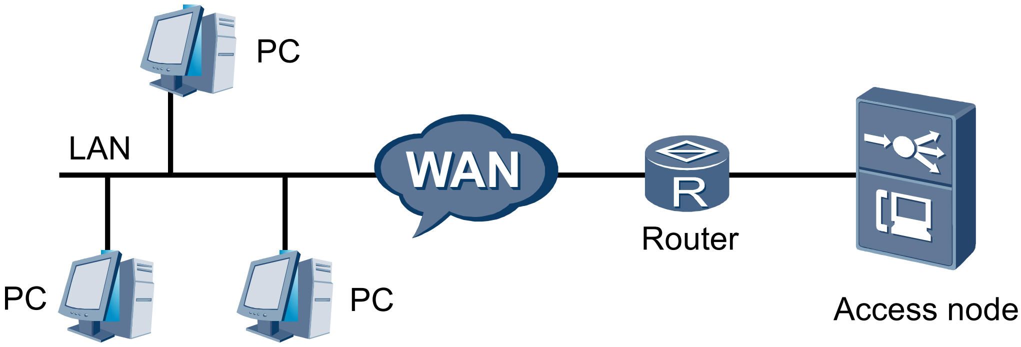
Figure 1-23 Example network for outband management through SSH in a LAN



NOTE

The MA5600T/MA5603T is connected to the LAN using the straight using cable, and the IP address of the maintenance Ethernet port of the MA5600T/MA5603T is in the same network segment as the IP address of the maintenance terminal. Alternatively, the Ethernet port of the maintenance terminal can be directly connected to the maintenance Ethernet port of the MA5600T/MA5603T to manage the MA5600T/MA5603T in the outband management mode. In such a condition, a crossover cable must be used.

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



Data Plan

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

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

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

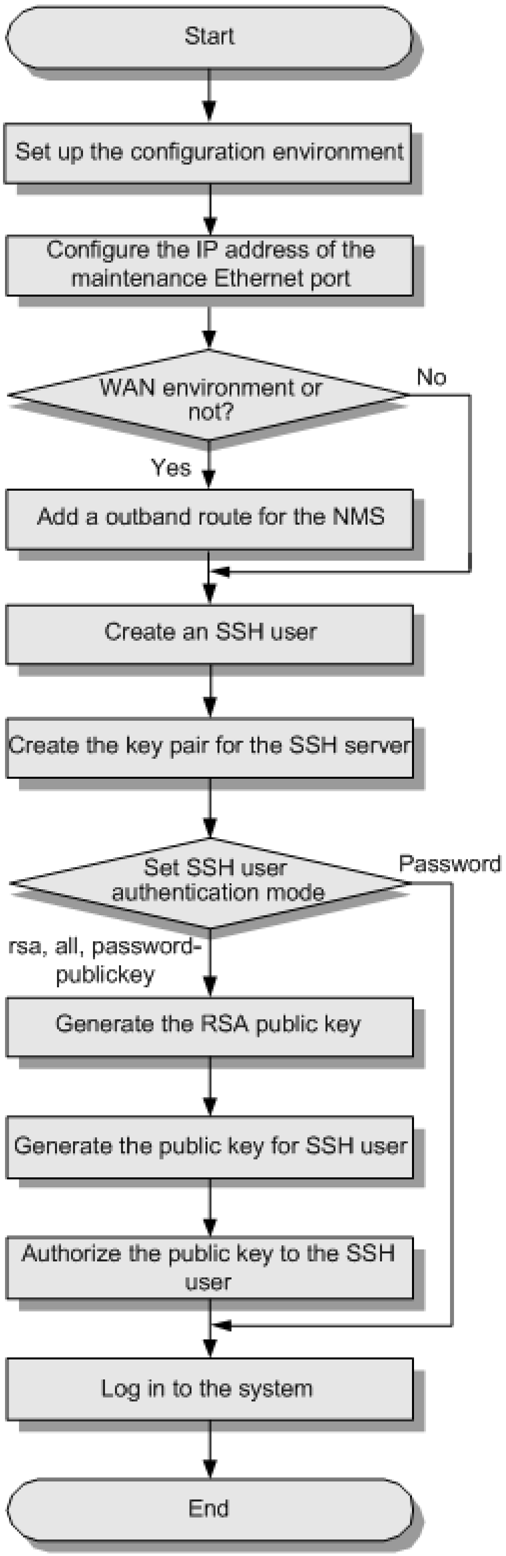
Table 1-17 Data plan for the outband management through SSH in a WAN

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

Flowchart

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

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


Start
Set up the configuration environment
Configure the IP address of the maintenance Ethernet port
WAN environment or not?
No
Yes
Add a outband route for the NMS
Create an SSH user
Create the key pair for the SSH server
Set SSH user authentication mode
Password
rsa, all, password-publickey
Generate the RSA public key
Generate the public key for SSH user
Authorize the public key to the SSH user
Log in to the system
End

Procedure

Step 1 Set up the network environment.

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

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

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

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

Step 3 Add a route for the outband management.

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

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

Step 4 Create a user.

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

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

Step 5 Create the local RSA key pair.

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

CAUTION

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

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

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

Step 6 Set the SSH user authentication mode.

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

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

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

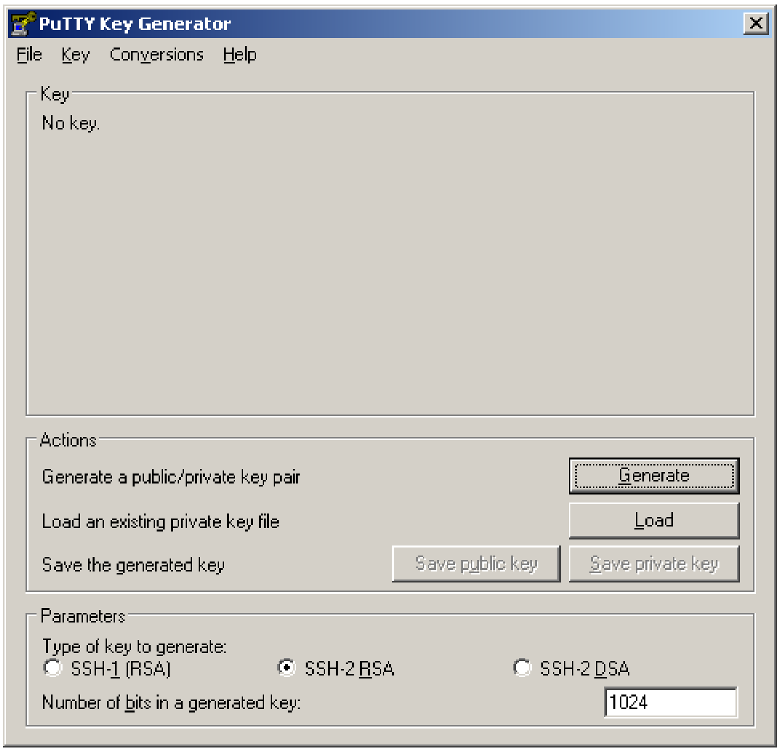
```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

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

Step 7 Generate the RSA public key.

1. Run the key generator.

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

Figure 1-26 Interface of the key generator



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

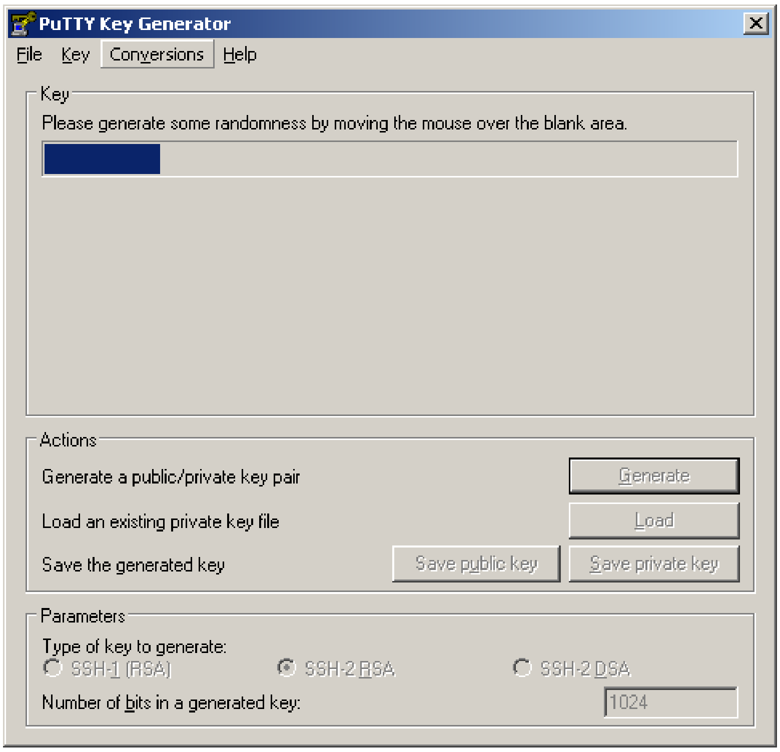
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

2. Generate the client key.

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

Figure 1-27 Interface of the key generator



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

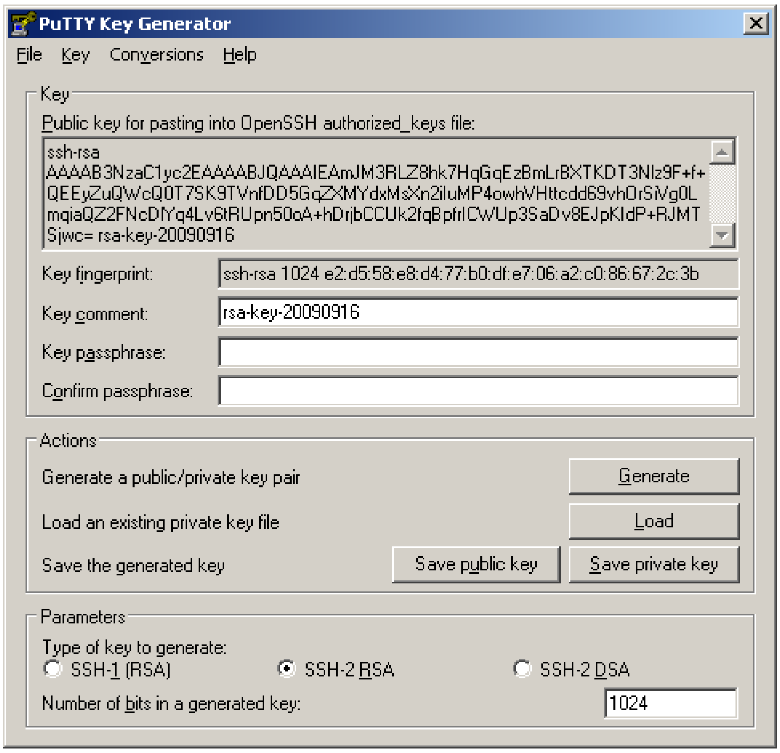
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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

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



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAmJM3RLZ8hk7HqGqEzBmLrBXTKDT3NIz9F+f+
QEEyZuQWcQ0T7SK9TVnfDD5GqZXMYdxMsXn2iluMP4owhVHttcdd69vh0rSiVg0L
mqiaQZ2FNcDIYq4Lv6tRUpn50oA+hDrjbCCUk2fqBpfrlCWUp3SaDv8EJpKIdP+RJMT
Sjwc= rsa-key-20090916
```

Key fingerprint: ssh-rsa 1024 e2:d5:58:e8:d4:77:b0:df:e7:06:a2:c0:86:67:2c:3b

Key comment: rsa-key-20090916

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

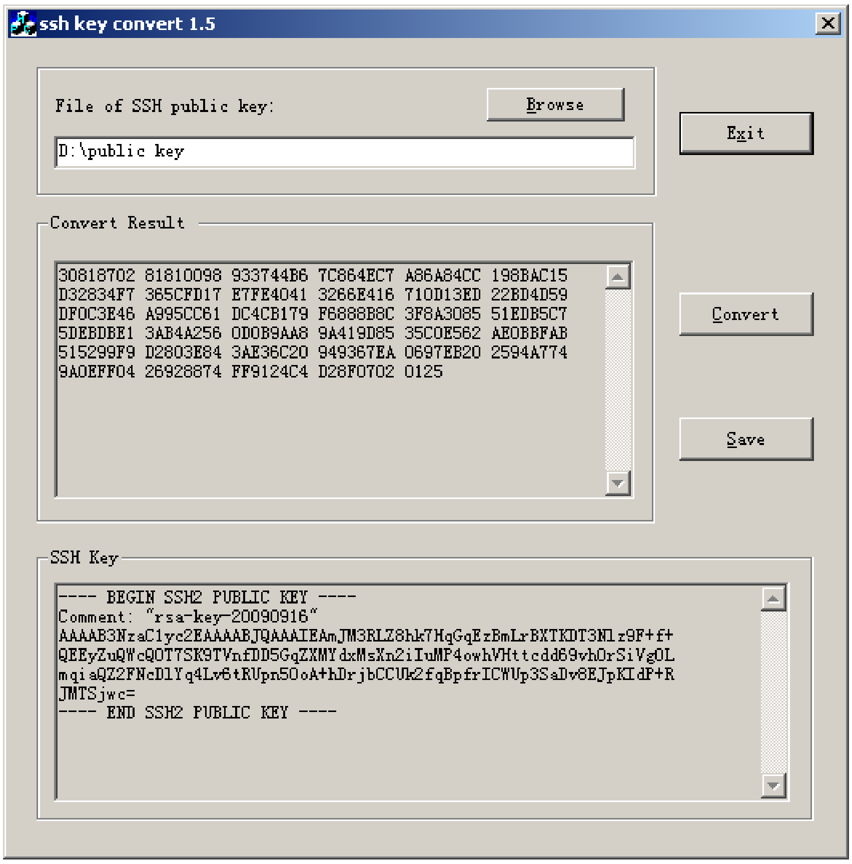
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

3. Generate the RSA public key.

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

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



File of SSH public key: D:\public key

Convert Result

```
30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC15
D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D59
DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C7
5DEBDBE1 3AB4A256 0D0B9AA8 9A419D85 35C0E562 AE0BBFAB
515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A774
9A0EFF04 26928874 FF9124C4 D28F0702 0125
```

SSH Key

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090916"
AAAAB3NzaC1yc2EAAAABJQAAAIEAmJM3RLZ8hk7HqGqEzBmLrBXTKDT3N1z9F+f+
QEEyZuQWcQOT7SK9TVnfDD5GqZXMYdxMsXn2iIuMP4owhVHttcdd69vhOrSiVgOL
mqiaQZ2FNcDlYq4Lv6tRUpn5OoA+hDrjbCCUk2fqBpfrICWUp3SaDv8EJpKIdP+R
JMTSjwc=
---- END SSH2 PUBLIC KEY ----
```

Step 8 Generate the public key for the SSH user.

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

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

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

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

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

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

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

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

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

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

Step 9 Assign the public key to the SSH user.

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

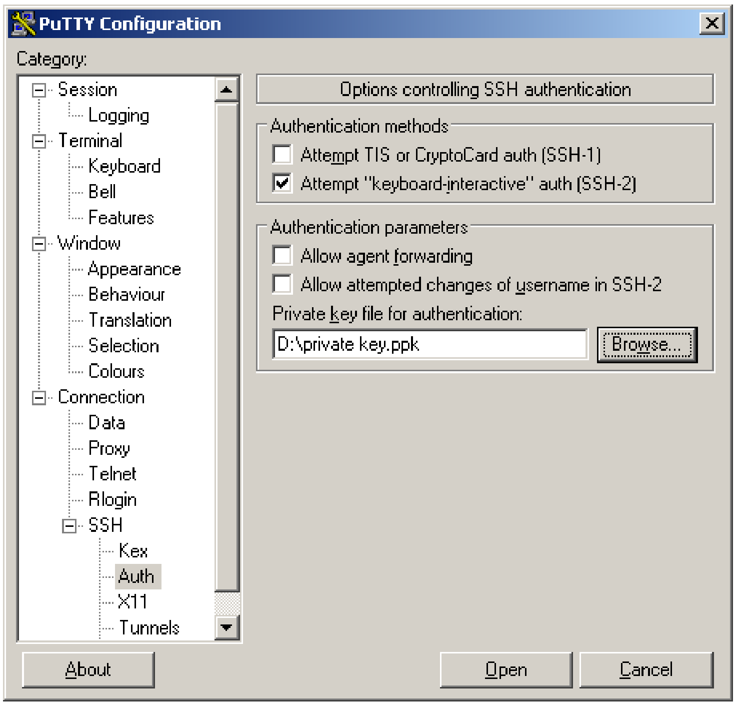
```
huawei(config)#ssh user huawei assign rsa-key key
```

Step 10 Log in to the system.

1. Run the client software.

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

Figure 1-30 Interface of the SSH client software



Authentication methods

☐ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding

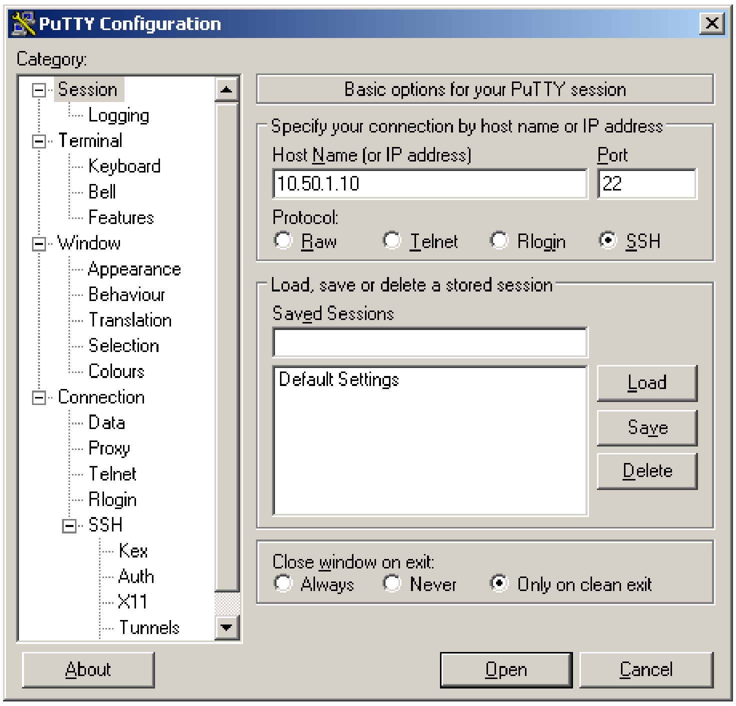
☐ Allow attempted changes of username in SSH-2

Private key file for authentication: D:\private key.ppk

2. Log in to the system.

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

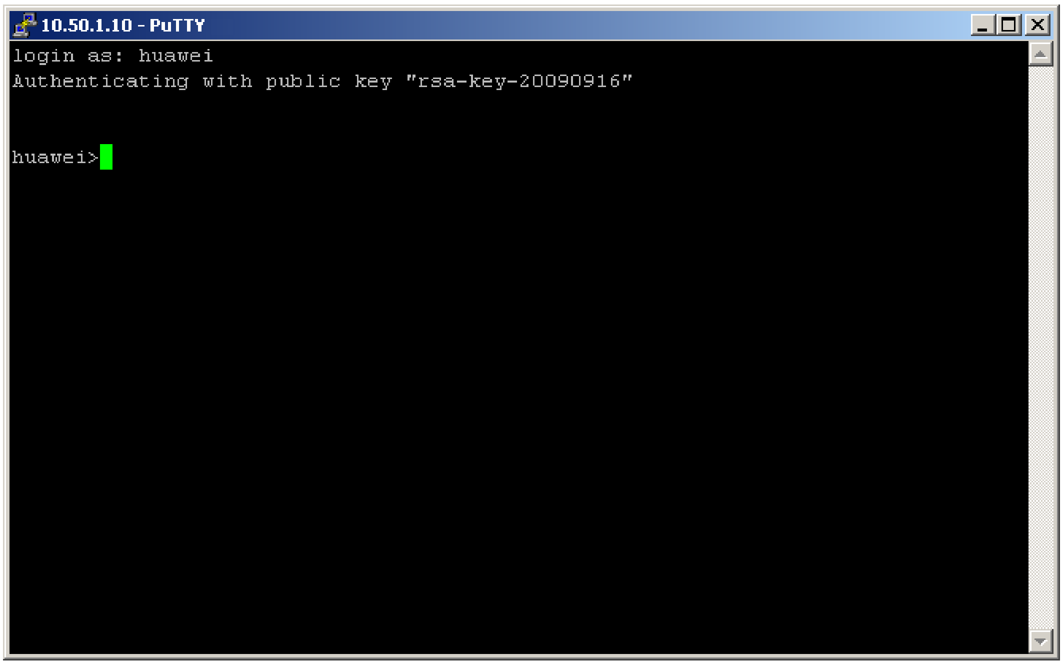
Figure 1-31 Interface for logging in to the system using the SSH client software



Host Name (or IP address): 10.50.1.10
Port: 22
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH
Saved Sessions: Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

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

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



```
login as: huawei
Authenticating with public key "rsa-key-20090916"


huawei>
```

----End

Result

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

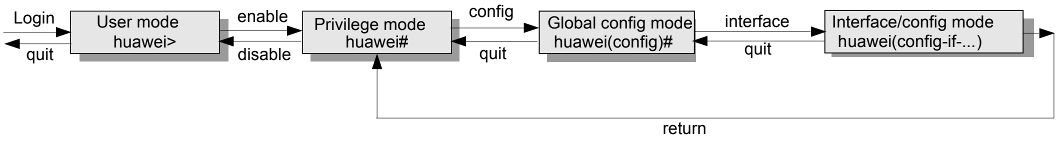
NOTE

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

Follow-up Procedure

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

Figure 1-33



Login Through SSH (Inband Management)

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

Prerequisites

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

NOTE

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

- For details about how to log in to the MA5600T/MA5603T by using the local serial port, see **Login Through the Local Serial Port**.
- For details about how to log in to the MA5600T/MA5603T by using the ETH port, see the following:

- Configure the IP address of the PC that is used for logging in to the MA5600T/MA5603T. This IP address is on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, configure the IP address to 10.11.104.6.
- After logging in to the MA5600T/MA5603T, run the **ip address** command to change the IP address of the device to 10.50.1.10/24.
- Change the IP address of the PC to be on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, change the IP address of the device to 10.50.1.11/24.

Networking

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

NOTE

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

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

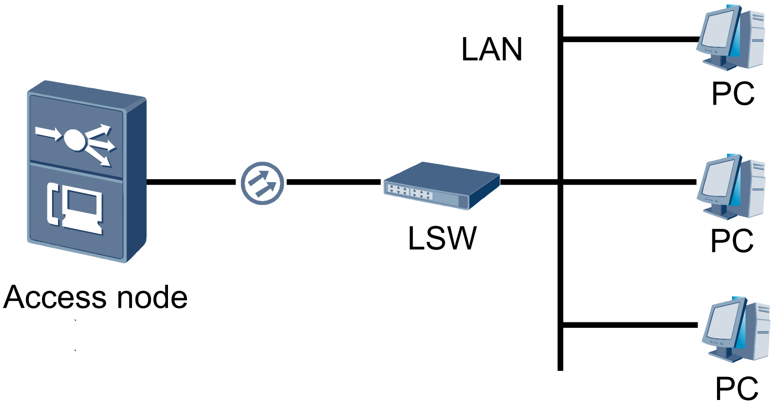
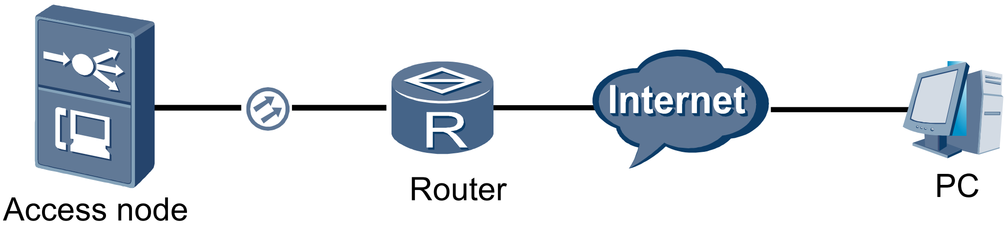


Figure 1-35 Example network for inband management through SSH in a WAN



Data Plan

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

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

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

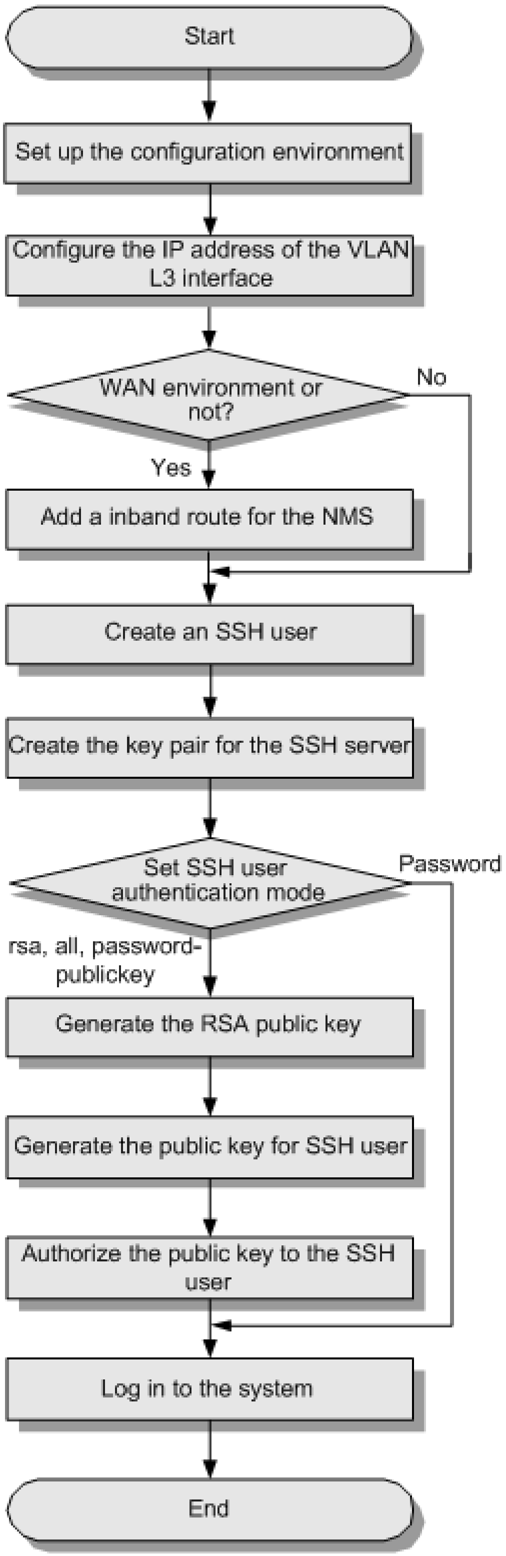
Table 1-19 Data plan for the inband management through SSH in a WAN

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

Flowchart

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

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


Start
Set up the configuration environment
Configure the IP address of the VLAN L3 interface
WAN environment or not?
No
Yes
Add a inband route for the NMS
Create an SSH user
Create the key pair for the SSH server
Set SSH user authentication mode
Password
rsa, all, password-publickey
Generate the RSA public key
Generate the public key for SSH user
Authorize the public key to the SSH user
Log in to the system
End

Procedure

Step 1 Set up the network environment.

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

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

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

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

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

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

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

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

NOTE

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

Step 3 Add a route for the inband management.

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

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

Step 4 Create a user.

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

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

Step 5 Create the local RSA key pair.

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

CAUTION

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

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

Step 6 Set the SSH user authentication mode.

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

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

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

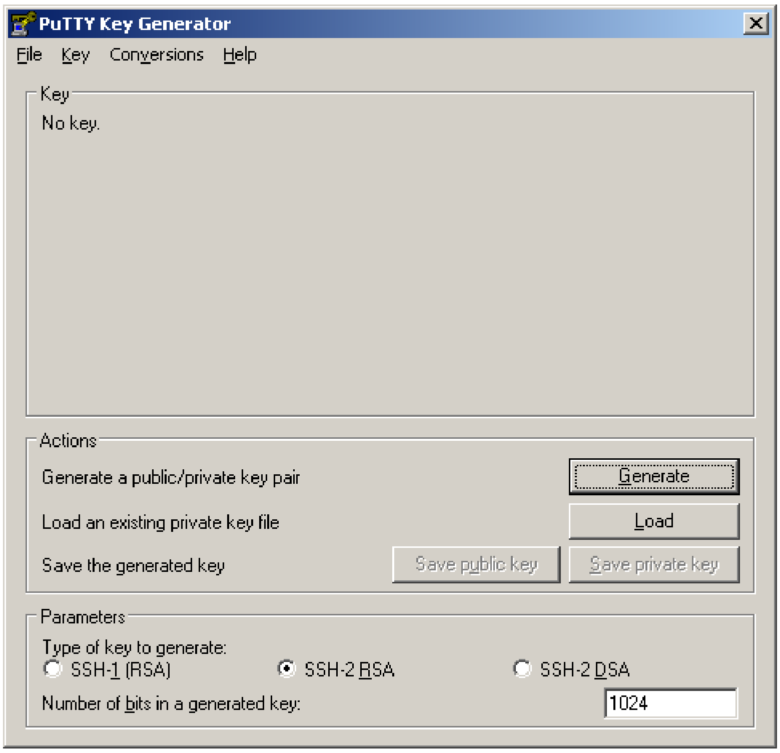
```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

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

Step 7 Generate the RSA public key.

1. Run the key generator.

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

Figure 1-37 Interface of the key generator



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

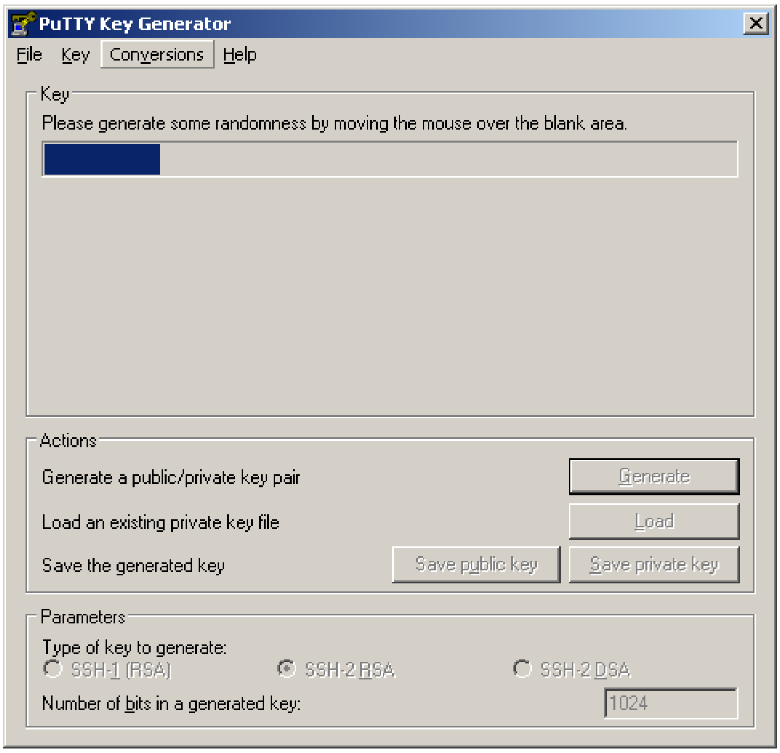
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

2. Generate the client key.

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

Figure 1-38 Interface of the key generator



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

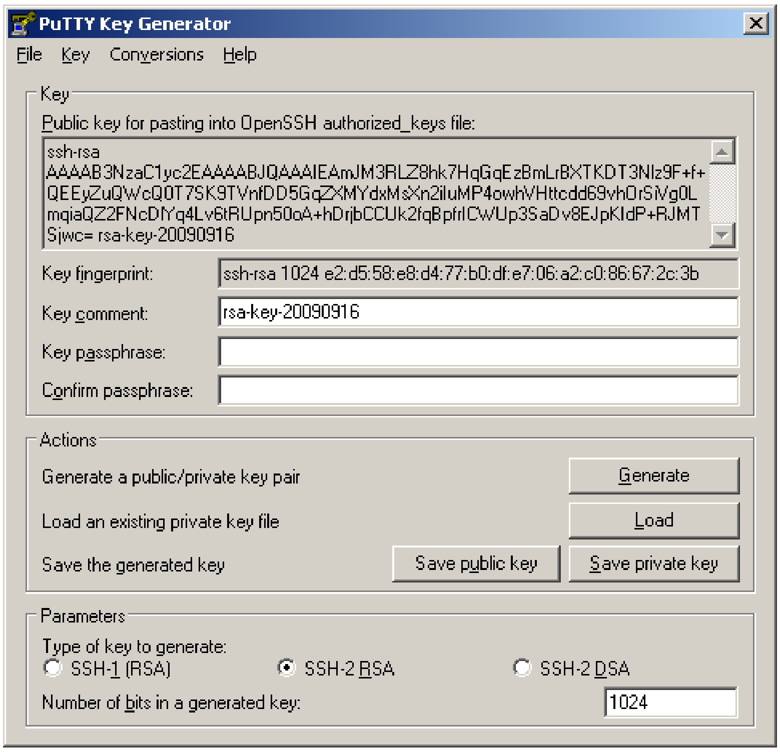
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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

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



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAmJM3RLZ8hk7HqGqEzBmLrBXTKDT3NIz9F+f+
QEEyZuQWcQ0T7SK9TVnfDD5GqZXMYdxMsXn2iluMP4owhVHttcdd69vh0rSiVg0L
mqiaQZ2FNcDlYq4Lv6tRUpn50oA+hDrjbCCUk2fqBpfrlCWUp3SaDv8EJpKIdP+RJMT
Sjwc= rsa-key-20090916
```

Key fingerprint: ssh-rsa 1024 e2:d5:58:e8:d4:77:b0:df:e7:06:a2:c0:86:67:2c:3b

Key comment: rsa-key-20090916

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

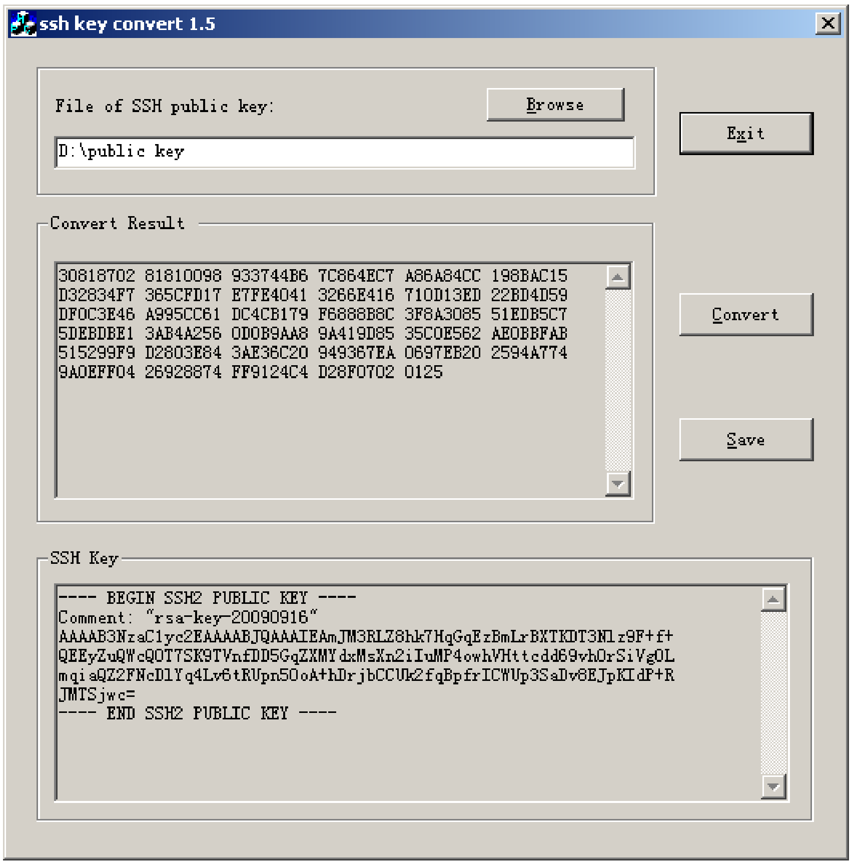
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

3. Generate the RSA public key.

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

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



```
D:\public key
```

```
30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC15
D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D59
DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C7
5DEBDBE1 3AB4A256 0D0B9AA8 9A419D85 35C0E562 AE0BBFAB
515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A774
9A0EFF04 26928874 FF9124C4 D28F0702 0125
```

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090916"
AAAAB3NzaC1yc2EAAAABJQAAAIEAmJM3RLZ8hk7HqGqEzBmLrBXTKDT3Nlz9F+f+
QEEyZuQWcQOT7SK9TVnfDD5GqZXMYdxMsXn2iIuMP4owhVHttcdd69vhOrSiVgOL
mqiaQZ2FNcDlYq4Lv6tRUpn5OoA+hDrjbCCUk2fqBpfrICWUp3SaDv8EJpKIdP+R
JMTSjwc=
---- END SSH2 PUBLIC KEY ----
```

Step 8 Generate the public key for the SSH user.

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

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

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

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

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

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

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

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

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

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

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

Step 9 Assign the public key to the SSH user.

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

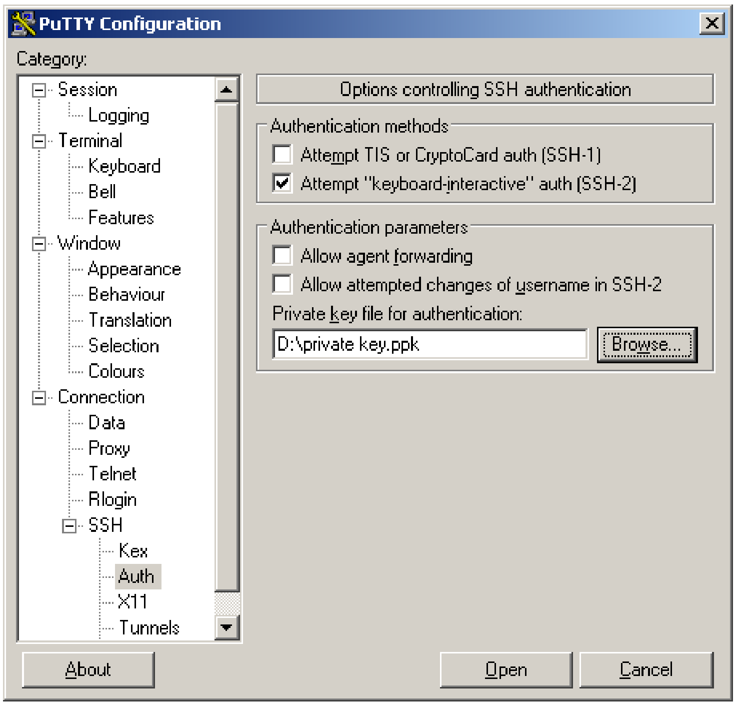
```
huawei(config)#ssh user huawei assign rsa-key key
```

Step 10 Log in to the system.

1. Run the client software.

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

   Figure 1-41 Interface of the SSH client software



Authentication methods

☐ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding

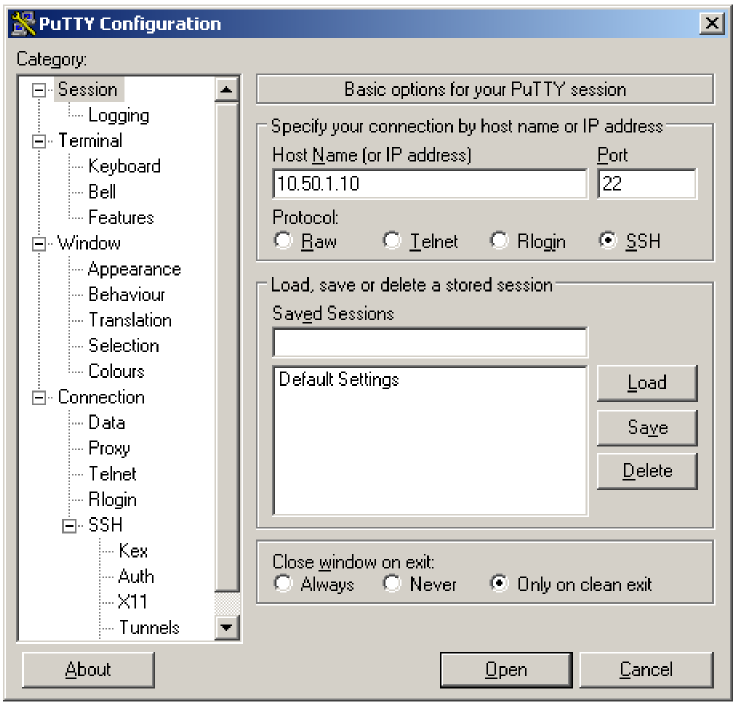
☐ Allow attempted changes of username in SSH-2

Private key file for authentication: D:\private key.ppk

2. Log in to the system.

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

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



Specify your connection by host name or IP address

Host Name (or IP address): 10.50.1.10

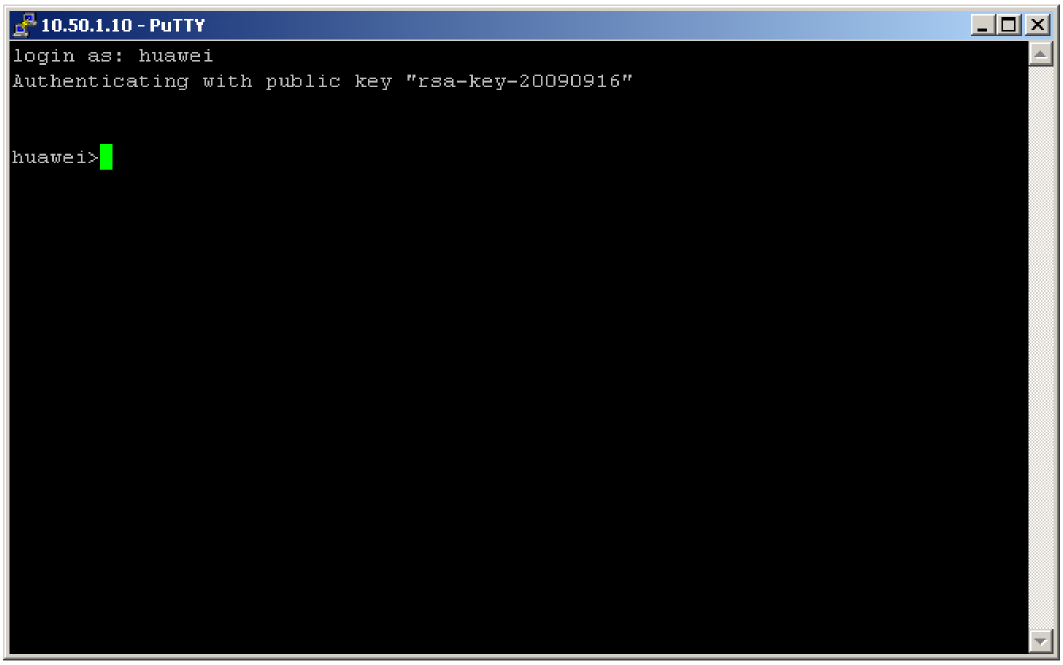
Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Close window on exit: ○ Always ○ Never ● Only on clean exit

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

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



```
login as: huawei
Authenticating with public key "rsa-key-20090916"


huawei>
```

----End

Result

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

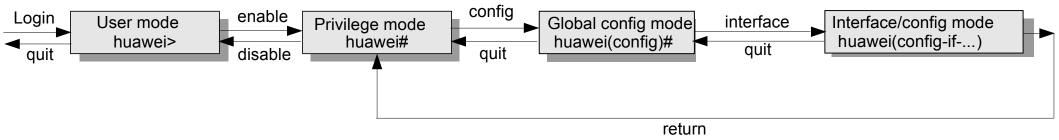
NOTE

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

Follow-up Procedure

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

Figure 1-44



1.3.6 Checking the Software State

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

Procedure

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

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

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

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

----End

Result

- The version of the host software, the version of the patch, the version of the boards and the state of the board software meet the deployment requirement.

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

Example

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

```
huawei>display language

  Local:
      Description: CHINESE SIMPLIFIED (DEFAULT LANGUAGE)
      Version:     MA5600V800R011C00
      Encoding:    GBK

  General:
      Description: ENGLISH (DEFAULT LANGUAGE)
      Version:     MA5600V800R011C00
      Encoding:    ANSI
huawei(config)#display patch all
  Software Version:MA5600V800R011C00
  SPC200T
  ------------------------------------------------------------------------
  Current Patch State:
  ------------------------------------------------------------------------
  Patch Name        Patch State     Delivery     Attribute     Dependency
  ------------------------------------------------------------------------
  SPC200T           running         temporary    cold patch    NO
  ------------------------------------------------------------------------
  Total:1
  Patches in the system cannot be rolled back
huawei>display version
{ <cr>|backplane<K>|frameid/slotid<S><Length 1-15> }:

  Command:
          display version

  VERSION : MA5600V800R011C00
  PRODUCT : MA5600T/
MA5603T

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

  Program Area A Version : MA5600V800R011C00
  Program Area B Version : MA5600V800R011C00

  Data Area A Version : MA5600V800R011C00
  Data Area B Version : MA5600V800R011C00
  --------------------------------------------------

  Uptime is 1 day(s), 5 hour(s), 7 minute(s), 33 second(s)

huawei#display version 0/9
  Main Board: H801SCUN
  ---------------------------------------
  PCB           Version: H801SCUN  VER B
  Base     BIOS Version: 213
  Extended BIOS Version: 216
  Software      Version: MA5600V800R011C00
  Logic         Version: (U48)113
  MAB           Version: 0002

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

1.3.7 Loading a Configuration Script

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

Prerequisites

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

Procedure

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

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

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

CAUTION

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

----End

Result

The loaded configuration script takes effect.

1.3.8 Changing the System Name

This topic describes how to customize the useful system name to differentiate MA5600T/MA5603Ts. This facilitates the management of the MA5600T/MA5603T.

Context

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

Procedure

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

----End

Result

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

Example

To name the first MA5600T/MA5603T at Longgang (a district in Shenzhen, Guangdong, China) **guangdong_shenzhen_longgang_MA5600T/MA5603T_A** based on the rule province_city_district_device name_SN, do as follows:

```
huawei(config)#guangdong_shenzhen_longgang_MA5600T/MA5603T_A
guangdong_shenzhen_longgang_MA5600T/MA5603T_A(config)#
```

1.3.9 Configuring the System Time

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

Procedure

Step 1 Configure the system time.

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

Step 2 Configure the system time zone.

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

NOTE

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

Step 3 Configure the system time stamp.

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

NOTE

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

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

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

NOTE

- The NTP protocol supports the client/server, peer, broadcast, and multicast working modes. The following uses the client/server mode as an example. If you need to set the working mode to other modes, see **2.3 Configuring the Network Time**.
- The L3 interface and the interface IP address must be available for the client and the server to communicate with each other.
- In the client/server mode, you need to configure only the client and the NTP master clock of the server.
- In the client/server mode, the client is synchronized to the server but the server will not be synchronized to the client.
- The clock stratum of the synchronizing device must be smaller than that of the synchronized device. Otherwise, the clock synchronization fails.
- The device that runs the NTP protocol can be synchronized to other clock sources or function as the clock source for synchronizing other clocks. In addition, this device and other devices can be set to synchronized from each other. When the device works in the client mode, you need not set the system time and the device is automatically synchronized to the remote server.

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

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

----End

Result

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

Example

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

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

  Command:
          time time-stamp utc
```

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

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

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

```
huawei(config)A#timezone GMT- 4:00
huawei(config)A#time 2010-01-01 12:10:10
huawei(config)A#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 2:00
```

1.3.10 Configuring a System User

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

Adding a System User

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

Prerequisites

You must have the administrator authority or higher authority.

Context

- The super user and the administrator have the authority to add a user at a lower level, that is:
  - The super user can add an administrator, an operator, or a common user.
  - The administrator can add only an operator or a common user.
- By default, the system has a super user with the name of root and password of admin. The super user cannot be added or deleted.
- The user name must be unique, and cannot be **all** or **online**.
- The super user and the administrator can add multiple users consecutively. Up to 127 (total 128 including the root user) users can be added to the system.
- The system supports up to 10 concurrently online terminal users.

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

Table 1-20 User attributes

User Attribute	Description
Account	An account is also called a user name and consists of 6-15 printable characters. The user name is unique in the system. It cannot contain any space and is case insensitive.
Password	A password consists of 6-15 characters. It must contain at least one digit and one letter, and is case-sensitive.
User profile	The name of a user profile consists of 1-15 printable characters. A user profile includes the validity period of the user name, validity period of the password, login time, and logout time.
Authority	Users are classified into three levels: common user, operator, and administrator. **NOTE** According to the operation authority, users of the MA5600T/MA5603T are classified into four levels: common user, operator, administrator, and super user. The user at one level can add only the user at a lower level. The following lists the authority of all users. ● Common users can perform basic system operations and simple query operations. ● Operators can configure the device and the services. ● For the administrator and the super user, they have the following similarities and differences: ● Similarities: ● Perform all configurations. ● Maintain and manage the device, user account, and user authority. ● Differences: ● Only one super user exists in the system; however, multiple administrators can coexist in the system. ● The super user can add an administrator, but an administrator has no authority to add the super user.

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

Procedure

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

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

----End

Result

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

Example

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

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

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

Modifying the System User Attributes

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

Prerequisites

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

Context

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

Table 1-21 Modifying the user attributes

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

Procedure

Step 1 Modify the system user attributes.

NOTE

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

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

  The password of a user consists of 6-15 characters, in which at least one digit and one letter must be contained. The password is case sensitive.

- Run the **terminal user user-profile** command to modify the profile bound to a user.
- Run the **terminal user level** command to modify the authority of a user.
- Run the **terminal user reenter** command to change the permitted reenter number of a user.
- Run the **terminal user apdinfo** command to modify the appended information about a user.

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

Step 2 Check the user information.

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

----End

Result

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

Example

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

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

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

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

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

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

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

1.3.11 Configuring a Board

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

Adding a Board Offline

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

Prerequisites

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

Context

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

Procedure

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

NOTE

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

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

----End

Result

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

Example

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

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

huawei(config)#display board 0/2

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

  -------------------------------------------------------------
    Port   Port   min-distance   max-distance   Optical-module
           type       (km)           (km)            status
  -------------------------------------------------------------
```

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

Confirming a Board

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

Prerequisites

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

Procedure

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

NOTE

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

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

----End

Result

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

Example

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

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

huawei(config)#display board 0/2

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

  -----------------------------------------------------------------------------
  Port    Port Type   Port Status      Line Profile  Alarm Profile  Ext Profile
  -----------------------------------------------------------------------------
     0    ADSL        Activating         1002             1           --
     1    ADSL        Activating         1002             1           --
     2    ADSL        Activating          1002              1           --
     3    ADSL        Activating          1002              1           --
     4    ADSL        Activating          1002              1           --
     5    ADSL        Activating          1002              1           --
     6    ADSL        Activating          1002              1           --
     7    ADSL        Activating          1002              1           --
     8    ADSL        Activating          1002              1           --
     9    ADSL        Activating          1002              1           --
    10    ADSL        Activating          1002              1           --
    11    ADSL        Activating          1002              1           --
    12    ADSL        Activating          1002              1           --
    13    ADSL        Activating          1002              1           --
    14    ADSL        Activating          1002              1           --
---- More ( Press 'Q' to break ) ----
```

Checking the Board Status

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

Procedure

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

----End

Result

All the boards work in the normal state. That is, all of the board status is displayed as **Normal**.

Example

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

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

1.3.12 Checking the Status of the Upstream Port

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

Procedure

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

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

----End

Result

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

1.3.13 Checking the Status of the Service Port

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

Prerequisites

NOTE

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

Procedure

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

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

----End

Result

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

- If the user port is an ADSL2+ port: **Status** is displayed as **Activated**.

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

1.3.14 Enabling the ONT Automatic Discovery function

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

Procedure

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

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

NOTE

Only GPON supports this operation.

----End

Result

Run the **display port info** command to query the configuration.

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

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

1.3.15 Testing the Optical Power of an Optical Port

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

Measuring the Transmit Optical Power of an OLT PON Port

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

Prerequisites

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

Tools, Meters and Materials

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

Impact on the System

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

Precautions

DANGER

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

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

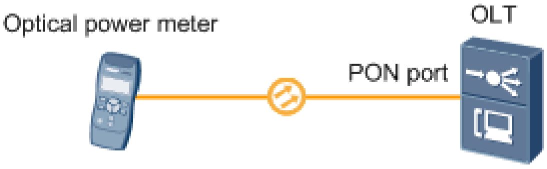
Procedure

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

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

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

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



NOTE

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

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

----End

Result

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

Measuring the Receive Optical Power of an OLT PON Port

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

Prerequisites

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

Tools, Meters and Materials

Burst optical power meter

Impact on System

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

Precautions

⚠ **DANGER**

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

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

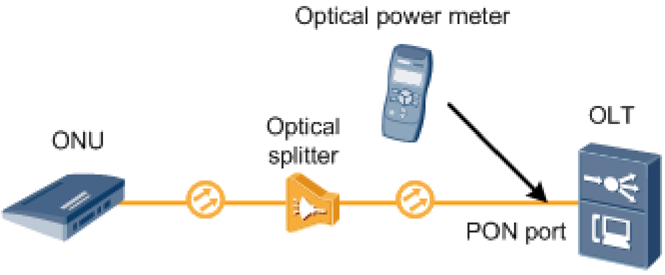
Procedure

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

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

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

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



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

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

----End

Result

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

Measuring the Transmit Optical Power of an ONU PON Port

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

Prerequisites

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

Tools and Meters

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

Impact on the System

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

Precautions

DANGER

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

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

Procedure

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

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

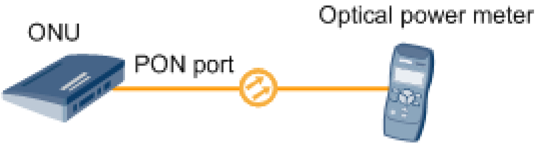
Step 2 Remove all optical fibers connected to the PON ports on the ONU and ensure that the ONU is not connected to any optical splitters or OLTs.

NOTE

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

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

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



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

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

NOTE

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

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

NOTE

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

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

----End

Result

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

Measuring the Receive Optical Power of an ONU PON Port

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

Prerequisites

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

Tools and Meters

Burst optical power meter or ordinary optical power meter

Impact on the System

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

Precautions

DANGER

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

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

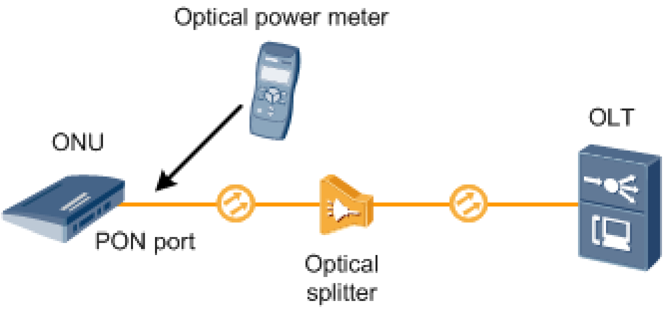
Procedure

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

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

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

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



NOTE

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

----End

Result

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

NOTE

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

1.3.16 Commissioning the EMU

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

Environment Monitoring Application

This topic describes the environment monitoring applications in different cabinets.

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

Table 1-22 Environment monitoring applications in different cabinets

Monitoring Solution	Cabinet Type	Typical Configuration
H801ESC Monitoring Solution	N63E-22	● Two MA5600T shelves ● One MA5600T shelf + one SPL shelf
EPS75-4815AF Monitoring Solution (PMIB01)	F01D500	One MA5600T(MA5603T) shelf
EPS30-4815AF Monitoring Solution (PMIB01)	F01S300	One MA5600T(MA5603T) shelf
Power3000 Monitoring Solution	-	Use this program when you need to monitor the external power supply Power 3000
Heat Exchanger Monitoring Solution	-	Heat Exchanger
Fan Tray Monitoring Solution	-	Fan Tray

Commissioning the EMU_ESC

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

Context

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

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

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

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

Table 1-23 Default configuration of the H801ESC board

Parameter	Default Value
Sub-node	15
Analog parameters	ESC analog parameter IDs: ● 0: allocated to the board temperature sensor by default (unable to be changed by the user). ● 1-4: allocated to the voltage sensor by default. – 1 indicates -48 V input of channel 0. – 2 indicates -48 V input of channel 1. – 3 indicates -48 V input of channel 2. – 4 indicates -48 V input of channel 3. ● 5-8: user-defined analog parameters allocated to other extended analog sensors, such as the temperature sensor and the humidity sensor.
	Upper and lower alarm thresholds ● Temperature: 5°C to 55°C ● Humidity: 0% RH to 80% RH

Parameter	Default Value
Digital parameters	ESC digital parameter IDs ● Allocated by default (unable to be changed by the user) – 0: MDF – 1: door status sensor 0 – 9: water – 10-13: lightning arresters 0-3 – 14-15: switches 11 and 12 – 16-17: switches 21 and 22 – 18-19: switches 31 and 32 – 20-21: switches 41 and 42 – 22: external sensor power ● User-defined IDs – 2-8: allocated to other extended digital sensors.
	Definition of user-defined alarm indexes 1: AC voltage; 2: AC switch; 3: battery voltage; 4: battery fuse; 5: load fuse; 6: rectifier unit; 7: secondary power supply; 8: door status of the cabinet; 9: door status of the equipment room; 10: window; 11: theft; 12: MDF; 13: fan; 14: fire; 15: smoke; 16: water; 17: diesel; 18: abnormal smell 19: air conditioner; 20: lightning arrester; 21: user-defined alarms of digital parameters

Procedure

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

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

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

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

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

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

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

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

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

----End

Result

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

Example

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

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

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

  EMU ID: 1                            ESC system parameter
  ----------------------------------------------------------------------------
  AnalogID Name           AlmUpper AlmLower TestUpper TestLower Unit    Type
     0     Temperature       55     5         127       -128    C       Voltage
     1     Input_-48V_0      72     38        127       -128    Volt    Voltage
     2     Input_-48V_1      72     38        127       -128    Volt    Voltage
     3     Input_-48V_2      72     38        127       -128    Volt    Voltage
     4     Input_-48V_3      72     38        127       -128    Volt    Voltage
     5     Temperature_1     70     -30       127       -128    C       Voltage
     6     -                 127    -128      127       -128    -       Voltage
     7     -                 127    -128      127       -128    -       Voltage
     8     -                 127    -128      127       -128    -       Voltage
  ----------------------------------------------------------------------------
  DigitalID Name              Level    |DigitalID Name              Level
```

```
          0     Wiring               1     |  1     Door0                0
          2     -                    1     |  3     -                    1
          4     -                    1     |  5     -                    1
          6     -                    1     |  7     Door_1               1     8
     -                    1     |    9     Water_Alarm          1
          10    Arrester 0           0     |  11    Arrester 1           0
          12    Arrester 2           0     |  13    Arrester 3           0
          14    SW11                 0     |  15    SW12                 0
          16    SW21                 0     |  17    SW22                 0
          18    SW31                 0     |  19    SW32                 0
          20    SW41                 0     |  21    SW42                 0
          22    Outer Sensor Power   0
        ----------------------------------------------------------------------------
```

Configuring the Environment Monitoring Parameters of the EPS30-4815AF

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

Mapping Between Monitoring Parameters and Device Ports

Table 1-24 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-24 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port
Temperature	Temperature and humidity
Humidity	Temperature and humidity
Digital 0	JTD1
Digital 1	JTD2
Digital 2	JTD3
Digital 3	JTD4
Digital 4	JTD5
Digital 5	JTD6
Digital 6	JTD7

NOTE

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

Data Plan

In this topic, the application in the F01S300 cabinet is considered as an example. Table 1-25 provides the data plan for configuring the monitoring parameters of the EPS30-4815AF.

Table 1-25 Data plan for configuring the monitoring parameters of the EPS30-4815AF

Item	Data Plan for the F01D500 Cabinet	Remarks
EMU	Type: POWER4830L	During the configuration of the EPS30-4815AF, the type of the EPS30-4815AF is selected as **POWER4830L**.
	SN: 0	-
	Subnode ID: 0	The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic	This parameter is set according to the actual requirements. automatic: The power system automatically adjusts the charging mode of batteries according to the status of the battery set. equalizing: The battery is charged forcibly so as to quickly compensate for the lost capacity of the battery. floating: The battery adjusts charging/ discharging when it is in saturation. Default: automatic.
	Equalized charging voltage of the battery: 56.5 V	This parameter is set according to the actual requirements. When setting the equalized charging voltage of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 56.5 V.
	Float charging voltage of the battery: 53.5 V	This parameter is set according to the actual requirements. When setting the float charging of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 53.5 V.
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	This parameter is set according to the actual requirements. In the normal state, the current of the power supply is not limited. The current-limiting function is enabled when the charging current of the battery set > current-limiting coefficient x nominal capacity of the battery set. Default value: 0.15.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Interval of battery equalized charging: 60 days	This parameter is set according to the actual requirements. If the continuous float charging duration of the rectifier unit exceeds the preset equalized charging interval, the battery enters the equalized charging state. Default: 60 days.
	Number of battery sets: 1	This parameter is set according to the actual requirements. The number of battery sets can be set to 0 or 1. That is, the system supports up to one battery set. Default value: 1.
	Capacity of the battery set: 75 AH	The battery capacity is configured according to the actual value. A 50 or 92 AH battery set is configured for the F01S300 cabinet, and a 75 AH battery set is configured for the F01E400 cabinet. Default: 65 AH.
Temperature compensation parameter of the battery	Upper temperature threshold of the battery set: 80°C	This parameter is set according to the actual requirements. Default: 80°C.
	Lower temperature threshold of the battery set: -20°C	This parameter is set according to the actual requirements. Default: -20°C.
	Temperature compensation coefficient of the battery set: 80 mV	This parameter is set according to the actual requirements. The temperature compensation coefficient refers to the variable of the float charging voltage of the battery set when the temperature of the battery set changes by every 1°C. Default: 80 mV.
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery set power-off permission status: permit	This parameter is set according to the actual requirements. Default: permit.
	Load power-off voltage: 44 V	This parameter is set according to the actual requirements. Default: 44 V.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Battery set power-off voltage: 43 V	This parameter is set according to the actual requirements. Default: 43 V.
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V	This parameter is set according to the actual requirements. When the AC voltage exceeds the preset overvoltage alarm threshold, the system reports an AC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 280 V.
	AC undervoltage alarm threshold of the power supply: 180 V	This parameter is set according to the actual requirements. When the AC voltage falls below the preset undervoltage alarm threshold, the system reports an AC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 180 V.
	DC overvoltage alarm threshold of the power supply: 58 V	This parameter is set according to the actual requirements. When the DC voltage exceeds the preset overvoltage alarm threshold, the system reports a DC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 58 V.
	DC undervoltage alarm threshold of the power supply: 45 V	This parameter is set according to the actual requirements. When the DC voltage falls below the preset undervoltage alarm threshold, the system reports a DC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 45 V.
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery high-temperature power-off permission status: permit	This parameter is set according to the actual requirements. Default: forbid.
	Temperature for load high-temperature power-off: 70°C	This parameter is set according to the actual requirements. Default: 65°C.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Temperature for battery high-temperature power-off: 53°C	This parameter is set according to the actual requirements. Default: 53°C.
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	This parameter is set according to the actual requirements. When the actual temperature reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 50°C.
	Lower alarm threshold of the temperature: -5°C	This parameter is set according to the actual requirements. When the actual temperature is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 0°C.
	Upper alarm threshold of the humidity: 80% RH	This parameter is set according to the actual requirements. When the actual humidity reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 80% RH.
	Lower alarm threshold of the humidity: 10% RH	This parameter is set according to the actual requirements. When the actual humidity is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 10% RH.
External extended digital parameters	Digital parameter ID: 0	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm.
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm.
	Valid level of digital parameter 1: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2	This digital parameter is set according to the actual requirements.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm.
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 4	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the smoke sensor is set here to monitor whether there is smoke in the actual environment. When there is smoke, the host reports an alarm.
	Valid level of digital parameter 4: high level	When the high level represents the valid level, the host does not report an alarm in the case of high level.
	Digital parameter ID: 5	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm.
	Valid level of digital parameter 5: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6	This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm.
	Valid level of digital parameter 6: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.

Configuration Process

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

Figure 1-49 shows the configuration process, and Table 1-26 lists the commands used during the configuration.

Figure 1-49 Configuration process of the EPS30-4815AF

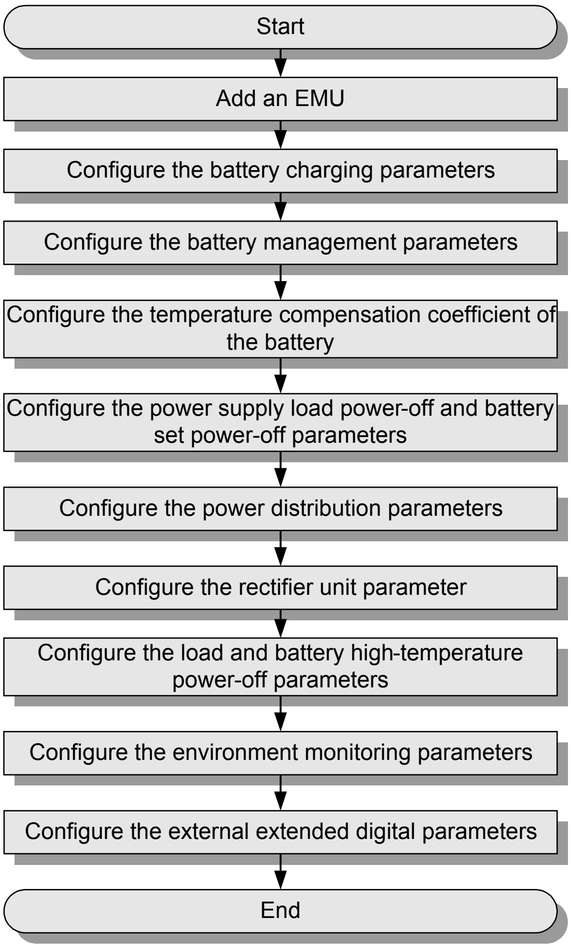

Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the rectifier unit parameter
Configure the load and battery high-temperature power-off parameters
Configure the environment monitoring parameters
Configure the external extended digital parameters
End

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

To...	Run the Command...
Add an EMU	**emu add**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**

To...	Run the Command...
Configure the temperature compensation coefficient of the battery	**power battery temperature**
Configure the power supply load power-off and battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the load and battery high-temperature power-off parameters	**power temperature-off**
Configure the environment monitoring parameters	**power environment**
Configure the external extended digital parameters	**power outside-digital**
Query the configuration parameters of the power system	**display power system parameter**

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

1. Log in to the device through the maintenance terminal and add an EMU.

```
huawei(config)#emu add 0 POWER4830L 0 0 POWER4830L
```

2. Query the status of the EPS30-4815AF.

```
huawei(config)#display emu 0
--------------------------------------------------------------------
  EMU name    : power4830l
  EMU type    : Pwr4875L
  Used or not : Used
  EMU state   : Normal
  Frame ID    : 0
  Subnode     : 0
--------------------------------------------------------------------
```

3. Enter the environment monitoring configuration mode and query the default configuration.

```
huawei(config)#interface emu 0
huawei(config-if-power4830l-0)#display power system parameter
  EMU ID: 0                             Power system
information

----------------------------------------------------------------------------
  Charge control state: Automatic
control
  Equalizing voltage  : 56.50V      Floating voltage      :
53.50V
  Charge Lmt quotiety : 0.15        Equalizing time       : 60
days
  Battery number      : 1           Battery 0 capacity    : 65
AH
  battery temperature test upper :  80C  battery temperature test lower:
-20C
```

```
  temperature redeem quotiety    :
80mV
  battery temperature alarm upper:  50C  battery temperature alarm lower:
0C
  Load off permit     : Forbid      Load off voltage      :
44.00V
  Battery off permit  : Permit      Battery off voltage   :
43.00V
  AC over alarm volt  : 280V        AC lack alarm voltage :
180V
  DC over alarm volt  : 58 V        DC lack alarm voltage : 45
V
  Power module number :
5
  module 0 address: 1               module 0 switch state   :
On
  module 1 address: 2               module 1 switch state   :
On
  module 2 address: 3               module 2 switch state   :
On
  module 3 address: 4               module 3 switch state   :
On
  module 4 address: 5               module 4 switch state   :
On
  Load high-temperature-off permit        :
Forbid
  Load high-temperature-off temperature   : 65
C
  Battery high-temperature-off permit     :
Permit
  Battery high-temperature-off temperature: 53
C

----------------------------------------------------------------------------
huawei(config-if-power4830l-0)#display power environment parameter

  EMU ID: 0                            Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        50       0        55        -5      C
Current
     1     Humidity           80       10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     -
1
     4     -                     1     |   5     -
1
     6     -
1
  ----------------------------------------------------------------------------
```

The results show that the power, temperature, and humidity parameters have been configured automatically in the system; however, certain parameters need to be modified, and certain extended monitoring parameters need to be added.

4. Configure the battery charging parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power charge** command.

5. Configure the battery management parameters.

```
huawei(config-if-power4830l-0)#power battery parameter 0.15 60 1 75
```

6. Configure the temperature compensation coefficient of the battery.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power battery temperature** command.

7. Configure the power supply load power-off and battery set power-off parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power off** command.

8. Configure the power distribution parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power supply-parameter** command.

9. Configure the rectifier unit parameter.

10. Configure the load and battery high-temperature power-off parameters.

```
huawei(config-if-power4830l-0)#power temperature-off load-off-state forbid
load-off-temperature 70 battery-off-state permit battery-off-temperature 53
```

11. Configure the environment parameters.

   - Configure the temperature parameters.

```
huawei(config-if-power4830l-0)#power environment temperature 68 -5 80 -20
```

   - Configure the humidity parameters.

     If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power environment humidity** command.

12. Configure the extended digital parameters.

```
huawei(config-if-power4830l-0)#power outside_digital 3 available-level low-
level name SPD digital-alarm 20
huawei(config-if-power4830l-0)#power outside-digital 4 available-level high-
level name Smoke digital-alarm 15
huawei(config-if-power4830l-0)#power outside-digital 5 available-level low-
level name HEX digital-alarm 13
huawei(config-if-power4830l-0)#power outside-digital 6 available-level low-
level name MDF-door digital-alarm 9
```

13. Query the information about the configured parameters and environment parameters of the power system.

```
huawei(config-if-power4830l-0)#display power system parameter
EMU ID: 0                            Power system information

----------------------------------------------------------------------------
  Charge control state: Automatic
control
  Equalizing voltage  : 56.50V      Floating voltage      :
53.50V
  Charge Lmt quotiety : 0.15        Equalizing time       : 60
days
  Battery number      : 1           Battery 0 capacity    : 75
AH
  Batt_temp_test_upper: 80 C        Batt_temp_test_lower  :
-20C
  Temp redeem quotiety: 80
mV
  Load off permit     : Forbid      Load off voltage      :
44.00V
  Battery off permit  : Permit      Battery off voltage   :
43.00V
  AC over alarm volt  : 280V        AC lack alarm voltage :
180V
  DC over alarm volt  : 58 V        DC lack alarm voltage : 45
V
  Load high-temperature-off permit        :
Forbid
```

```
  Load high-temperature-off temperature   : 70
C
  Battery high-temperature-off permit     :
Permit
  Battery high-temperature-off temperature: 53
C

-----------------------------------------------------------------------------

huawei(config-if-power4830l-0)#display power environment parameter

  EMU ID: 0                            Power environment configration
parameter

-----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        68      -5       80        -20     C
Current
     1     Humidity           80      10       100       0       %R.H.
Current

-----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     SPD
0
     4     Smoke                 1     |   5     Hex
0
     6     MDF-door
0
  -----------------------------------------------------------------------------
```

14. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated.

```
huawei(config-if-power4830l-0)#display power alarm
  EMU ID: 0                            Power alarm
information

-----------------------------------------------------------------------------
  Mains supply yes : Yes            Mains supply lack :
Normal
  Total Vol lack   :
Normal
  Load fuse        :
Connect
  Load off         : On             Battery off       :
On
  Battery 0 loop   :
Disconnect
  Module 0         :
Normal
  Module 1         :
Normal
  Door alarm       : Alarm          Water alarm       :
Normal
  Smoke alarm        : Normal         Wiring alarm      :
Normal
  Environment Temperature       : Normal  Environment Humidity       :
Normal

-----------------------------------------------------------------------------
  Name                             State |Name
State
  Spare Dig0                       Normal|Spare Dig1
Normal
  Spare Dig2                       Normal|Spare Dig3(SPD)
```

```
Normal
  Spare Dig4(Smoke)                Normal|Spare Dig5(HEX)
Normal
  Spare Dig6(MDF-door)
Normal

----------------------------------------------------------------------------
huawei(config-if-power4830l-0)#quit
```

NOTE

The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable. These two door status sensors are automatically configured by the system. The door status alarm is generated because the door is open.

15. Save the data.
    ```
    huawei(config)#save
    ```
16. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Configuring the Environment Monitoring Parameters of the EPS75-4815AF

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

Mapping Between Monitoring Parameters and Device Ports

Table 1-27 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-27 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

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

Monitoring Parameter Displayed on the Host	Device Port	Application in the N66 Cabinet	Application in the F01D500 Cabinet
Digital 3	JTD4	Not connected by default, used to add a user-defined monitoring digital parameter	surge protector
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter	Smoke sensor
Digital 5	JTD6	Not connected by default, used to add a user-defined monitoring digital parameter	Heat exchanger
Digital 6	JTD7	Not connected by default, used to add a user-defined monitoring digital parameter	Door status sensor of the MDF compartment
Door alarm	JTM1	Not connected by default, used to monitor a door status sensor	Door status sensors of the device compartment and heat exchanger compartment
Wiring alarm	JTP1	Not connected by default, used to monitor a MDF sensor	MDF
Battery Tem	BAT_WE	Battery temperature sensor	Battery temperature sensor
environment Tem/environment Hum	TEM-HU	Not connected by default.	Temperature and humidity sensor

NOTE

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

Data Plan

The data plan of the EPS75-4815AF in the N66 cabinet is the same as that in the F01D500 cabinets. In this topic, the application in the F01D500 cabinet is considered as an example. **Table 1-28** provides the data plan for configuring the monitoring parameters of the EPS75-4815AF.

Table 1-28 Data plan for configuring the monitoring parameters of the EPS75-4815AF

Item	Data Plan for the F01D500 Cabinet	Remarks
EMU	Type: POWER4875L	During the configuration of the EPS75-4815AF, the type of the EPS75-4815AF is selected as **POWER4875L**.
	SN: 0	-
	Subnode ID: 0	The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic	This parameter is set according to the actual requirements. automatic: The power system automatically adjusts the charging mode of batteries according to the status of the battery set. equalizing: The battery is charged forcibly so as to quickly compensate for the lost capacity of the battery. floating: The battery adjusts charging/ discharging when it is in saturation. Default: automatic.
	Equalized charging voltage of the battery: 56.5 V	This parameter is set according to the actual requirements. When setting the equalized charging voltage of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 56.5 V.
	Float charging voltage of the battery: 53.5 V	This parameter is set according to the actual requirements. When setting the float charging of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 53.5 V.
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	This parameter is set according to the actual requirements. In the normal state, the current of the power supply is not limited. The current-limiting function is enabled when the charging current of the battery set > current-limiting coefficient x nominal capacity of the battery set. Default value: 0.15.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Interval of battery equalized charging: 60 days	This parameter is set according to the actual requirements. If the continuous float charging duration of the rectifier unit exceeds the preset equalized charging interval, the battery enters the equalized charging state. Default: 60 days.
	Number of battery sets: 1	This parameter is set according to the actual requirements. The number of battery sets can be set to 0 or 1. That is, the system supports up to one battery set. Default value: 1.
	Capacity of the battery set: 150 AH	The battery capacity is configured according to the actual value. The N66 cabinet uses different external batteries according to the actual conditions, the F01D500 cabinet uses the 150 AH or 194 AH batteries. Default: 65 AH.
Temperature compensation parameter of the battery	Upper temperature threshold of the battery set: 80°C	This parameter is set according to the actual requirements. Default: 80°C.
	Lower temperature threshold of the battery set: -20°C	This parameter is set according to the actual requirements. Default: -20°C.
	Temperature compensation coefficient of the battery set: 80 mV	This parameter is set according to the actual requirements. The temperature compensation coefficient refers to the variable of the float charging voltage of the battery set when the temperature of the battery set changes by every 1°C. Default: 80 mV.
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery set power-off permission status: permit	This parameter is set according to the actual requirements. Default: permit.
	Load power-off voltage: 44 V	This parameter is set according to the actual requirements. Default: 44 V.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Battery set power-off voltage: 43 V	This parameter is set according to the actual requirements. Default: 43 V.
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V	This parameter is set according to the actual requirements. When the AC voltage exceeds the preset overvoltage alarm threshold, the system reports an AC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 280 V.
	AC undervoltage alarm threshold of the power supply: 180 V	This parameter is set according to the actual requirements. When the AC voltage falls below the preset undervoltage alarm threshold, the system reports an AC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 180 V.
	DC overvoltage alarm threshold of the power supply: 58 V	This parameter is set according to the actual requirements. When the DC voltage exceeds the preset overvoltage alarm threshold, the system reports a DC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 58 V.
	DC undervoltage alarm threshold of the power supply: 45 V	This parameter is set according to the actual requirements. When the DC voltage falls below the preset undervoltage alarm threshold, the system reports a DC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 45 V.
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery high-temperature power-off permission status: permit	This parameter is set according to the actual requirements. Default: forbid.
	Temperature for load high-temperature power-off: 70°C	This parameter is set according to the actual requirements. Default: 65°C.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Temperature for battery high-temperature power-off: 53°C	This parameter is set according to the actual requirements. Default: 53°C.
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	This parameter is set according to the actual requirements. When the actual temperature reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 50°C.
	Lower alarm threshold of the temperature: -5°C	This parameter is set according to the actual requirements. When the actual temperature is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 0°C.
	Upper alarm threshold of the humidity: 80% RH	This parameter is set according to the actual requirements. When the actual humidity reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 80% RH.
	Lower alarm threshold of the humidity: 10% RH	This parameter is set according to the actual requirements. When the actual humidity is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 10% RH.
External extended digital parameters	Digital parameter ID: 0	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm.
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm.
	Valid level of digital parameter 1: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2	This digital parameter is set according to the actual requirements.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm.
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 4	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the smoke sensor is set here to monitor whether there is smoke in the actual environment. When there is smoke, the host reports an alarm.
	Valid level of digital parameter 4: high level	When the high level represents the valid level, the host does not report an alarm in the case of high level.
	Digital parameter ID: 5	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm.
	Valid level of digital parameter 5: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6	This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm.
	Valid level of digital parameter 6: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.

Configuration Process

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

Figure 1-50 shows the configuration process, and Table 1-29 lists the commands used during the configuration.

Figure 1-50 Configuration process of the EPS75-4815AF

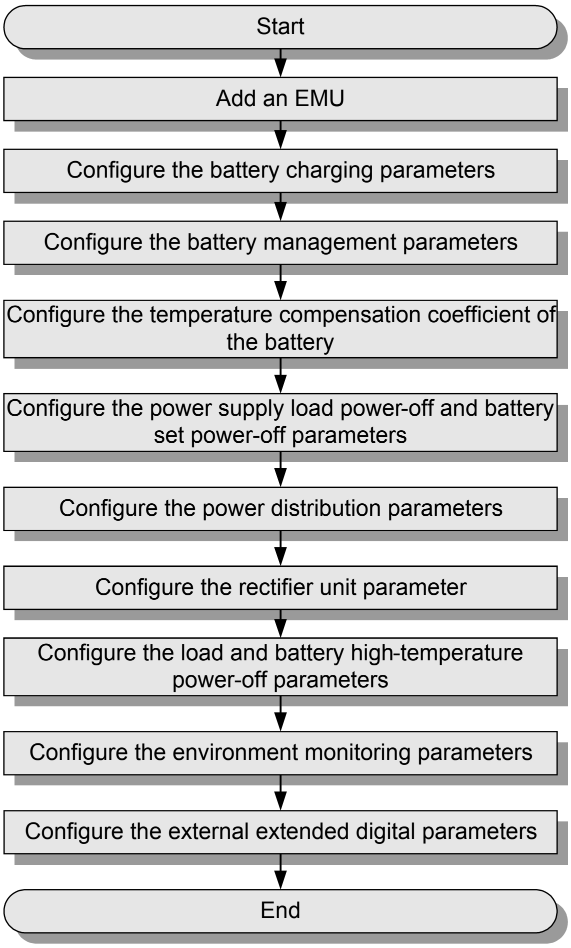

Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the rectifier unit parameter
Configure the load and battery high-temperature power-off parameters
Configure the environment monitoring parameters
Configure the external extended digital parameters
End

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

To...	Run the Command...
Add an EMU	**emu add**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**

To...	Run the Command...
Configure the temperature compensation coefficient of the battery	**power battery temperature**
Configure the power supply load power-off and battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the load and battery high-temperature power-off parameters	**power temperature-off**
Configure the environment monitoring parameters	**power environment**
Configure the external extended digital parameters	**power outside-digital**
Query the configuration parameters of the power system	**display power system parameter**

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

1. Log in to the device through the maintenance terminal and add an EMU.

   ```
   huawei(config)#emu add 0 POWER4875L 0 0 POWER4875L
   ```

2. Query the status of the EPS75-4815AF.

   ```
   huawei(config)#display emu 0
   --------------------------------------------------------------------
     EMU name    : POWER4875L
     EMU type    : Pwr4875L
     Used or not : Used
     EMU state   : Normal
     Frame ID    : 0
     Subnode     : 0

   --------------------------------------------------------------------
   ```

3. Enter the environment monitoring configuration mode and query the default configuration.

   ```
   huawei(config)#interface emu 0
   huawei(config-if-power4875l-0)#display power system parameter

   EMU ID: 0                             Power system information

   ----------------------------------------------------------------------------
     Charge control state: Automatic
   control
     Equalizing voltage  : 56.50V      Floating voltage      :
   53.50V
     Charge Lmt quotiety : 0.15        Equalizing time       : 60
   days
     Battery number      : 1           Battery 0 capacity    : 65
   AH
     Batt_temp_test_upper: 80 C        Batt_temp_test_lower  :
   ```

```
-20C
  Temp redeem quotiety: 80
mV
  Load off permit     : Forbid      Load off voltage       :
44.00V
  Battery off permit  : Permit      Battery off voltage    :
43.00V
  AC over alarm volt  : 280V        AC lack alarm voltage :
180V
  DC over alarm volt  : 58 V        DC lack alarm voltage : 45
V
  Load high-temperature-off permit        :
Forbid
  Load high-temperature-off temperature   : 65
C
  Battery high-temperature-off permit     :
Forbid
  Battery high-temperature-off temperature: 53
C

-----------------------------------------------------------------------------
huawei(config-if-power4875l-0)#display power environment parameter


  EMU ID: 1                             Power environment configration
parameter

-----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        50      0        80        -20     C
Current
     1     Humidity           80      10       100       0       %R.H.
Current

-----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     -
1
     4     -                     1     |   5     -
1
     6     -
1
  -----------------------------------------------------------------------------
```

The results show that the power, temperature, and humidity parameters have been configured automatically in the system; however, certain parameters need to be modified, and certain extended monitoring parameters need to be added.

4. Configure the battery charging parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power charge** command.

5. Configure the battery management parameters.

   ```
   huawei(config-if-power4875l-0)#power battery parameter 0.15 60 1 150
   ```

6. Configure the temperature compensation coefficient of the battery.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power battery temperature** command.

7. Configure the power supply load power-off and battery set power-off parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power off** command.

8. Configure the power distribution parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power supply-parameter** command.

9. Configure the rectifier unit parameter.

10. Configure the load and battery high-temperature power-off parameters.

    ```
    huawei(config-if-power4875l-0)#power temperature-off load-off-state forbid
    load-off-temperature 70 battery-off-state permit battery-off-temperature 53
    ```

11. Configure the environment parameters.

    - Configure the temperature parameters.

    ```
    huawei(config-if-power4875l-0)#power environment temperature 68 -5 80 -20
    ```

    - Configure the humidity parameters.

      If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power environment humidity** command.

12. Configure the extended digital parameters.

    ```
    huawei(config-if-power4875l-0)#power outside_digital 3 available-level low-
    level name SPD digital-alarm 20
    huawei(config-if-power4875l-0)#power outside-digital 4 available-level high-
    level name Smoke digital-alarm 15
    huawei(config-if-power4875l-0)#power outside-digital 5 available-level low-
    level name HEX digital-alarm 13
    huawei(config-if-power4875l-0)#power outside-digital 6 available-level low-
    level name MDF-door digital-alarm 9
    ```

13. Query the information about the configured parameters and environment parameters of the power system.

    ```
    huawei(config-if-power4875l-0)#display power system parameter

      EMU ID: 0                             Power system
    information

    ----------------------------------------------------------------------------
      Charge control state: Automatic
    control
      Equalizing voltage  : 56.50V      Floating voltage      :
    53.50V
      Charge Lmt quotiety : 0.15        Equalizing time       : 60
    days
      Battery number      : 1           Battery 0 capacity    : 65
    AH
      Batt_temp_test_upper: 80 C        Batt_temp_test_lower  :
    -20C
      Temp redeem quotiety: 80
    mV
      Load off permit     : Forbid      Load off voltage      :
    44.00V
      Battery off permit  : Permit      Battery off voltage   :
    43.00V
      AC over alarm volt  : 280V        AC lack alarm voltage :
    180V
      DC over alarm volt  : 58 V        DC lack alarm voltage : 45
    V
      Load high-temperature-off permit        :
    Forbid
      Load high-temperature-off temperature   : 70
    C
      Battery high-temperature-off permit     :
    Permit
      Battery high-temperature-off temperature: 53
    C

    ----------------------------------------------------------------------------
    ```

```
huawei(config-if-power4875l-0)#display power environment parameter

  EMU ID: 0                             Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        68      -5       80        -20       C
Current
     1     Humidity           80      10       100       0         %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     SPD
0
     4     Smoke                 1     |   5     Hex
0
     6     MDF-door
0
  ----------------------------------------------------------------------------
```

14. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated.

```
huawei(config-if-power4875l-0)#display power alarm
  EMU ID: 0                             Power alarm
information

----------------------------------------------------------------------------
  Mains supply yes : Yes            Mains supply lack :
Normal
  Total Vol lack   :
Normal
  Load fuse        :
Connect
  Load off         : On             Battery off       :
On
  Battery 0 loop   :
Disconnect
  Module 0         :
Offline
  Module 1         :
Normal
  Module 2         :
Normal
  Module 3         :
Offline
  Module 4         :
Offline
  Door alarm       : Alarm          Water alarm       :
Normal
  Smoke alarm        : Normal         Wiring alarm      :
Normal
  Environment Temperature       : Normal  Environment Humidity       :
Normal

----------------------------------------------------------------------------
  Name                            State |Name
State
  Spare Dig0                      Normal|Spare Dig1
Normal
  Spare Dig2                      Normal|Spare Dig3(SPD)
Normal
  Spare Dig4(Smoke)               Normal|Spare Dig5(HEX)
```

```
Normal
  Spare Dig6(MDF-door)
Normal

---------------------------------------------------------------------------
huawei(config-if-power4875l-0)#quit
```

NOTE

The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable. These two door status sensors are automatically configured by the system. The door status alarm is generated because the door is open.

15. Save the data.
    ```
    huawei(config)#save
    ```
16. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Configuring the Environment Monitoring Parameters of the GEPS4845

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

Mapping Between Monitoring Parameters and Device Ports

Table 1-30 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-30 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

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

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

NOTE

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

Data Plan

In this topic, the application in the F01D500 cabinet is considered as an example. **Table 1-31** provides the data plan for configuring the monitoring parameters of the GEPS4845.

Table 1-31 Data plan for configuring the monitoring parameters of the GEPS4845

Item	Data Plan for the F01D500 Cabinet	Remarks
EMU	Type: POWER4845	During the configuration of the GEPS4845, the type of the GEPS4845 is selected as **POWER4845**.
	SN: 0	-
	Subnode ID: 0	The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic	This parameter is set according to the actual requirements. automatic: The power system automatically adjusts the charging mode of batteries according to the status of the battery set. equalizing: The battery is charged forcibly so as to quickly compensate for the lost capacity of the battery. floating: The battery adjusts charging/ discharging when it is in saturation. Default: automatic.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Equalized charging voltage of the battery: 56.5 V	This parameter is set according to the actual requirements. When setting the equalized charging voltage of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 56.5 V.
	Float charging voltage of the battery: 53.5 V	This parameter is set according to the actual requirements. When setting the float charging of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 53.5 V.
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	This parameter is set according to the actual requirements. In the normal state, the current of the power supply is not limited. The current-limiting function is enabled when the charging current of the battery set > current-limiting coefficient x nominal capacity of the battery set. Default value: 0.15.
	Interval of battery equalized charging: 60 days	This parameter is set according to the actual requirements. If the continuous float charging duration of the rectifier unit exceeds the preset equalized charging interval, the battery enters the equalized charging state. Default: 60 days.
	Number of battery sets: 1	This parameter is set according to the actual requirements. The number of battery sets can be set to 0 or 1. That is, the system supports up to one battery set. Default value: 1.
	Capacity of the battery set: 150 AH	The battery capacity is configured according to the actual value. The F01D500 cabinet uses the 150 AH or 194 AH batteries. Default: 65 AH.
Temperature compensation parameter of the battery	Upper temperature threshold of the battery set: 60°C	This parameter is set according to the actual requirements. Default: 60°C.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Lower temperature threshold of the battery set: -40°C	This parameter is set according to the actual requirements. Default: -40°C.
	Temperature compensation coefficient of the battery set: 100 mV	This parameter is set according to the actual requirements. The temperature compensation coefficient refers to the variable of the float charging voltage of the battery set when the temperature of the battery set changes by every 1° C. Default: 100 mV.
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery set power-off permission status: permit	This parameter is set according to the actual requirements. Default: permit.
	Load power-off voltage: 43.5 V	This parameter is set according to the actual requirements. Default: 43.5 V.
	Battery set power-off voltage: 43 V	This parameter is set according to the actual requirements. Default: 43 V.
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V	This parameter is set according to the actual requirements. When the AC voltage exceeds the preset overvoltage alarm threshold, the system reports an AC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 280 V.
	AC undervoltage alarm threshold of the power supply: 180 V	This parameter is set according to the actual requirements. When the AC voltage falls below the preset undervoltage alarm threshold, the system reports an AC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 180 V.

Item	Data Plan for the F01D500 Cabinet	Remarks
	DC overvoltage alarm threshold of the power supply: 58 V	This parameter is set according to the actual requirements. When the DC voltage exceeds the preset overvoltage alarm threshold, the system reports a DC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 58 V.
	DC undervoltage alarm threshold of the power supply: 45 V	This parameter is set according to the actual requirements. When the DC voltage falls below the preset undervoltage alarm threshold, the system reports a DC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 45 V.
Rectifier unit parameter	The number of the power rectifier modules:3	This parameter is set according to the actual requirements.the GEPS4845 supports up to 3 rectifier modules. Default:0
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery high-temperature power-off permission status: permit	This parameter is set according to the actual requirements. Default: forbid.
	Temperature for load high-temperature power-off: 70°C	This parameter is set according to the actual requirements. Default: 65°C.
	Temperature for battery high-temperature power-off: 53°C	This parameter is set according to the actual requirements. Default: 50°C.
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	This parameter is set according to the actual requirements. When the actual temperature reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 40°C.
	Lower alarm threshold of the temperature: -5°C	This parameter is set according to the actual requirements. When the actual temperature is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 0°C.

Item	Data Plan for the F01D500 Cabinet	Remarks
	Upper alarm threshold of the humidity: 80% RH	This parameter is set according to the actual requirements. When the actual humidity reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 80% RH.
	Lower alarm threshold of the humidity: 10% RH	This parameter is set according to the actual requirements. When the actual humidity is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 10% RH.
External extended digital parameters	Digital parameter ID: 0	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm.
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm.
	Valid level of digital parameter 1: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm.
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.

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

Configuration Process

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

Figure 1-51 shows the configuration process, and **Table 1-32** lists the commands used during the configuration.

Figure 1-51 Configuration process of the GEPS4845

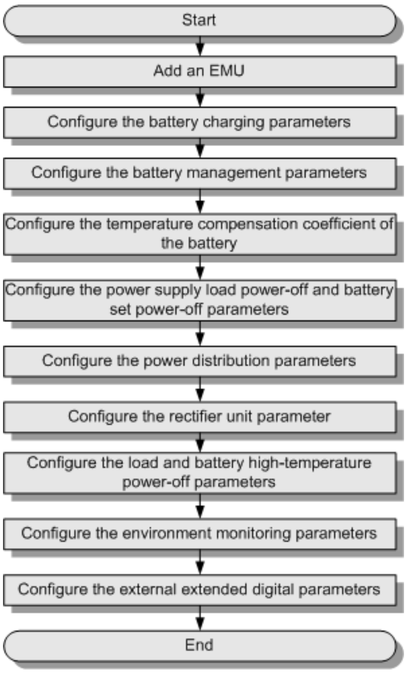

Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the rectifier unit parameter
Configure the load and battery high-temperature power-off parameters
Configure the environment monitoring parameters
Configure the external extended digital parameters
End

Table 1-32 Commands for configuring the GEPS4845

To...	Run the Command...
Add an EMU	**emu add**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**
Configure the temperature compensation coefficient of the battery	**power battery temperature**
Configure the power supply load power-off and battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the rectifier unit parameter	**power module-num**
Configure the load and battery high-temperature power-off parameters	**power temperature-off**

To...	Run the Command...
Configure the environment monitoring parameters	**power environment**
Configure the external extended digital parameters	**power outside-digital**
Query the configuration parameters of the power system	**display power system parameter**

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

1. Log in to the device through the maintenance terminal and add an EMU.

   ```
   huawei(config)#emu add 0 POWER4845 0 0 power4845
   ```

2. Query the status of the GEPS4845.

   ```
   huawei(config)#display emu 0
   --------------------------------------------------------------------
     EMU name    : power4845
     EMU type    : Pwr4845
     Used or not : Used
     EMU state   : Normal
     Frame ID    : 0
     Subnode     : 0

   --------------------------------------------------------------------
   ```

3. Enter the environment monitoring configuration mode and query the default configuration.

   ```
   huawei(config)#interface emu 0
   huawei(config-if-power4845-0)#display power system parameter

     EMU ID: 0                             Power system
   information

   ----------------------------------------------------------------------------
     Charge control state: Automatic
   control
     Equalizing voltage  : 56.50V      Floating voltage      :
   53.50V
     Charge Lmt quotiety : 0.15        Equalizing time       : 60
   days
     Battery number      : 1           Battery 0 capacity    : 65
   AH
     Battery temperature test upper: 60 C  Battery temperature test lower:
   -40C
     Temp redeem quotiety: 100
   mV
     Load off permit     : Forbid      Load off voltage      :
   43.50V
     Battery off permit  : Permit      Battery off voltage   :
   43.00V
     AC over alarm volt  : 280V        AC lack alarm voltage :
   180V
     DC over alarm volt  : 58 V        DC lack alarm voltage : 45
   V
     Power module number :
   3
     Module 0  address   : 1           Module 0  control state:
   On
     Module 1  address   : 2           Module 1  control state:
   On
   ```

```
  Module 2  address   : 3           Module 2  control state:
On
  Load high-temperature-off permit        :
Forbid
  Load high-temperature-off temperature   : 65
C
  Battery high-temperature-off permit     :
Forbid
  Battery high-temperature-off temperature: 50
C

----------------------------------------------------------------------------

huawei(config-if-power4845-0)#display power environment parameter

  EMU ID: 0                             Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        40      0        55        -5      C
Current
     1     Humidity           80      10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     -
1
     4     -                     1     |   5     -
1
     6     -
1

----------------------------------------------------------------------------
```

The results show that the power, temperature, and humidity parameters have been configured automatically in the system; however, certain parameters need to be modified, and certain extended monitoring parameters need to be added.

4. Configure the battery charging parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power charge** command.

5. Configure the battery management parameters.

   ```
   huawei(config-if-power4845-0)#power battery parameter 0.15 60 1 150
   ```

6. Configure the temperature compensation coefficient of the battery.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power battery temperature** command.

7. Configure the power supply load power-off and battery set power-off parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power off** command.

8. Configure the power distribution parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power supply-parameter** command.

9. Configure the rectifier unit parameter.

10. Configure the load and battery high-temperature power-off parameters.

```
huawei(config-if-power4845-0)#power temperature-off load-off-state forbid
load-off-temperature 70 battery-off-state permit battery-off-temperature 53
```

11. Configure the environment parameters.
   - Configure the temperature parameters.

   ```
   huawei(config-if-power4845-0)#power environment temperature 68 -5 60 -40
   ```

   - Configure the humidity parameters.

     If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power environment humidity** command.
12. Configure the extended digital parameters.

   ```
   huawei(config-if-power4845-0)#power outside-digital 3 available-level low-
   level name SPD digital-alarm 20
   huawei(config-if-power4845-0)#power outside-digital 4 available-level high-
   level name Smoke digital-alarm 15
   huawei(config-if-power4845-0)#power outside-digital 5 available-level low-
   level name HEX digital-alarm 13
   huawei(config-if-power4845-0)#power outside-digital 6 available-level low-
   level name MDF-door digital-alarm 9
   ```

13. Query the information about the configured parameters and environment parameters of the power system.

   ```
   huawei(config-if-power4845-0)#display power system parameter

     EMU ID: 0                             Power system
   information

   ----------------------------------------------------------------------------
     Charge control state: Automatic
   control
     Equalizing voltage  : 56.50V      Floating voltage      :
   53.50V
     Charge Lmt quotiety : 0.15        Equalizing time       : 60
   days
     Battery number      : 1           Battery 0 capacity    : 150
   AH
     Battery temperature test upper: 60 C  Battery temperature test lower:
   -40C
     Temp redeem quotiety: 100
   mV
     Load off permit     : Forbid      Load off voltage      :
   43.50V
     Battery off permit  : Permit      Battery off voltage   :
   43.00V
     AC over alarm volt  : 280V        AC lack alarm voltage :
   180V
     DC over alarm volt  : 58 V        DC lack alarm voltage : 45
   V
     Power module number :
   3
     Module 0  address   : 1           Module 0  control state:
   On
     Module 1  address   : 2           Module 1  control state:
   On
     Module 2  address   : 3           Module 2  control state:
   On
     Load high-temperature-off permit        :
   Forbid
     Load high-temperature-off temperature   : 65
   C
     Battery high-temperature-off permit     :
   Forbid
     Battery high-temperature-off temperature: 50
   C

   ----------------------------------------------------------------------------
   ```

```
huawei(config-if-power4845-0)#display power environment parameter

  EMU ID: 0                             Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        40      0        55        -5      C
Current
     1     Humidity           80      10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     SPD
0
     4     Smoke                 1     |   5     HEX
0
     6     MDF-door
0

----------------------------------------------------------------------------
```

14. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated.

```
huawei(config-if-power4845-0)#display power alarm
  EMU ID: 0                             Power alarm
information

----------------------------------------------------------------------------
  AC supply yes : Yes               AC supply lack : Normal
  DC Vol lack   : Normal
  Load fuse        : Connect        Second fuse       :
Connect
  Battery-high-temperature-off : Off   Battery-lack-voltage-off :
On
  Battery loop     :
Connect
  Module 0         :
Normal
  Module 1         :
Normal
  Module 2         :
Normal
  Door alarm       : Alarm          Water alarm       :
Normal
  Smoke alarm      : Normal         Wiring alarm      :
Normal
  Environment Temperature       : Normal  Environment Humidity       :
Normal
  Battery 1 Temp-Sensor         : Invalid Environment 1 Temp-Sensor  :
Invalid
  Environment Humidity-Sensor   :
Invalid

----------------------------------------------------------------------------
  Name                            State |Name
State
  Spare Dig0                      Normal|Spare Dig1
Normal
  Spare Dig2                      Normal|Spare Dig3(SPD)
Normal
  Spare Dig4(Smoke)               Normal|Spare Dig5(HEX)
Normal
  Spare Dig6(MDF-door)
```

```
Normal
  ----------------------------------------------------------------------------
```

NOTE

The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable. These two door status sensors are automatically configured by the system. The door status alarm is generated because the door is open.

15. Save the data.
```
huawei(config-if-power4845-0)#quit
huawei(config)#save
```
16. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Configuring the Environment Monitoring Parameters of the ETP4830

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

Mapping Between Monitoring Parameters and Device Ports

Table 1-33 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-33 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

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

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01S300 Cabinet
Wiring alarm	JTP1	MDF
Battery Tem	VBTEM2	Battery temperature sensor
Environment Tem	VTEM2	Environment temperature sensor
Smoke	SMOKE	Smoke sensor

NOTE

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

Data Plan

In this topic, the application in the F01S300 cabinet is considered as an example. **Table 1-34** provides the data plan for configuring the monitoring parameters of the ETP4830.

Table 1-34 Data plan for configuring the monitoring parameters of the ETP4830

Item	Data Plan for the F01S300 Cabinet	Remarks
EMU	Type: SMU	During the configuration of the ETP4830, the type of the ETP4830 is selected as **SMU**.
	SN: 0	-
	Subnode ID: 0	The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic	This parameter is set according to the actual requirements. automatic: The power system automatically adjusts the charging mode of batteries according to the status of the battery set. equalizing: The battery is charged forcibly so as to quickly compensate for the lost capacity of the battery. floating: The battery adjusts charging/ discharging when it is in saturation. Default: automatic.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Equalized charging voltage of the battery: 56.5 V	This parameter is set according to the actual requirements. When setting the equalized charging voltage of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 56.5 V.
	Float charging voltage of the battery: 53.5 V	This parameter is set according to the actual requirements. When setting the float charging of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 53.5 V.
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	This parameter is set according to the actual requirements. In the normal state, the current of the power supply is not limited. The current-limiting function is enabled when the charging current of the battery set > current-limiting coefficient x nominal capacity of the battery set. Default value: 0.15.
	Interval of battery equalized charging: 60 days	This parameter is set according to the actual requirements. If the continuous float charging duration of the rectifier unit exceeds the preset equalized charging interval, the battery enters the equalized charging state. Default: 60 days.
	Number of battery sets: 1	This parameter is set according to the actual requirements. The number of battery sets can be set to 0 or 1. That is, the system supports up to one battery set. Default value: 1.
	Capacity of the battery set: 150 AH	The battery capacity is configured according to the actual value. The F01S300 cabinet uses the 50 AH or 92 AH batteries Default: 65 AH.
Temperature compensatio n parameter of the battery	Upper temperature threshold of the battery set: 80°C	This parameter is set according to the actual requirements. Default: 80°C.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Lower temperature threshold of the battery set: -20°C	This parameter is set according to the actual requirements. Default: -20°C.
	Temperature compensation coefficient of the battery set: 80 mV	This parameter is set according to the actual requirements. The temperature compensation coefficient refers to the variable of the float charging voltage of the battery set when the temperature of the battery set changes by every 1° C. Default: 80 mV.
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	This parameter is set according to the actual requirements. When the actual temperature reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 50°C.
	Lower alarm threshold of the temperature: -5°C	This parameter is set according to the actual requirements. When the actual temperature is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 0°C.
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery set power-off permission status: permit	This parameter is set according to the actual requirements. Default: permit.
	Load power-off voltage: 44 V	This parameter is set according to the actual requirements. Default: 44 V.
	Battery set power-off voltage: 43 V	This parameter is set according to the actual requirements. Default: 43 V.
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V	This parameter is set according to the actual requirements. When the AC voltage exceeds the preset overvoltage alarm threshold, the system reports an AC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 280 V.

Item	Data Plan for the F01S300 Cabinet	Remarks
	AC undervoltage alarm threshold of the power supply: 180 V	This parameter is set according to the actual requirements. When the AC voltage falls below the preset undervoltage alarm threshold, the system reports an AC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 180 V.
	DC overvoltage alarm threshold of the power supply: 58 V	This parameter is set according to the actual requirements. When the DC voltage exceeds the preset overvoltage alarm threshold, the system reports a DC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 58 V.
	DC undervoltage alarm threshold of the power supply: 45 V	This parameter is set according to the actual requirements. When the DC voltage falls below the preset undervoltage alarm threshold, the system reports a DC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 45 V.
Rectifier unit parameter	The number of the power rectifier modules:0	This parameter is set according to the actual requirements.the ETP4830 supports up to 5 rectifier modules. Default:0
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery high-temperature power-off permission status: permit	This parameter is set according to the actual requirements. Default: forbid.
	Temperature for load high-temperature power-off: 70°C	This parameter is set according to the actual requirements. Default: 65°C.
	Temperature for battery high-temperature power-off: 53°C	This parameter is set according to the actual requirements. Default: 53°C.
External extended digital parameters	Digital parameter ID: 0	This digital parameter is set according to the actual requirements.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 1: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm.
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 4	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 4: high level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 5	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm.
	Valid level of digital parameter 5: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6	This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Valid level of digital parameter 6: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the ETP4830 is configured correctly in the system.

Figure 1-52 shows the configuration process, and **Table 1-35** lists the commands used during the configuration.

Figure 1-52 Configuration process of the ETP4830

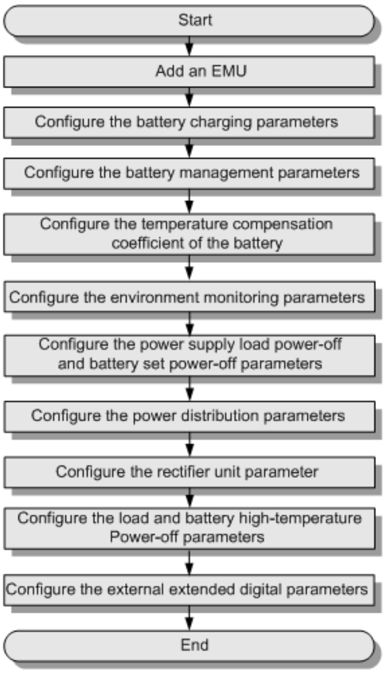

Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the environment monitoring parameters
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the rectifier unit parameter
Configure the load and battery high-temperature Power-off parameters
Configure the external extended digital parameters
End

Table 1-35 Commands for configuring the ETP4830

To...	Run the Command...
Add an EMU	**emu add**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**

To...	Run the Command...
Configure the temperature compensation coefficient of the battery	**power battery temperature**
Configure the environment monitoring parameters	**power environment**
Configure the power supply load power-off and battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the rectifier unit parameter	**power module-num**
Configure the load and battery high-temperature power-off parameters	**power temperature-off**
Configure the external extended digital parameters	**power outside-digital**
Query the configuration parameters of the power system	**display power system parameter**

The following considers the configuration in the F01S300 cabinet as an example to describe the process of configuring the environment monitoring parameters of the ETP4830.

1. Log in to the device through the maintenance terminal and add an EMU.

   ```
   huawei(config)#emu add 0 SMU 0 0 smu
   ```

2. Query the status of the smu.

   ```
   huawei(config)#display emu 0
   ---------------------------------------------------------------------
     EMU name    : smu
     EMU type    : SMU
     Used or not : Used
     EMU state   : Normal
     Frame ID    : 0
     Subnode     : 0

   ---------------------------------------------------------------------
   ```

3. Enter the environment monitoring configuration mode and query the default configuration.

   ```
   huawei(config)#interface emu 0
   huawei(config-if-smu-0)#display power system parameter

     EMU ID: 0                             Power system
   information

   -----------------------------------------------------------------------------
     Charge control state: Automatic
   control
     Equalizing voltage  : 56.50V      Floating voltage      :
   53.50V
     Charge Lmt quotiety : 0.15        Equalizing time       : 60
   ```

```
days
  Battery number      : 1           Battery 0 capacity    : 65
AH
  Battery temperature test upper :  80C  Battery temperature test lower:
-20C
  Temperature redeem quotiety    :
80mV
  Battery temperature alarm upper:  50C  Battery temperature alarm lower:
0C
  Load off permit     : Forbid      Load off voltage      :
44.00V
  Battery off permit  : Permit      Battery off voltage   :
43.00V
  AC over alarm volt  : 280V        AC lack alarm voltage :
180V
  DC over alarm volt  : 58 V        DC lack alarm voltage : 45
V
  Power module number :
0
  Load high-temperature-off permit        :
Forbid
  Load high-temperature-off temperature   : 65
C
  Battery high-temperature-off permit     :
Forbid
  Battery high-temperature-off temperature: 53
C

----------------------------------------------------------------------------

huawei(config-if-smu-0)#display power environment parameter

  EMU ID: 0                            Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        50       0        80        -20     C
Current
     1     Humidity           80       10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level    |DigitalID Name
Level
     0     -                     1      |   1     -
1
     2     -                     1      |   3     -
1
     4     -                     1      |   5     -
1
     6     -
1

----------------------------------------------------------------------------
```

The results show that the power, temperature, and humidity parameters have been configured automatically in the system; however, certain parameters need to be modified, and certain extended monitoring parameters need to be added.

4. Configure the battery charging parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power charge** command.

5. Configure the battery management parameters.

   ```
   huawei(config-if-smu-0)#power battery parameter 0.15 60 1 150
   ```

6. Configure the temperature compensation coefficient of the battery.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power battery temperature** command.

7. Configure the environment temperature parameters.

   ```
   huawei(config-if-smu-0)#power environment temperature 68 -5 80 -20
   ```

8. Configure the power supply load power-off and battery set power-off parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power off** command.

9. Configure the power distribution parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power supply-parameter** command.

10. Configure the rectifier unit parameter.

    If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power module-num** command.

11. Configure the load and battery high-temperature power-off parameters.

    ```
    huawei(config-if-smu-0)#power temperature-off load-off-state forbid load-off-
    temperature 70 battery-off-state permit battery-off-temperature 53
    ```

12. Configure the extended digital parameters.

    ```
    huawei(config-if-smu-0)#power outside-digital 3 available-level low-level name
    SPD digital-alarm 20
    huawei(config-if-smu-0)#power outside-digital 5 available-level low-level name
    HEX digital-alarm 13
    huawei(config-if-smu-0)#power outside-digital 6 available-level low-level name
    MDF-door digital-alarm 9
    ```

13. Query the information about the configured parameters and environment parameters of the power system.

    ```
    huawei(config-if-smu-0)#display power system parameter

      EMU ID: 0                           Power system
    information

    ----------------------------------------------------------------------------
      Charge control state: Automatic
    control
      Equalizing voltage  : 56.50V      Floating voltage      :
    53.50V
      Charge Lmt quotiety : 0.15        Equalizing time       : 60
    days
      Battery number      : 1           Battery 0 capacity    : 150
    AH
      Battery temperature test upper :  80C  Battery temperature test lower:
    -20C
      Temperature redeem quotiety    :
    80mV
      Battery temperature alarm upper:  50C  Battery temperature alarm lower:
    0C
      Load off permit     : Forbid      Load off voltage      :
    44.00V
      Battery off permit  : Permit      Battery off voltage   :
    43.00V
      AC over alarm volt  : 280V        AC lack alarm voltage :
    180V
      DC over alarm volt  : 58 V        DC lack alarm voltage : 45
    V
      Power module number :
    0
      Load high-temperature-off permit        :
    Forbid
    ```

```
  Load high-temperature-off temperature   : 70
C
  Battery high-temperature-off permit     :
Permit
  Battery high-temperature-off temperature: 53
C

----------------------------------------------------------------------------

huawei(config-if-smu-0)#display power environment parameter

  EMU ID: 0                             Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        68      -5       80        -20     C
Current
     1     Humidity           80      10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     SPD
0
     4     -                     1     |   5     HEX
0
     6     MDF-door
0

----------------------------------------------------------------------------
```

14. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated.

```
huawei(config-if-smu-0)#display power alarm

  EMU ID: 0                             Power alarm information
  ----------------------------------------------------------------------------
  Mains supply yes : Yes            Mains supply lack : Normal
  Total Vol lack   : Normal
  Load fuse        : Connect
  Load off         : On             Battery off       : On
  Battery loop   : Connect
  Module 0         : Normal
  Module 1         : Normal
  Module 2         : Normal
  Module 3         : Normal
  Module 4         : Normal
  Door alarm       : Alarm          Water alarm       : Normal
  Smoke alarm      : Normal         Wiring alarm      : Normal
  Environment Temperature       : Normal  Environment Humidity       :
Normal
  Battery Dectect  :
Normal

----------------------------------------------------------------------------
  Name                            State |Name
State
  Spare Dig0                      Normal|Spare Dig1
Normal
  Spare Dig2                      Normal|Spare Dig3(SPD)
Normal
  Spare Dig4                      Normal|Spare Dig5(HEX)
Normal
  Spare Dig6(MDF-door)
```

```
Normal
----------------------------------------------------------------------------
```

NOTE

The door status alarm is generated because the door is open.

15. Save the data.

```
huawei(config-if-smu-0)#quit
huawei(config)#save
```

16. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Configuring the Environment Monitoring Parameters of the ETP4890

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

Mapping Between Monitoring Parameters and Device Ports

Table 1-36 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

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

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01D500 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 2	JTD3	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 3	JTD4	surge protector (SPD)
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 5	JTD6	Heat exchanger
Digital 6	JTD7	Door status sensor of the MDF compartment
Door alarm	JTM1	Door status sensors of the device compartment and heat exchanger compartment
Wiring alarm	JTP1	MDF

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01D500 Cabinet
Battery Tem	VBTEM2	Battery temperature sensor
Environment Tem	VTEM2	Environment temperature sensor
Smoke	SMOKE	Smoke sensor

NOTE

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

Data Plan

In this topic, the application in the F01D500 cabinet is considered as an example. **Table 1-37** provides the data plan for configuring the monitoring parameters of the ETP4890.

Table 1-37 Data plan for configuring the monitoring parameters of the ETP4890

Item	Data Plan for the F01S300 Cabinet	Remarks
EMU	Type: SMU	During the configuration of the ETP4890, the type of the ETP4890 is selected as **SMU**.
	SN: 0	-
	Subnode ID: 0	The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic	This parameter is set according to the actual requirements. automatic: The power system automatically adjusts the charging mode of batteries according to the status of the battery set. equalizing: The battery is charged forcibly so as to quickly compensate for the lost capacity of the battery. floating: The battery adjusts charging/ discharging when it is in saturation. Default: automatic.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Equalized charging voltage of the battery: 56.5 V	This parameter is set according to the actual requirements. When setting the equalized charging voltage of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 56.5 V.
	Float charging voltage of the battery: 53.5 V	This parameter is set according to the actual requirements. When setting the float charging of the battery, make sure that DC overvoltage - 1 V > equalized charging voltage > float charging voltage + 2 V, and that DC undervoltage > load power-off voltage > battery power-off voltage. Default: 53.5 V.
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	This parameter is set according to the actual requirements. In the normal state, the current of the power supply is not limited. The current-limiting function is enabled when the charging current of the battery set > current-limiting coefficient x nominal capacity of the battery set. Default value: 0.15.
	Interval of battery equalized charging: 60 days	This parameter is set according to the actual requirements. If the continuous float charging duration of the rectifier unit exceeds the preset equalized charging interval, the battery enters the equalized charging state. Default: 60 days.
	Number of battery sets: 1	This parameter is set according to the actual requirements. The number of battery sets can be set to 0 or 1. That is, the system supports up to one battery set. Default value: 1.
	Capacity of the battery set: 150 AH	The battery capacity is configured according to the actual value. The F01S300 cabinet uses the 50 AH or 92 AH batteries Default: 65 AH.
Temperature compensation parameter of the battery	Upper temperature threshold of the battery set: 80°C	This parameter is set according to the actual requirements. Default: 80°C.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Lower temperature threshold of the battery set: -20°C	This parameter is set according to the actual requirements. Default: -20°C.
	Temperature compensation coefficient of the battery set: 80 mV	This parameter is set according to the actual requirements. The temperature compensation coefficient refers to the variable of the float charging voltage of the battery set when the temperature of the battery set changes by every 1° C. Default: 80 mV.
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	This parameter is set according to the actual requirements. When the actual temperature reaches or is higher than the upper alarm threshold, the system reports an alarm. Default: 50°C.
	Lower alarm threshold of the temperature: -5°C	This parameter is set according to the actual requirements. When the actual temperature is equal to or lower than the lower alarm threshold, the system reports an alarm. Default: 0°C.
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery set power-off permission status: permit	This parameter is set according to the actual requirements. Default: permit.
	Load power-off voltage: 44 V	This parameter is set according to the actual requirements. Default: 44 V.
	Battery set power-off voltage: 43 V	This parameter is set according to the actual requirements. Default: 43 V.
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V	This parameter is set according to the actual requirements. When the AC voltage exceeds the preset overvoltage alarm threshold, the system reports an AC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 280 V.

Item	Data Plan for the F01S300 Cabinet	Remarks
	AC undervoltage alarm threshold of the power supply: 180 V	This parameter is set according to the actual requirements. When the AC voltage falls below the preset undervoltage alarm threshold, the system reports an AC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 180 V.
	DC overvoltage alarm threshold of the power supply: 58 V	This parameter is set according to the actual requirements. When the DC voltage exceeds the preset overvoltage alarm threshold, the system reports a DC overvoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 58 V.
	DC undervoltage alarm threshold of the power supply: 45 V	This parameter is set according to the actual requirements. When the DC voltage falls below the preset undervoltage alarm threshold, the system reports a DC undervoltage alarm. In this case, the rectifier unit powers off automatically to protect the system. Default: 45 V.
Rectifier unit parameter	The number of the power rectifier modules:0	This parameter is set according to the actual requirements.the ETP4890 supports up to 5 rectifier modules. Default:0
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid	This parameter is set according to the actual requirements. Default: forbid.
	Battery high-temperature power-off permission status: permit	This parameter is set according to the actual requirements. Default: forbid.
	Temperature for load high-temperature power-off: 70°C	This parameter is set according to the actual requirements. Default: 65°C.
	Temperature for battery high-temperature power-off: 53°C	This parameter is set according to the actual requirements. Default: 53°C.
External extended digital parameters	Digital parameter ID: 0	This digital parameter is set according to the actual requirements.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 1: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm.
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 4	This digital parameter is set according to the actual requirements.
	Valid level of digital parameter 4: high level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 5	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm.
	Valid level of digital parameter 5: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6	This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm.

Item	Data Plan for the F01S300 Cabinet	Remarks
	Valid level of digital parameter 6: low level	When the low level represents the valid level, the host does not report an alarm in the case of low level.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the ETP4890 is configured correctly in the system.

Figure 1-53 shows the configuration process, and Table 1-38 lists the commands used during the configuration.

Figure 1-53 Configuration process of the ETP4890

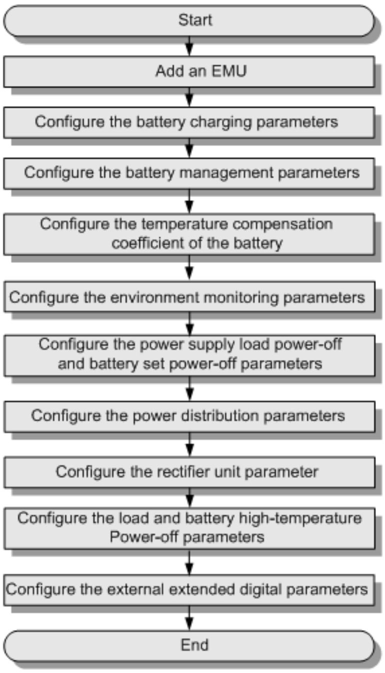

Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the environment monitoring parameters
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the rectifier unit parameter
Configure the load and battery high-temperature Power-off parameters
Configure the external extended digital parameters
End

Table 1-38 Commands for configuring the ETP4890

To...	Run the Command...
Add an EMU	**emu add**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**

To...	Run the Command...
Configure the temperature compensation coefficient of the battery	**power battery temperature**
Configure the environment monitoring parameters	**power environment**
Configure the power supply load power-off and battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the rectifier unit parameter	**power module-num**
Configure the load and battery high-temperature power-off parameters	**power temperature-off**
Configure the external extended digital parameters	**power outside-digital**
Query the configuration parameters of the power system	**display power system parameter**

The following considers the configuration in the F01D500 cabinet as an example to describe the process of configuring the environment monitoring parameters of the ETP4890.

1. Log in to the device through the maintenance terminal and add an EMU.

```
huawei(config)#emu add 0 SMU 0 0 smu
```

2. Query the status of the smu.

```
huawei(config)#display emu 0
--------------------------------------------------------------------
  EMU name    : smu
  EMU type    : SMU
  Used or not : Used
  EMU state   : Normal
  Frame ID    : 0
  Subnode     : 0

--------------------------------------------------------------------
```

3. Enter the environment monitoring configuration mode and query the default configuration.

```
huawei(config)#interface emu 0
huawei(config-if-smu-0)#display power system parameter

  EMU ID: 0                             Power system
information

----------------------------------------------------------------------------
  Charge control state: Automatic
control
  Equalizing voltage  : 56.50V      Floating voltage      :
53.50V
  Charge Lmt quotiety : 0.15        Equalizing time       : 60
```

```
days
  Battery number      : 1           Battery 0 capacity    : 65
AH
  Battery temperature test upper :  80C  Battery temperature test lower:
-20C
  Temperature redeem quotiety    :
80mV
  Battery temperature alarm upper:  50C  Battery temperature alarm lower:
0C
  Load off permit     : Forbid      Load off voltage      :
44.00V
  Battery off permit  : Permit      Battery off voltage   :
43.00V
  AC over alarm volt  : 280V        AC lack alarm voltage :
180V
  DC over alarm volt  : 58 V        DC lack alarm voltage : 45
V
  Power module number :
0
  Load high-temperature-off permit        :
Forbid
  Load high-temperature-off temperature   : 65
C
  Battery high-temperature-off permit     :
Forbid
  Battery high-temperature-off temperature: 53
C

----------------------------------------------------------------------------

huawei(config-if-smu-0)#display power environment parameter

  EMU ID: 0                            Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        50       0        80        -20     C
Current
     1     Humidity           80       10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     -
1
     4     -                     1     |   5     -
1
     6     -
1

----------------------------------------------------------------------------
```

The results show that the power, temperature, and humidity parameters have been configured automatically in the system; however, certain parameters need to be modified, and certain extended monitoring parameters need to be added.

4. Configure the battery charging parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power charge** command.

5. Configure the battery management parameters.

   ```
   huawei(config-if-smu-0)#power battery parameter 0.15 60 1 150
   ```

6. Configure the temperature compensation coefficient of the battery.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power battery temperature** command.

7. Configure the environment temperature parameters.

   ```
   huawei(config-if-smu-0)#power environment temperature 68 -5 80 -20
   ```

8. Configure the power supply load power-off and battery set power-off parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power off** command.

9. Configure the power distribution parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power supply-parameter** command.

10. Configure the rectifier unit parameter.

    If the planned data is the same as the query result, the parameters need not be configured. If the parameters need to be modified, run the **power module-num** command.

11. Configure the load and battery high-temperature power-off parameters.

    ```
    huawei(config-if-smu-0)#power temperature-off load-off-state forbid load-off-
    temperature 70 battery-off-state permit battery-off-temperature 53
    ```

12. Configure the extended digital parameters.

    ```
    huawei(config-if-smu-0)#power outside-digital 3 available-level low-level name
    SPD digital-alarm 20
    huawei(config-if-smu-0)#power outside-digital 5 available-level low-level name
    HEX digital-alarm 13
    huawei(config-if-smu-0)#power outside-digital 6 available-level low-level name
    MDF-door digital-alarm 9
    ```

13. Query the information about the configured parameters and environment parameters of the power system.

    ```
    huawei(config-if-smu-0)#display power system parameter

      EMU ID: 0                           Power system
    information

    ---------------------------------------------------------------------------
      Charge control state: Automatic
    control
      Equalizing voltage  : 56.50V      Floating voltage      :
    53.50V
      Charge Lmt quotiety : 0.15        Equalizing time       : 60
    days
      Battery number      : 1           Battery 0 capacity    : 150
    AH
      Battery temperature test upper :  80C  Battery temperature test lower:
    -20C
      Temperature redeem quotiety    :
    80mV
      Battery temperature alarm upper:  50C  Battery temperature alarm lower:
    0C
      Load off permit     : Forbid      Load off voltage      :
    44.00V
      Battery off permit  : Permit      Battery off voltage   :
    43.00V
      AC over alarm volt  : 280V        AC lack alarm voltage :
    180V
      DC over alarm volt  : 58 V        DC lack alarm voltage : 45
    V
      Power module number :
    0
      Load high-temperature-off permit        :
    Forbid
    ```

```
  Load high-temperature-off temperature   : 70
C
  Battery high-temperature-off permit     :
Permit
  Battery high-temperature-off temperature: 53
C

----------------------------------------------------------------------------

huawei(config-if-smu-0)#display power environment parameter

  EMU ID: 0                            Power environment configration
parameter

----------------------------------------------------------------------------
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit
Type
     0     Temperature        68      -5       80        -20     C
Current
     1     Humidity           80      10       100       0       %R.H.
Current

----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name
Level
     0     -                     1     |   1     -
1
     2     -                     1     |   3     SPD
0
     4     -                     1     |   5     HEX
0
     6     MDF-door
0

----------------------------------------------------------------------------
```

14. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated.

```
huawei(config-if-smu-0)#display power alarm

  EMU ID: 0                            Power alarm information
  ----------------------------------------------------------------------------
  Mains supply yes : Yes            Mains supply lack : Normal
  Total Vol lack   : Normal
  Load fuse        : Connect
  Load off         : On             Battery off       : On
  Battery loop   : Connect
  Module 0         : Normal
  Module 1         : Normal
  Module 2         : Normal
  Module 3         : Normal
  Module 4         : Normal
  Door alarm       : Alarm          Water alarm       : Normal
  Smoke alarm      : Normal         Wiring alarm      : Normal
  Environment Temperature       : Normal  Environment Humidity       :
Normal
  Battery Dectect  :
Normal

----------------------------------------------------------------------------
  Name                           State |Name
State
  Spare Dig0                     Normal|Spare Dig1
Normal
  Spare Dig2                     Normal|Spare Dig3(SPD)
Normal
  Spare Dig4                     Normal|Spare Dig5(HEX)
Normal
  Spare Dig6(MDF-door)
```

```
Normal
-----------------------------------------------------------------------------
```

NOTE

The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable. These two door status sensors are automatically configured by the system. The door status alarm is generated because the door is open.

15. Save the data.
```
huawei(config-if-smu-0)#quit
huawei(config)#save
```
16. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Configuring the Power3000 Environment Monitoring Mode

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

Data Plan

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

Table 1-39 Data plan for configuring Power3000 monitoring parameters

Configuration Item	Data Plan	Remarks
EMU	Type: POWER3000	During the configuration, the type of the Power3000 is set to POWER3000.
	Number: 0	-
	Subnode ID: 0	The subnode ID must be the same as the subnode setting of the corresponding DIP switch on the EMU, but must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic	This parameter is set according to actual requirements. automatic: The power system automatically adjusts the charging mode of the battery according to the status of the battery set. equalizing: The battery is charged forcibly to quickly compensate for the lost capacity of the battery. floating: The battery adjusts charging/ discharging according to its capacity status. Default: automatic

Configuration Item	Data Plan	Remarks
	Equalized charging voltage of the battery: 56.5 V	This parameter is set according to actual requirements. When setting the equalized charging voltage of the battery, ensure that (DC overvoltage - 1 V) > Equalized charging voltage > Floating charging voltage > (DC undervoltage + 2 V), and that DC undervoltage > Load power-off voltage > Battery power-off voltage. Default: 56.5 V
	Floating charging voltage of the battery: 53.5 V	This parameter is set according to actual requirements. When setting the floating charging voltage of the battery, ensure that (DC overvoltage - 1 V) > Equalized charging voltage > Floating charging voltage > (DC undervoltage + 2 V), and that DC undervoltage > Load power-off voltage > Battery power-off voltage. Default: 53.5 V
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	This parameter is set according to actual requirements. In the normal state, the current of the power supply is not limited. The current-limiting function is enabled when Charging current of the battery set > (Current-limiting coefficient x Nominal capacity of the battery set). Default: 0.15
	Interval of battery equalized charging: 60 days	This parameter is set according to actual requirements. The battery enters the equalized charging state when the continuous floating charging duration of the rectifier module exceeds the preset equalized charging interval. Default: 60 days
	Number of battery sets: 1	This parameter is set according to actual requirements. The number of battery sets can be set to 0 or 1. That is, the system supports a maximum of one battery set. Default: 1
	Capacity of the battery set: 65 AH	The battery capacity is set according to the actual value. Default: 65 AH
Temperature compensation parameters of the battery	Upper temperature threshold of the battery set: 80°C	This parameter is set according to actual requirements. Default: 60°C

Configuration Item	Data Plan	Remarks
	Lower temperature threshold of the battery set: -20°C	This parameter is set according to actual requirements. Default: -40°C
	Temperature compensation coefficient of the battery set: 80 mV	This parameter is set according to actual requirements. The temperature compensation coefficient refers to the variable of the floating charging voltage of the battery set when the temperature of the battery set changes by every 1° C. Default: 100 mV
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid	This parameter is set according to actual requirements. Default: forbid
	Battery set power-off permission status: permit	This parameter is set according to actual requirements. Default: permit
	Load power-off voltage: 43.50 V	This parameter is set according to actual requirements. Default: 43.50 V
	Battery set power-off voltage: 43.00 V	This parameter is set according to actual requirements. Default: 43.00 V
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V	This parameter is set according to actual requirements. When the AC voltage exceeds the preset overvoltage alarm threshold, the system reports an AC overvoltage alarm. In this case, the rectifier module is powered off to protect the system. Default: 280 V
	AC undervoltage alarm threshold of the power supply: 180 V	This parameter is set according to actual requirements. When the AC voltage falls below the preset undervoltage alarm threshold, the system reports an AC undervoltage alarm. In this case, the rectifier module is powered off to protect the system. Default: 180 V

Configuration Item	Data Plan	Remarks
	DC overvoltage alarm threshold of the power supply: 58 V	This parameter is set according to actual requirements. When the DC voltage exceeds the preset overvoltage alarm threshold, the system reports a DC overvoltage alarm. In this case, the rectifier module is powered off to protect the system. Default: 58 V
	DC undervoltage alarm threshold of the power supply: 45 V	This parameter is set according to actual requirements. When the DC voltage falls below the preset undervoltage alarm threshold, the system reports a DC undervoltage alarm. In this case, the rectifier module is powered off to protect the system. Default: 45 V
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid	This parameter is set according to actual requirements. Default: forbid
	Battery high-temperature power-off permission status: permit	This parameter is set according to actual requirements. Default: forbid
	Temperature for load high-temperature power-off: 70°C	This parameter is set according to actual requirements. Default: 65°C
	Temperature for battery high-temperature power-off: 53°C	This parameter is set according to actual requirements. Default: 50°C
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	This parameter is set according to actual requirements. When the actual temperature reaches or exceeds the upper alarm threshold, the system reports an alarm. Default: 40°C
	Lower alarm threshold of the temperature: -5°C	This parameter is set according to actual requirements. When the actual temperature reaches or falls below the lower alarm threshold, the system reports an alarm. Default: 0°C
	Upper alarm threshold of the humidity: 80% RH	This parameter is set according to actual requirements. When the actual humidity reaches or exceeds the upper alarm threshold, the system reports an alarm. Default: 80% RH

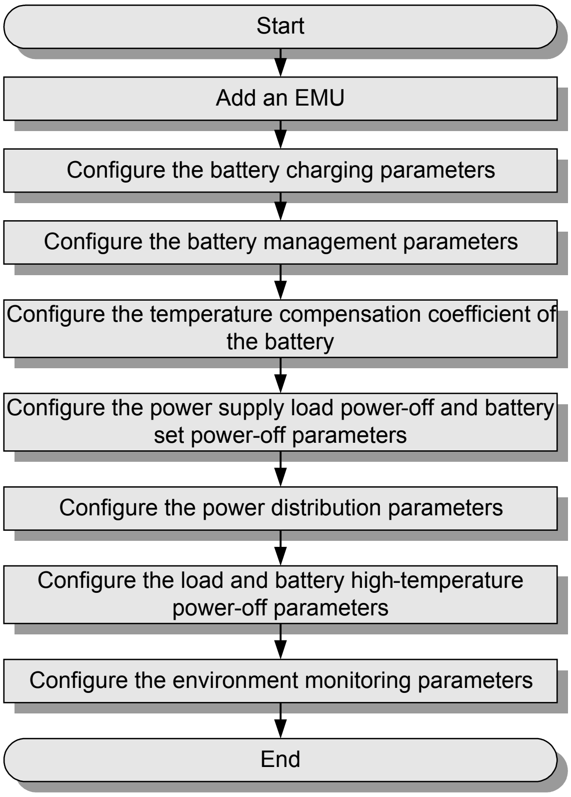
Configuration Item	Data Plan	Remarks
	Lower alarm threshold of the humidity: 10% RH	This parameter is set according to actual requirements. When the actual humidity reaches or falls below the lower alarm threshold, the system reports an alarm. Default: 10% RH
External extended digital parameters	Digital parameter ID: 0, 1, 2, 3, 4, 5 and 6	Digital parameters are set according to actual requirements.

Configuration Process

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

Figure 1-54 shows the configuration process, and **Table 1-40** lists the commands used during the configuration.

Figure 1-54 Configuration process of the Power3000 monitoring module


Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the load and battery high-temperature power-off parameters
Configure the environment monitoring parameters
End

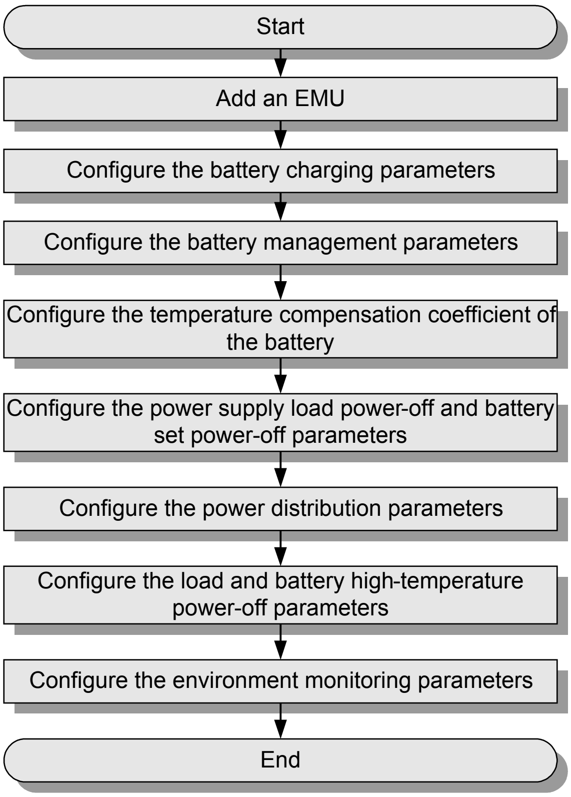

Start
Add an EMU
Configure the battery charging parameters
Configure the battery management parameters
Configure the temperature compensation coefficient of the battery
Configure the power supply load power-off and battery set power-off parameters
Configure the power distribution parameters
Configure the load and battery high-temperature power-off parameters
Configure the environment monitoring parameters
End

Table 1-40 Commands for configuring the Power3000 environment monitoring parameters

To...	Run the Command...
Add an EMU	**emu add**
Configure battery charging parameters	**power charge**
Configure battery management parameters	**power battery parameter**
Configure the temperature compensation coefficient of the battery	**power battery temperature**
Configure power supply load power-off and battery set power-off parameters	**power off**
Configure power distribution parameters	**power supply-parameter**
Configure load and battery high-temperature power-off parameters	**power temperature-off**
Configure environment monitoring parameters	**power environment**

To...	Run the Command...
Configure external extended digital parameters	**power outside-digital**
Query configuration parameters of the power system	**display power system parameter**

The following section describes the process of configuring Power3000 environment monitoring parameters.

1. Log in to the device by using the maintenance terminal and add an EMU.

   ```
   huawei(config)#emu add 0 POWER3000 0 0 POWER3000
   ```

2. Query the status of the Power3000.

   ```
   huawei(config)#display emu 0
   --------------------------------------------------------------------
     EMU name    : POWER3000
     EMU type    : Pwr3000
     Used or not : Used
     EMU state   : Normal
     Frame ID    : 0
     Subnode     : 0
   --------------------------------------------------------------------
   ```

3. Enter the environment monitoring configuration mode and query the default configuration.

   ```
   huawei(config)#interface emu 0
   huawei(config-if-power3000-0)#display power system parameter
     EMU ID: 0                             Power system information
     ----------------------------------------------------------------------------
     Charge control state: Automatic control
     Equalizing voltage  : 56.50V      Floating voltage      : 53.50V
     Charge Lmt quotiety : 0.15        Equalizing time       : 60 days
     Battery number      : 0
     Batt_temp_test_upper: 60 C        Batt_temp_test_lower  : -40C
     Temp redeem quotiety: 100mV
     Load off permit     : Forbid      Load off voltage      : 43.50V
     Battery off permit  : Permit      Battery off voltage   : 43.00V
     Shunt quotiety      : 100A
     AC over alarm volt  : 280V        AC lack alarm voltage : 180V
     DC over alarm volt  : 58 V        DC lack alarm voltage : 45 V
     Power module number : 12
     Module 0 address    : 1           Module 0 control state: On
     Module 1 address    : 2           Module 1 control state: On
     Module 2 address    : 3           Module 2 control state: On
     Module 3 address    : 4           Module 3 control state: On
     Module 4 address    : 5           Module 4 control state: On
     Module 5 address    : 6           Module 5 control state: On
     Module 6 address    : 7           Module 6 control state: On
     Module 7 address    : 8           Module 7 control state: On
     Module 8 address    : 9           Module 8 control state: On
     Module 9 address    : 10          Module 9 control state: On
     Module 10 address    : 11         Module 10 control state: On
     Module 11 address    : 12         Module 11 control state: On
     Load high-temperature-off permit        : Forbid
     Load high-temperature-off temperature   : 65 C
     Battery high-temperature-off permit     : Forbid
     Battery high-temperature-off temperature: 50 C
     ----------------------------------------------------------------------------
   huawei(config-if-power3000-0)#display power environment parameter

     EMU ID: 0                             Power environment configration
   parameter
     ----------------------------------------------------------------------------
   ```

```
  AnalogID Name            AlmUpper AlmLower TestUpper TestLower Unit     Type
     0     Temperature        40      0        55        -5      C
Current
     1     Humidity           80      10       100       0       %R.H.
Current
  ----------------------------------------------------------------------------
  DigitalID Name              Level   |DigitalID Name              Level
     0     -                    1     |   1     -                    1
     2     -                    1     |   3     -                    1
     4     -                    1     |   5     -                    1
     6     -                    1
  ----------------------------------------------------------------------------
```

The results show that the power, temperature, and humidity parameters have been configured automatically in the system; however, some parameters need to be modified, and some extended monitoring parameters need to be added.

4. Configure battery charging parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If modification is needed, run the **power charge** command to configure related parameters.

5. Configure battery management parameters.

   ```
   huawei(config-if-power3000-0)#power battery parameter 0.15 60 1 65
   ```

6. Configure the temperature compensation coefficient of the battery.

   If the planned data is the same as the query result, the parameters need not be configured. If modification is needed, run the **power battery temperature** command to configure related parameters.

7. Configure power supply load power-off and battery set power-off parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If modification is needed, run the **power off** command to configure related parameters.

8. Configure power distribution parameters.

   If the planned data is the same as the query result, the parameters need not be configured. If modification is needed, run the **power supply-parameter** command to configure related parameters.

9. Configure load and battery high-temperature power-off parameters.

   ```
   huawei(config-if-power3000-0)#power temperature-off load-off-state forbid
   load-off-temperature 70 battery-off-state permit battery-off-temperature 53
   ```

10. Configure environment parameters.

    - Configure the temperature.

    ```
    huawei(config-if-power3000-0)#power environment temperature 68 -5 80 -20
    ```

    - Configure the humidity.

      If the planned data is the same as the query result, the humidity need not be configured. If modification is needed, run the **power environment humidity** command to configure the humidity.

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

    ```
    huawei(config-if-power3000-0)#display power system parameter
      EMU ID: 3                             Power system information
      ----------------------------------------------------------------------------
      Charge control state: Automatic control
      Equalizing voltage  : 56.50V      Floating voltage      : 53.50V
      Charge Lmt quotiety : 0.15        Equalizing time       : 60 days
      Battery number      : 1           Battery 0 capacity    : 65  AH
      Batt_temp_test_upper: 60 C        Batt_temp_test_lower  : -40C
      Temp redeem quotiety: 100mV
      Load off permit     : Forbid      Load off voltage      : 43.50V
    ```

```
  Battery off permit  : Permit      Battery off voltage   : 43.00V
  Shunt quotiety      : 100A
  AC over alarm volt  : 280V        AC lack alarm voltage : 180V
  DC over alarm volt  : 58 V        DC lack alarm voltage : 45 V
  Power module number : 12
  Module 0 address    : 1           Module 0 control state: On
  Module 1 address    : 2           Module 1 control state: On
  Module 2 address    : 3           Module 2 control state: On
  Module 3 address    : 4           Module 3 control state: On
  Module 4 address    : 5           Module 4 control state: On
  Module 5 address    : 6           Module 5 control state: On
  Module 6 address    : 7           Module 6 control state: On
  Module 7 address    : 8           Module 7 control state: On
  Module 8 address    : 9           Module 8 control state: On
  Module 9 address    : 10          Module 9 control state: On
  Module 10 address    : 11         Module 10 control state: On
  Module 11 address    : 12         Module 11 control state: On
  Load high-temperature-off permit        : Forbid
  Load high-temperature-off temperature   : 70 C
  Battery high-temperature-off permit     : Permit
  Battery high-temperature-off temperature: 53 C

----------------------------------------------------------------------------
huawei(config-if-power3000-0)#display power environment parameter

  EMU ID: 0                             Power environment configration
parameter
  ----------------------------------------------------------------------------
  AnalogID Name           AlmUpper AlmLower TestUpper TestLower Unit    Type
     0     Temperature       68       -5        80        -20       C
Current
     1     Humidity          80       10        100       0         %R.H.
Current
  ----------------------------------------------------------------------------
  DigitalID Name               Level   |DigitalID Name               Level
     0     -                     1     |   1     -                     1
     2     -                     1     |   3     -                     1
     4     -                     1     |   5     -                     1
     6     -                     1
  ----------------------------------------------------------------------------
huawei(config-if-power3000-0)#quit
```

12. Save the data.

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

Commissioning the EMU_TCU

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

Context

NOTE

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

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

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

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

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

Table 1-41 Default configuration of the TCU

Parameter	Default Value
Sub-node	7

Procedure

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

NOTE

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

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

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

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

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

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

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

----End

Result

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

Example

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

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

huawei(config)#interface emu 2

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

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

  Command:
          tcu heat temperature -10 30
  Send command to environment monitor board ,please waiting for the ack

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

Commissioning the EMU_FAN

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

Context

NOTE

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

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

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

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

Table 1-42 lists the default configuration of the FAN.

Table 1-42 Default configuration of the FAN

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

Procedure

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

NOTE

The FAN communicates with the MA5600T/MA5603T in the master node and sub-node mode. Therefore, the DIP switches of the sub-nodes for the FAN must be consistent with those for the MA5600T/MA5603T. For details about how to configure the DIP switches of the FAN, see the Description of DIP Switches in **Checking the Settings of DIP Switches on the Fan Monitoring Board**.

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

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

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

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

NOTE

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

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

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

----End

Result

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

Example

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

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

huawei(config)#interface emu 0

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

  EMU ID: 0
  FAN configration parameter:
  ----------------------------------------------------------------------------
  FAN timing mode: Auto timing by temperature
  ----------------------------------------------------------------------------
  Alarm_name                        Permit/Forbid
  Read temperature fault                Permit
  Fan block                             Permit
  Temperature high                      Permit
  Power fault                           Permit
  ----------------------------------------------------------------------------
```

1.3.17 Saving and Backing Up Data

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

Manually Saving and Backing Up Data

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

Prerequisites

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

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

NOTE

You need to configure only one of the above-mentioned three file transfer modes.

Procedure

- Manually save data.

  System data files are saved manually.

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

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

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

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

  System data files are backed up manually.

  Prerequisite

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

The system data files include the database file and the configuration file. **Table 1-44** lists the commands for manually backing up the data files and describes command functions.

Table 1-44 List of commands for manually backing up the data files

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

- Select one of the backup modes in **Table 1-44** to manually back up the system data according to the actual requirements.

----End

Result

1. The system displays a message indicating that the database file and the configuration file have been saved successfully.
2. After the backup is completed, you can locate the file backed up in the path that you set in the FTP tool.

Example

Manually saving data

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

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

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

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

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

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

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

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

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

huawei(config)#
  1 [2010-07-12 14:32:18+08:00]:The percentage of saved data on 9 slot's main
control board is: 98%

huawei(config)#

huawei(config)#
  1 [2010-07-12 14:32:19+08:00]:The data of 9 slot's main control board is
saved
 completely
```

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

```
huawei#save configuration

huawei#
  It will take several minutes to save configuration file, please wait...

huawei#
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

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

```
WS6803(config)#save
{ <cr>|configuration<K>|data<K> }:

  Command:
          save

huawei(config)#
  It will take several minutes to save configuration file, please wait...

huawei(config)#
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated

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

huawei(config)#
  1 [2010-07-12 14:35:05+08:00]:The percentage of saved data on 9 slot's main
control board is: 21%

huawei(config)#
  1 [2010-07-12 14:35:08+08:00]:The percentage of saved data on 9 slot's main
control board is: 27%
```

```
huawei(config)#
  1 [2010-07-12 14:35:11+08:00]:The percentage of saved data on 9 slot's main
control board is: 66%

huawei(config)#
  1 [2010-07-12 14:35:14+08:00]:The percentage of saved data on 9 slot's main
control board is: 72%

huawei(config)#
  1 [2010-07-12 14:35:17+08:00]:The percentage of saved data on 9 slot's main
control board is: 78%

huawei(config)#
  1 [2010-07-12 14:35:20+08:00]:The percentage of saved data on 9 slot's main
control board is: 96%

huawei(config)#
  1 [2010-07-12 14:35:23+08:00]:The percentage of saved data on 9 slot's main
control board is: 98%

huawei(config)#

huawei(config)#
  1 [2010-07-12 14:35:25+08:00]:The data of 9 slot's main control board is
saved
 completely
```

Manually backing up data

1. For configuring and enabling the FTP tool on the backup sever, see **Configuring the FTP Transfer Mode**.
2. Select one of the following modes to back up the database file or the configuration file to the server.
   - Assume that the IP address of the backup server is 10.10.10.1 and the database file name is data0.dat. To back up the database file to the backup server through FTP, do as follows:

```
huawei(config)#backup data ftp 10.10.10.1 data0.dat

Command:
          backup data tftp 10.10.10.1
data0.dat
  Please save database file before backup, or the database file that is
backed
up may be not the lastest one. Are you sure to continue? (y/n)[n]: y
  Load(backup,duplicate,...) begins, please wait and notice the rate of
progress
  Any operation such as reboot or switchover will cause failure and
unpredictable result
  Backing up files starts from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type: Host data,
Backup Object: Active control board

huawei(config)#

huawei(config)#
  Backing up files is successful from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type: Host data,
Backup Object: Active control board
```

   - Assume that the IP address of the backup server is 10.10.10.1 and the configuration file name is config0.txt. To back up the configuration file to the backup server through FTP, do as follows:

```
huawei(config)#backup configuration ftp 10.10.10.1 config0.txt
  Please save configuration file before backup, or the configuration
file
backuped may be not the lastest. Are you sure to continue? (y/n)[n]:
```

```
y
  Load(backup,duplicate,...) begins, please wait and notice the rate of
progress
  Any operation such as reboot or switchover will cause failure and
unpredictable result
  Backing up files starts from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type:
Configuration
file, Backup Object: Active control board

huawei#

huawei#
  Backing up files is successful from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type:
Configuration
file, Backup Object: Active control board
```

Configuring the Auto-save and Auto-backup Functions

This topic describes how to configure the auto-save and auto-backup functions so that data is automatically saved in the flash memory or backed up to the server. These functions ensure that data or configuration files are not lost after emergency restart.

Prerequisites

The file transfer mode is configured. For details, see the following descriptions.

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

NOTE

You need to configure only one of the above-mentioned three file transfer modes.

Procedure

Step 1 Configure the auto-save function and an auto-backup server.

- Configure the auto-save function

  If the auto-save function is enabled, the system periodically checks whether data is modified at the preset time or at a preset interval. If data is modified, the system automatically saves the modified data. Otherwise, the system does not perform the auto-save operation.

  Data to be saved includes database files and configuration files. **Table 1-45** lists the commands and functions of auto-save operations.

Table 1-45 Auto-save operations

Auto-save	Command	Function
Set the auto-save file type.	**autosave type { all | configuration | data }**	● data: Saves only database files. ● configuration: Saves only configuration files. ● all: Saves both database files and configuration files.

Auto-save	Command	Function
Save database files automatically at the preset time.	**autosave time**	● The system saves data at the preset time. ● By default, the system automatically saves data at 00:00:00 every day.
Save database files automatically at an interval.	**autosave interval**	● The system automatically saves data at a preset interval. ● By default, the system saves database files at an interval of 30 minutes.

NOTE

- By default, the **autosave interval** function is disabled in the system. That is, the system does not automatically save data. Hence, you need to manually save data.
- When the **autosave interval** function is enabled, you still can manually save data.
- If data is saved frequently, the system will be affected. Therefore, it is suggested that you set the auto-save interval to longer than 60 minutes. It is better to set the auto-save interval to equal to or longer than one day.
- Before upgrading the system, run the **autosave interval***off* or **autosave time***off* command to disable the auto-save function to prevent upgrade failure due to the conflict between upgrade and auto-save operations.

CAUTION

After the system upgrade is complete, you must re-enable the auto-save function if the auto-save function is required.

- Configure an auto-backup server.

  An auto-backup server backs up data, configuration, and logs of a device to an external server. After an auto-backup server is configured, you can configure the auto-backup function.

  Auto-backup servers are classified into an active auto-backup server and standby auto-backup server.

  - You can configure only an active auto-backup server or you can configure active and standby auto-backup servers to ensure that data is backed up.
  - When the active auto-backup server does not work properly, data is automatically backed up to the standby auto-backup server.

  Run the **file-server autobakup** command to configure the active and standby auto-backup servers for backing up data, configuration, and logs.

  NOTE

  The file transfer mode, user name, and password configured must be the same as those of xFTP.

Step 2 Configure the auto-backup function.

The database files, configuration files, and logs in the system are automatically backed up to a specified external server.

Table 1-46 lists the commands and functions of auto-backup operations.

Table 1-46 Auto-backup operations

Auto-backup	Command	Function
Back up database files automatically.	**auto-backup manual data**	Immediately and automatically back up database files to the auto-backup server.
	● **auto-backup period data interval** ● **auto-backup period data enable**	● Automatically back up database files to the auto-backup server at an interval. ● Set the interval and start time of automatically backing up database files and then enable the auto-backup function for database files.
Back up configuration files automatically.	**auto-backup manual configuration**	Immediately and automatically back up configuration files to the auto-backup server.
	● **auto-backup period configuration interval** ● **auto-backup period configuration enable**	● Automatically back up configuration files to the auto-backup server at an interval. ● Set the interval and start time of automatically backing up configuration files and then enable the auto-backup function for configuration files.
Back up logs.	● **auto-backup period log interval** ● **auto-backup period log enable**	Set the interval and start time of automatically backing up logs and then enable the auto-backup function for logs.

----End

Result

1. After the auto-save function is configured, run the **display autosave configuration** command to query the preset time and preset interval.
2. After the auto-backup server is configured, run the **display file-server auto-backup** command to query configuration information about the file server, including server type, file transfer mode, IP address, user name, and password (the last three parameters are for only FTP and SFTP).
3. After the auto-backup function is configured, you can browse backup files in the path that files configured in xFTP are saved to. The file names are assigned by the system.

Example

Configure the auto-save function.

1. Configure the type of auto-save data, including database files and configuration files.

```
huawei(config)#autosave
type
{ all<K>|configuration<K>|
data<K> }:all


Command:
          autosave type all
```

2. Configure the auto-save function at a specified time or at a preset interval.

- Set the auto-save time at 02:00:00 and enable the auto-save function.

```
huawei(config)#autosave time
02:00:00
  System autosave time switch:
off
  Autosave time:
02:00:00
  Autosave type: data and configuration file

huawei(config)#autosave time
on
  System autosave time switch:
on
  Autosave time:
02:00:00
  Autosave type: data and configuration file
```

- Set the auto-save interval to 1440 minutes and enable the **autosave interval** function. The system checks whether the configuration data is modified every 1440 minutes. If the configuration data is modified, the system automatically saves the modified configuration. Otherwise, the system does not perform the auto-save operation.

CAUTION

The **autosave interval** command conflicts with the **autosave time** command. You can use either of the commands to enable the auto-save function. To switch from one function to the other one, you need to disable the enabled function first.

```
huawei(config)#autosave interval
1440
  System autosave interval switch:
off
  Autosave interval: 1440
minutes
  Autosave type: data and configuration file

huawei(config)#autosave interval
on
  System autosave interval switch:
on
  Autosave interval: 1440
minutes
  Autosave type: data and configuration
file

  System autosave modified configuration switch:
on
  Autosave interval: 30
```

```
minutes
  Autosave type: data and configuration file
```

Configure the auto-backup function.

1. Select any of the following modes to back up database files, configuration files, and logs to the backup server.
   - To enable the auto-backup function for the database file, and set the auto-backup interval to one day and the start time to 02:30, do as follows:
     ```
     huawei(config)#auto-backup period data interval 1 time 02:30
     huawei(config)#auto-backup period data enable
     ```
   - To enable the auto-backup function for the configuration file, and set the auto-backup interval to one day and the start time to 03:30, do as follows:
     ```
     huawei(config)#auto-backup period configuration interval 1 time 03:00
     huawei(config)#auto-backup period configuration enable
     ```
   - To enable the auto-backup function for the logs, and set the auto-backup interval to one day and the start time to 06:00, do as follows:
     ```
     huawei(config)#auto-backup period log interval 1 time 06:00
     huawei(config)#auto-backup period log enable
     ```

1.4 Interconnection Commissioning

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

1.4.1 Commissioning the Interconnection with the NMS

The MA5600T/MA5603T provides the function of interconnecting with the network management system, with which the administrator can maintain and manage the MA5600T/MA5603T through the NMS. This topic considers the iManager U2000 Network Management System (hereinafter referred to as the U2000) as an example to describe how to perform the interconnection commissioning between the U2000 and the MA5600T/MA5603T in the inband mode and the outband mode.

Commissioning Outband Network Management (SNMP V1 & V2)

This topic describes how to implement the outband network management on the MA5600T/MA5603T using the local maintenance Ethernet port (outband network management port). This enables the U2000 to maintain the MA5600T/MA5603T using this management channel. In the outband network management mode, a non-service channel is used to transmit the management information. With the use of the non-service channel, the management channel is separated from the service channel, which is more reliable than in the inband network management mode.

Service Requirements

In the network as shown in **Figure 1-55**, the service requirements are as follows:

- The MA5600T/MA5603T provides the outband network management channel using the local maintenance Ethernet port.
- A static route is used between the MA5600T/MA5603T and the U2000.

Figure 1-55 Example network for the outband network management

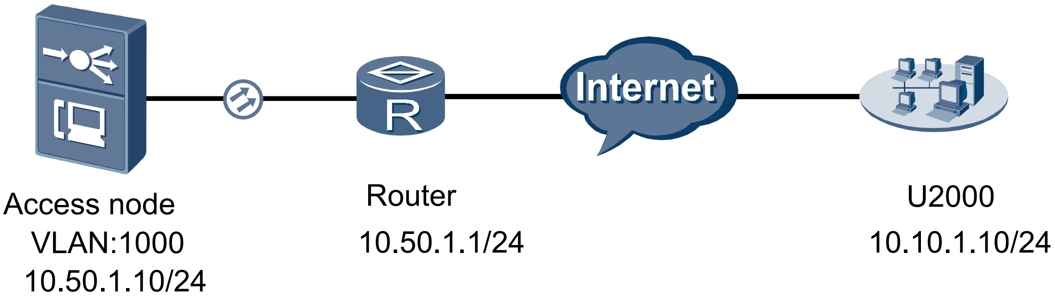
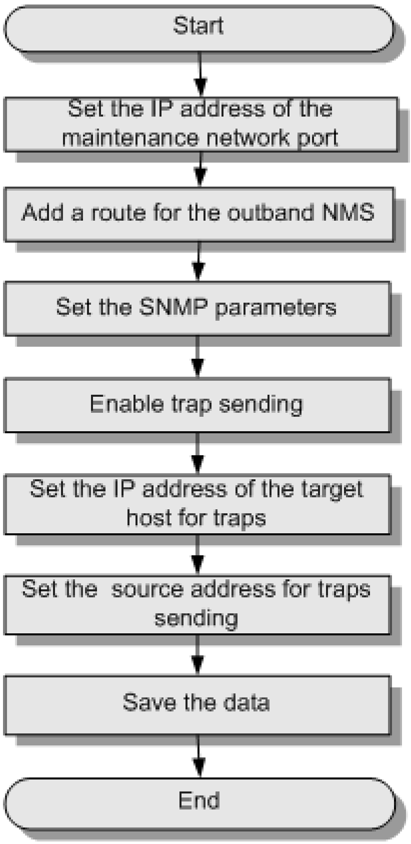


Figure 1-56 shows the flowchart for commissioning the outband network management on the device.

Figure 1-56 Flowchart for commissioning the outband network management on the device


Start
Set the IP address of the maintenance network port
Add a route for the outband NMS
Set the SNMP parameters
Enable trap sending
Set the IP address of the target host for traps
Set the source address for traps sending
Save the data
End

Procedure

- Commission the outband network management on the device.
  1. Configure the IP address of the maintenance Ethernet port.

     The IP address of the local maintenance Ethernet port (outband network management port) of the MA5600T/MA5603T is 10.50.1.10/24.

NOTE

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

```
huawei(config)#interface meth 0
huawei(config-if-meth0)#ip address 10.50.1.10 255.255.255.0
huawei(config-if-meth0)#quit
```

2. Add a route for the outband network management.

   Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T).

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

3. Set the SNMP parameters.

   a. Configure the community name and the access authority.

      The read community name is **public**, and the write community name is **private**.

      NOTE

      The configurations of the read community name and the write community name must be the same as the configurations on the U2000.

      ```
      huawei(config)#snmp-agent community read public
      huawei(config)#snmp-agent community write private
      ```

   b. (Optional) Set the ID and the contact means of the administrator.

      The contact means of the administrator is **HW-075528780808**.

      ```
      huawei(config)#snmp-agent sys-info contact HW-075528780808
      ```

   c. (Optional) Set the location of the device.

      The location of the device is **Shenzhen_China**.

      ```
      huawei(config)#snmp-agent sys-info location Shenzhen_China
      ```

   d. Set the SNMP version.

      - The SNMP version is SNMP V1.

        ```
        huawei(config)#snmp-agent sys-info version v1
        ```

      - The SNMP version is SNMP V2.

        ```
        huawei(config)#snmp-agent sys-info version v2c
        ```

      NOTE

      The SNMP version must be the same as the SNMP version set on the U2000.

4. Enable the function of sending traps.

   On the MA5600T/MA5603T, enable the function of sending traps to the U2000.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

5. Configure the IP address of the destination host for the traps.

   - When the SNMP V1 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V1**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

     ```
     huawei(config)#snmp-agent target-host trap-hostname huawei address
     10.10.1.10
      trap-paramsname ABC
     huawei(config)#snmp-agent target-host trap-paramsname
      ABC v1 securityname private
     ```

   - When the SNMP V2 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V2**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC
 v2c securityname private
```

6. Set the IP address of the maintenance Ethernet port as the source IP address for sending traps.

   Set the SNMP packets to be forwarded from the maintenance Ethernet port of the MA5600T/MA5603T. That is, the source address of the traps is meth 0.

   ```
   huawei(config)#snmp-agent trap source meth 0
   ```

7. Save the data.

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

- Commission the outband network management on the U2000.

1. Configure the gateway of the route from the U2000 to network segment 10.50.1.0/24 to 10.10.1.1.

   - In the Solaris OS, do as follows:

     Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

     Run the **netstat -r** command to query the information about the current routing table.

   - In the Windows OS, do as follows:

     Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

     Run the **route print** command to query the information about the current routing table.

   NOTE

   If the IP address of the outband network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.

2. Log in to the U2000.

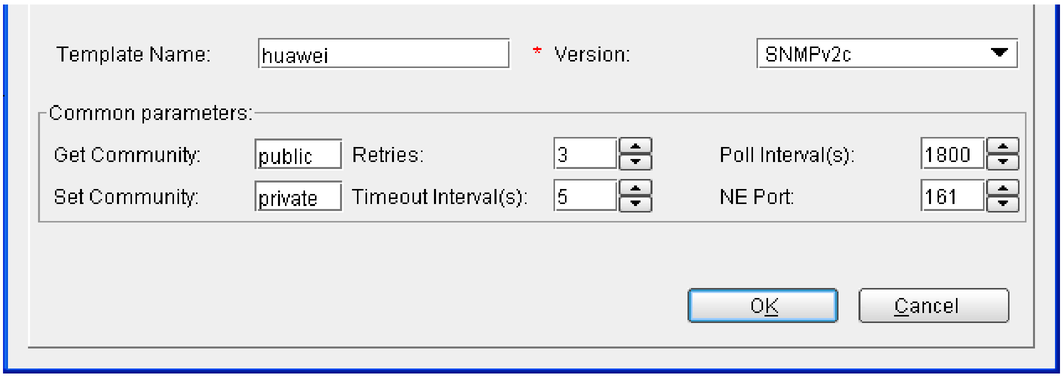
3. Set the SNMP parameters. A default SNMP profile exists in the system. Use the default profile in this service. If a new profile is required, do as follows:

   a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.

   b. On the **NE Access Parameters** tab page, click **Reset**. In the dialog box that is displayed, click the corresponding tab, and then click **Add**.

   c. - When the SNMP V1 is used, choose **SNMP v1 Parameter**, set the SNMP parameters in the lower pane, as shown in the following figure (the other parameters except **Profile name** use the default settings).

Figure 1-57 Set the SNMP parameters



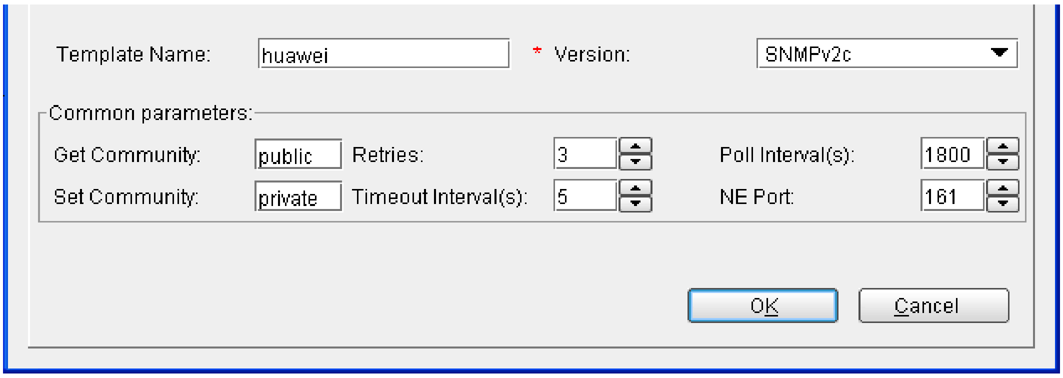
Template Name: huawei
* Version: SNMPv2c

Common parameters:

Get Community: public
Retries: 3
Poll Interval(s): 1800
Set Community: private
Timeout Interval(s): 5
NE Port: 161

- When the SNMP V2 is used, choose **SNMP v2 Parameter**, set the SNMP parameters in the lower pane, as shown in the following figure (the other parameters except **Profile name** use the default settings).

Figure 1-58 Set the SNMP parameters



Template Name: huawei
* Version: SNMPv2c

Common parameters:

Get Community: public
Retries: 3
Poll Interval(s): 1800
Set Community: private
Timeout Interval(s): 5
NE Port: 161

NOTE

The configurations of **Get Community** and **Set Community** are the same as the configurations on the MA5600T/MA5603T.

d. Click **OK**.

e. Select the added SNMP parameters. Click **OK**.

f. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

g. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

4. Add a device.

a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

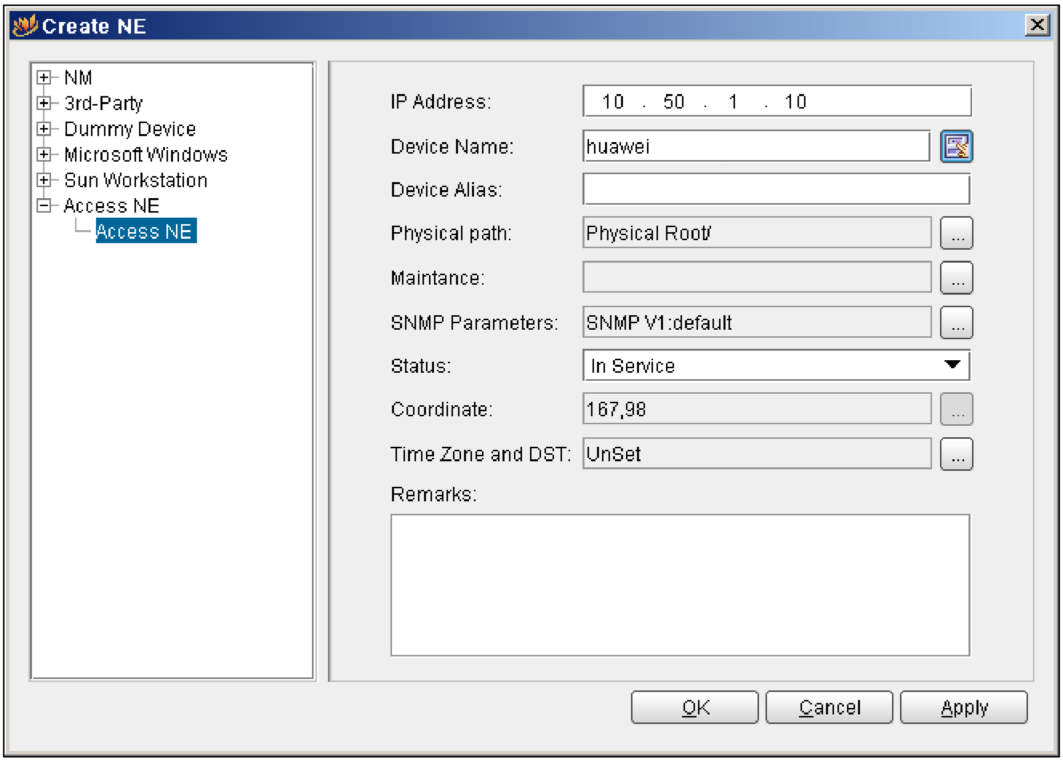
b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

c. In the right pane, set the parameters.

- When the SNMP V1 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V1:default**.

Figure 1-59 Add device



IP Address: 10 . 50 . 1 . 10

Device Name: huawei

Device Alias:

Physical path: Physical Root/

Maintance:

SNMP Parameters: SNMP V1:default

Status: In Service

Coordinate: 167,98

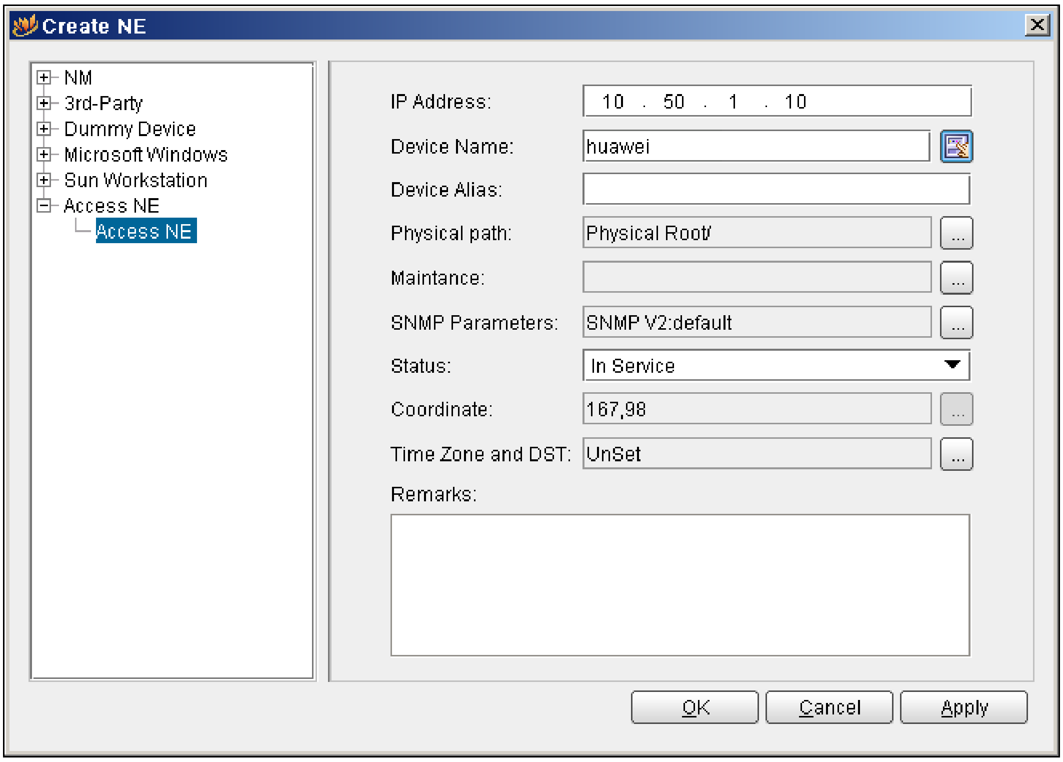
Time Zone and DST: UnSet

Remarks:

- When the SNMP V2 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V2:default**.

Figure 1-60 Add device



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V2:default
Status: In Service
Coordinate: 167,98
Time Zone and DST: UnSet
Remarks:

d. Click **OK**. The system displays a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T using the U2000.

Configuration File

The following describes the script for commissioning the outband network management on the device (SNMP V1).

```
interface meth 0
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v1

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v1 securityname private
```

```
snmp-agent trap source meth 0

save
```

The following describes the script for commissioning the outband network management on the device (SNMP V2).

```
interface meth 0
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v2c

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v2c securityname private

snmp-agent trap source meth 0

save
```

Commissioning Outband Management (SNMP V3)

This topic describes how to implement the outband network management on the MA5600T/MA5603T using the local maintenance Ethernet port (outband network management port). This enables the U2000 to maintain the MA5600T/MA5603T using this management channel. In the outband network management mode, a non-service channel is used to transmit the management information. With the use of the non-service channel, the management channel is separated from the service channel, which is more reliable than in the inband network management mode.

Service Requirements

In the network as shown in **Figure 1-61**, the service requirements are as follows:

- The MA5600T/MA5603T provides the outband network management channel through the local maintenance Ethernet port.
- A static route is used between the MA5600T/MA5603T and the U2000.
- SNMP V3 is used (more reliable than V1 and V2, providing network security and access control management functions).

Figure 1-61 Example network for the outband network management

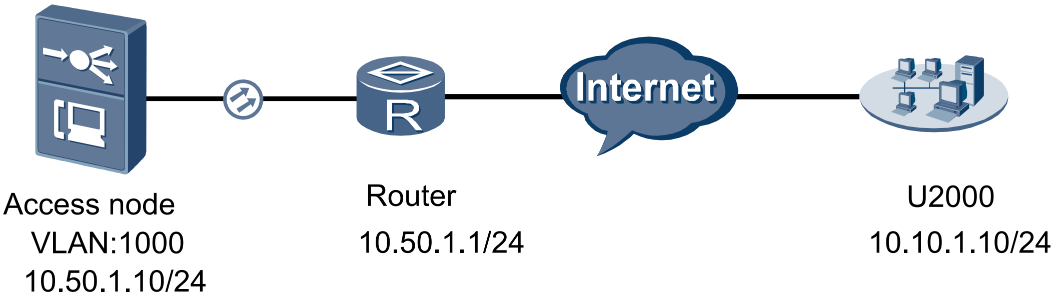
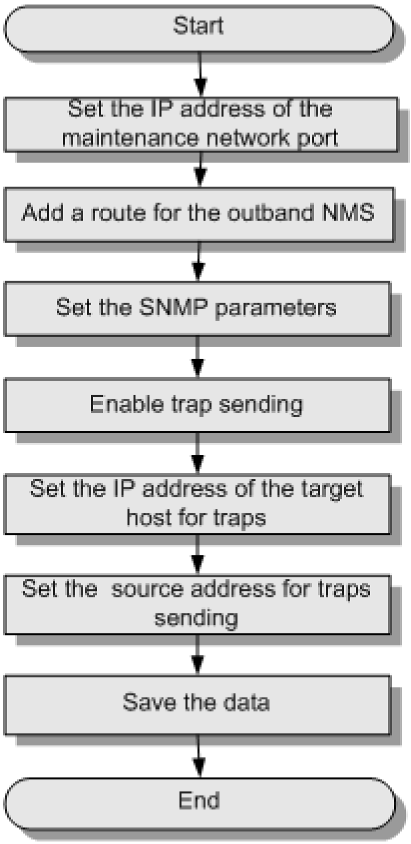


Figure 1-62 shows the flowchart for commissioning the outband network management on the device.

Figure 1-62 Flowchart for commissioning the outband network management on the device


Start
Set the IP address of the maintenance network port
Add a route for the outband NMS
Set the SNMP parameters
Enable trap sending
Set the IP address of the target host for traps
Set the source address for traps sending
Save the data
End

Procedure

- Commission the outband network management on the device.
  1. Configure the IP address of the maintenance Ethernet port.

     The IP address of the local maintenance Ethernet port (outband network management port) of the MA5600T/MA5603T is 10.50.1.10/24.

     NOTE

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

     ```
     huawei(config)#interface meth 0
     huawei(config-if-meth0)#ip address 10.50.1.10 255.255.255.0
     huawei(config-if-meth0)#quit
     ```
  2. Add a route for the outband network management.

     Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T).

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

3. Set the SNMP parameters.

   a. Configure the SNMP user, group, and view.

      The user name is **user1**, the group name is **group1**, the user authentication mode is **SHA**, the authentication password is **authkey123**, the user encryption mode is **des56**, the encryption password is **prikey123**, the read and write view names are **hardy**, and the view includes the internet subtree.

      ```
      huawei(config)#snmp-agent usm-user v3 user1 group1
      authentication-mode sha authkey123 privacy-mode des56 prikey123
      huawei(config)#snmp-agent group v3 group1 privacy read-view hardy
      write-view hardy
      huawei(config)#snmp-agent mib-view hardy include internet
      ```

   b. (Optional) Set the ID and contact means of the administrator.

      The contact means of the administrator is **HW-075528780808**.

      ```
      huawei(config)#snmp-agent sys-info contact HW-075528780808
      ```

   c. (Optional) Set the location of the device.

      The location of the device is **Shenzhen_China**.

      ```
      huawei(config)#snmp-agent sys-info location Shenzhen_China
      ```

   d. (Optional) Configure the engine ID of the SNMP entity.

      The engine ID of the SNMP entity is set to 0123456789.

      NOTE

      The context engine ID of the SNMP must be the same as that on the U2000.

      ```
      huawei(config)#snmp-agent local-engineid 0123456789
      ```

   e. Set the SNMP version.

      The SNMP version is SNMP V3.

      NOTE

      The SNMP version must be the same as the SNMP version set on the U2000.

      ```
      huawei(config)#snmp-agent sys-info version v3
      ```

4. Enable the function of sending traps.

   On the MA5600T/MA5603T, enable the function of sending traps to the U2000.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

5. Configure the IP address of the destination host for the traps.

   The host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, the SNMP version is **V3**, the parameter security name is **user1** (when the SNMP V3 is used, the parameter security name is the USM user name), and the traps are authenticated and encrypted.

   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei
   address 10.10.1.10 trap-paramsname ABC
   huawei(config)#snmp-agent target-host trap-paramsname
   ABC v3 securityname user1 privacy
   ```

6. Set the IP address of the maintenance Ethernet port as the source IP address for sending traps.

   Set the SNMP packets to be forwarded from the maintenance Ethernet port of the MA5600T/MA5603T. That is, the source address of the traps is meth 0.

   ```
   huawei(config)#snmp-agent trap source meth 0
   ```

7. Save the data.

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

- Commission the outband network management on the U2000.

1. Configure the gateway of the route from the U2000 server to network segment 10.50.1.0/24 to 10.10.1.1.
   - In the Solaris OS, do as follows:

     Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

     Run the **netstat -r** command to query the information about the current routing table.
   - In the Windows OS, do as follows:

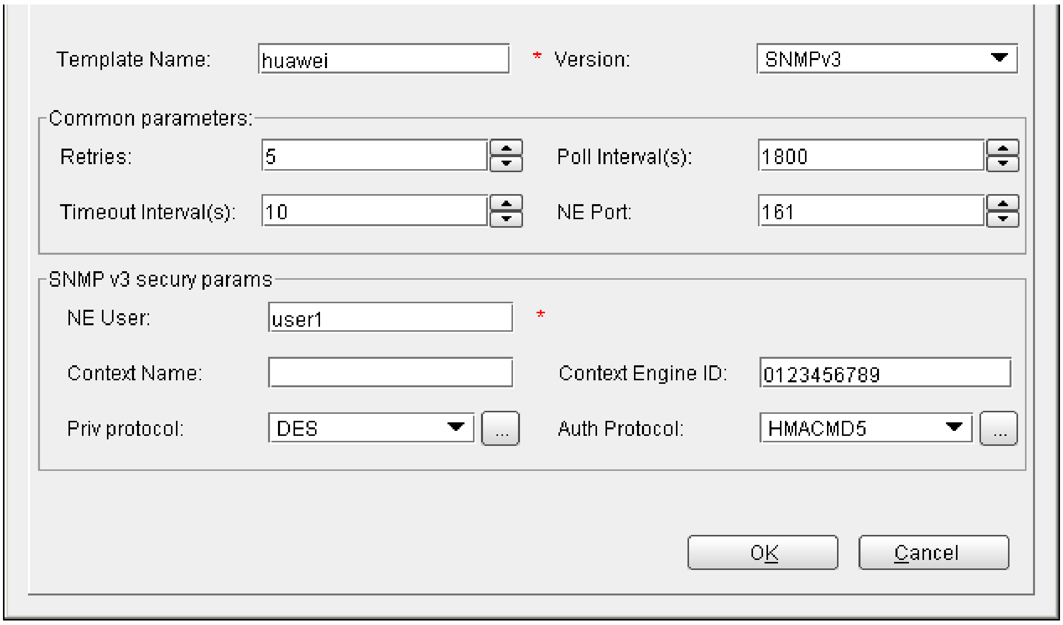
     Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

     Run the **route print** command to query the information about the current routing table.

   NOTE

   When the IP address of the network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
2. Set the SNMP parameters.
   a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.
   b. On the **NE Access Parameters** tab page, click **Reset**. In the dialog box that is displayed, click the corresponding tab, and then click **Add**.
   c. Choose **SNMP v3 Parameter**, set the SNMP parameters in the lower pane, as shown in **Figure 1-63**.

Figure 1-63 Set the SNMP parameters



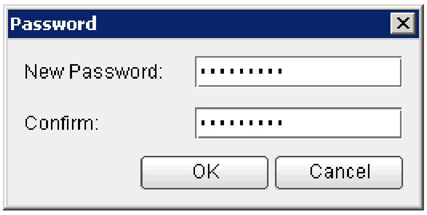
Template Name: huawei
* Version: SNMPv3

Common parameters:
Retries: 5
Poll Interval(s): 1800
Timeout Interval(s): 10
NE Port: 161

SNMP v3 secury params
NE User: user1 *
Context Name:
Context Engine ID: 0123456789
Priv protocol: DES
Auth Protocol: HMACMD5

After selecting corresponding protocols in **Priv Protocol** and **Auth Protocol**, click ... next to the parameter, and set the passwords of data encryption protocol and authentication protocol, as shown in **Figure 1-64**.

Figure 1-64 Set the password



NOTE

NE User, **Context Engine ID**, **Priv Protocol** and password, and **Auth Protocol** and password must be the same as those configured on the MA5600T/MA5603T. You can run the **display snmp-agent usm-user** command to query the device user, data encryption protocol, and authentication protocol on the MA5600T/MA5603T and run the **display snmp-agent local-engineid** command to query the context engine ID on the MA5600T/MA5603T.

d. Click **OK**.

e. Select the added SNMP parameters. Click **OK**.

f. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

g. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

3. Add a device.

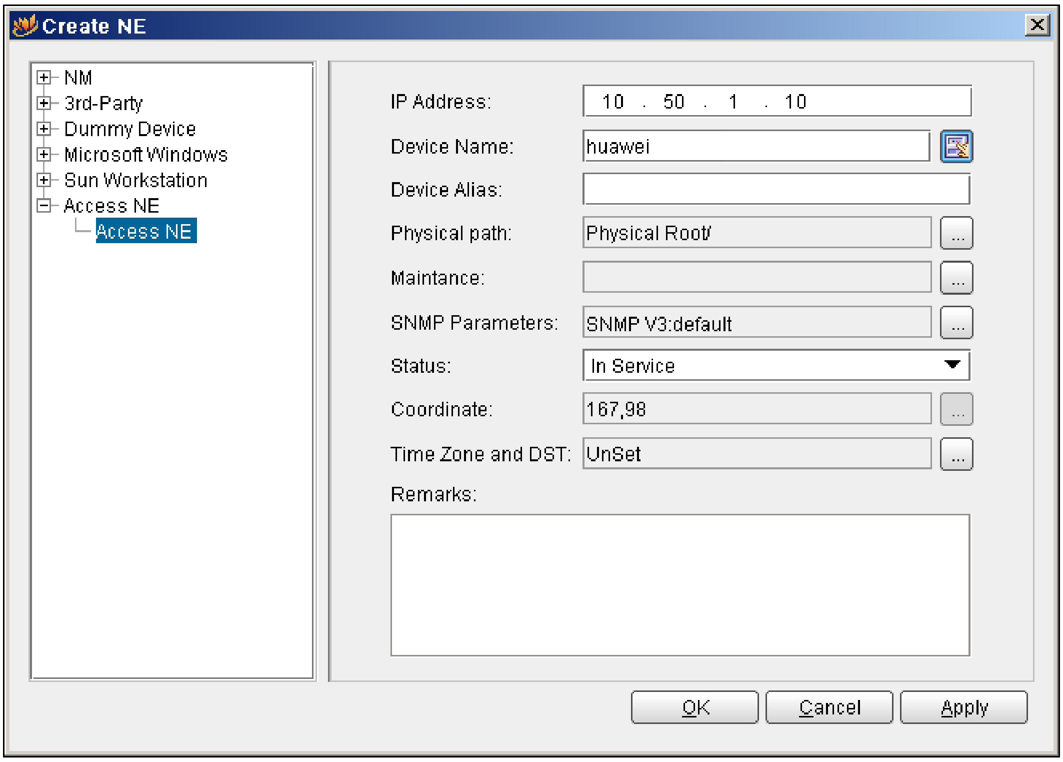
a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

c. In the dialog box that is displayed, set the required parameters, as shown in **Figure 1-65**.

IP address is **10.50.1.10**, **Device Name** is **huawei**, **SNMP Parameters** is **SNMP V3:default**.

Figure 1-65 Add device



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V3:default
Status: In Service
Coordinate: 167,98
Time Zone and DST: UnSet
Remarks:

4. Click **OK**. The system prompts a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T through the U2000.

Configuration File

The following describes the script for commissioning the outband network management on the device.

```
interface meth 0
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1
snmp-agent usm-user v3 user1 group1 authentication-mode md5 authkey123 privacy-mode
des56 prikey123
snmp-agent group v3 group1 privacy read-view hardy write-view hardy

snmp-agent mib-view hardy include internet

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v3

snmp-agent trap enable standard
```

```
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy

snmp-agent trap source meth 0

save
```

Commissioning Inband Management (SNMP V1 and V2)

This topic describes how to implement the inband network management on the MA5600T/MA5603T through the upstream port (inband network management port). This enables the U2000 to maintain the MA5600T/MA5603T through this management channel. In the inband network management mode, the service channel of the device is used to transmit the management information. The network is flexible and requires no additional devices, which helps save the cost for carriers. This network, however, is difficult to maintain.

Service Requirements

In the network as shown in **Figure 1-66**, the service requirements are as follows:

- The MA5600T/MA5603T provides the inband network management through the upstream port.
- The upstream port of the GIU board on the MA5600T/MA5603T is used as the inband network management port.
- A static route is used between the MA5600T/MA5603T and the U2000.

Figure 1-66 Example network for the inband network management

=

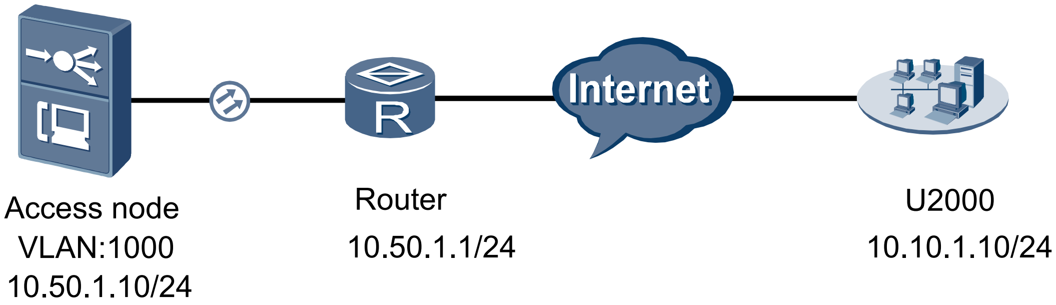
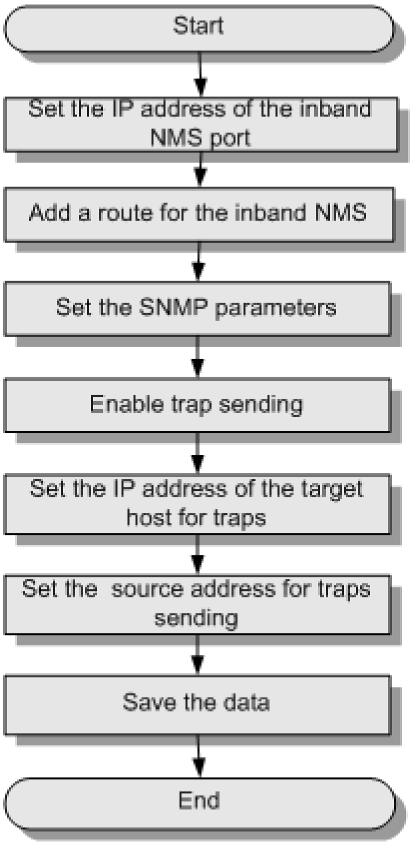


Figure 1-67 shows the flowchart for commissioning the inband network management.

Figure 1-67 Flowchart for commissioning the inband network management


Start
Set the IP address of the inband NMS port
Add a route for the inband NMS
Set the SNMP parameters
Enable trap sending
Set the IP address of the target host for traps
Set the source address for traps sending
Save the data
End

Procedure

- Commission the inband network management on the device.

1. Configure the IP address of the inband network management port.

   The upstream port (inband network management port) is 0/19/0, the VLAN ID is 1000, the VLAN type is standard VLAN, and the IP address is 10.50.1.10/24.

   ```
   huawei(config)#vlan 1000 standard
   huawei(config)#port vlan 1000 0/19 0
   huawei(config)#interface vlanif 1000
   huawei(config-if-vlanif1000)#ip address 10.50.1.10 255.255.255.0
   huawei(config-if-vlanif1000)#quit
   ```

   NOTE

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

2. Add a route for the inband network management.

   Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T).

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

3. Set the SNMP parameters.

   a. Configure the community name and the access authority.

The read community name is **public**, and the write community name is **private**.

NOTE

The configurations of the read community name and the write community name must be the same as the configurations on the U2000.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

b. (Optional) Set the ID and the contact means of the administrator.

The contact means of the administrator is **HW-075528780808**.

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
```

c. (Optional) Set the location of the device.

The location of the device is **Shenzhen_China**.

```
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

d. Set the SNMP version.

- The SNMP version is SNMP V1.

```
huawei(config)#snmp-agent sys-info version v1
```

- The SNMP version is SNMP V2.

```
huawei(config)#snmp-agent sys-info version v2c
```

NOTE

The SNMP version must be the same as the SNMP version set on the U2000.

4. Enable the function of sending traps.

On the MA5600T/MA5603T, enable the function of sending traps to the U2000.

```
huawei(config)#snmp-agent trap enable standard
```

5. Configure the IP address of the destination host for the traps.

- When the SNMP V1 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V1**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
10.10.1.10
 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname
 ABC v1 securityname private
```

- When the SNMP V2 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V2**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC
 v2c securityname private
```

6. Configure the IP address of the VLAN interface as the source address for sending traps.

Enable the forwarding of the SNMP packets from the L3 interface of VLAN 1000 of the MA5600T/MA5603T.

```
huawei(config)#snmp-agent trap source vlanif 1000
```

7. Save the data.

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

- Commission the inband network management on the U2000.

1. Configure the gateway of the route from the U2000 to network segment 10.50.1.0/24 to 10.10.1.1.
   - In the Solaris OS, do as follows:

     Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

     Run the **netstat -r** command to query the information about the current routing table.
   - In the Windows OS, do as follows:

     Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

     Run the **route print** command to query the information about the current routing table.

   NOTE

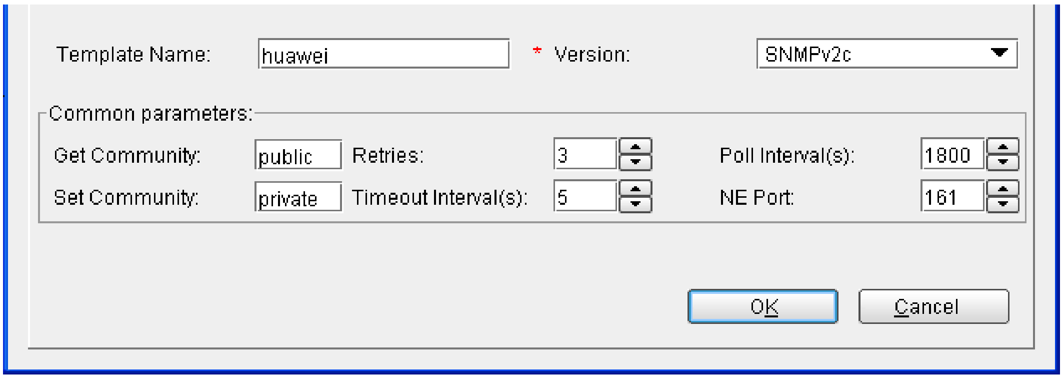
   If the IP address of the outband network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
2. Log in to the U2000.
3. Set the SNMP parameters. A default SNMP profile exists in the system. Use the default profile in this service. If a new profile is required, do as follows:

   a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.

   b. On the **NE Access Parameters** tab page, click **Reset**. In the dialog box that is displayed, click the corresponding tab, and then click **Add**.

   c. – When the SNMP V1 is used, choose **SNMP v1 Parameter**, set the SNMP parameters in the lower pane, as shown in the following figure (the other parameters except **Profile name** use the default settings).

Figure 1-68 Set the SNMP parameters



Template Name: huawei

* Version: SNMPv2c

Common parameters:

Get Community: public

Retries: 3

Poll Interval(s): 1800

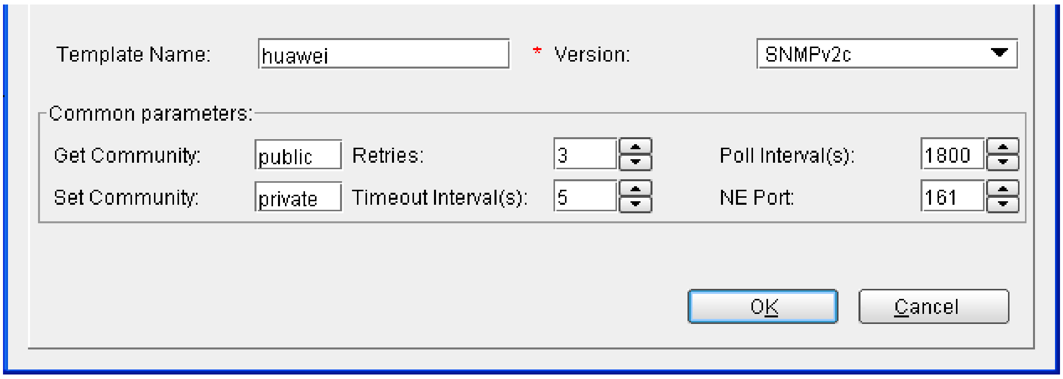
Set Community: private

Timeout Interval(s): 5

NE Port: 161

– When the SNMP V2 is used, choose **SNMP v2 Parameter**, set the SNMP parameters in the lower pane, as shown in the following figure (the other parameters except **Profile name** use the default settings).

Figure 1-69 Set the SNMP parameters



Template Name: huawei

* Version: SNMPv2c

Common parameters:

Get Community: public

Retries: 3

Poll Interval(s): 1800

Set Community: private

Timeout Interval(s): 5

NE Port: 161

NOTE

The configurations of **Get Community** and **Set Community** are the same as the configurations on the MA5600T/MA5603T.

d. Click **OK**.

e. Select the added SNMP parameters. Click **OK**.

f. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

g. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

4. Add a device.

a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

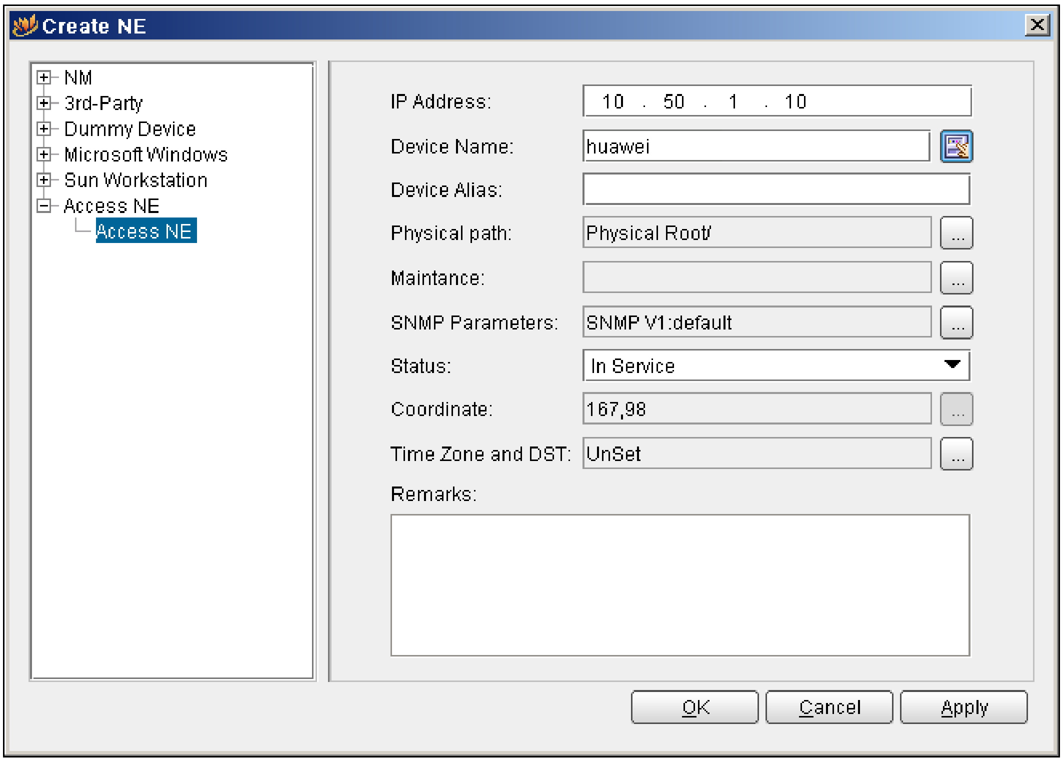
b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

c. In the right pane, set the parameters.

- When the SNMP V1 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V1:default**.

Figure 1-70 Add device



IP Address: 10 . 50 . 1 . 10

Device Name: huawei

Device Alias:

Physical path: Physical Root/

Maintance:

SNMP Parameters: SNMP V1:default

Status: In Service

Coordinate: 167,98

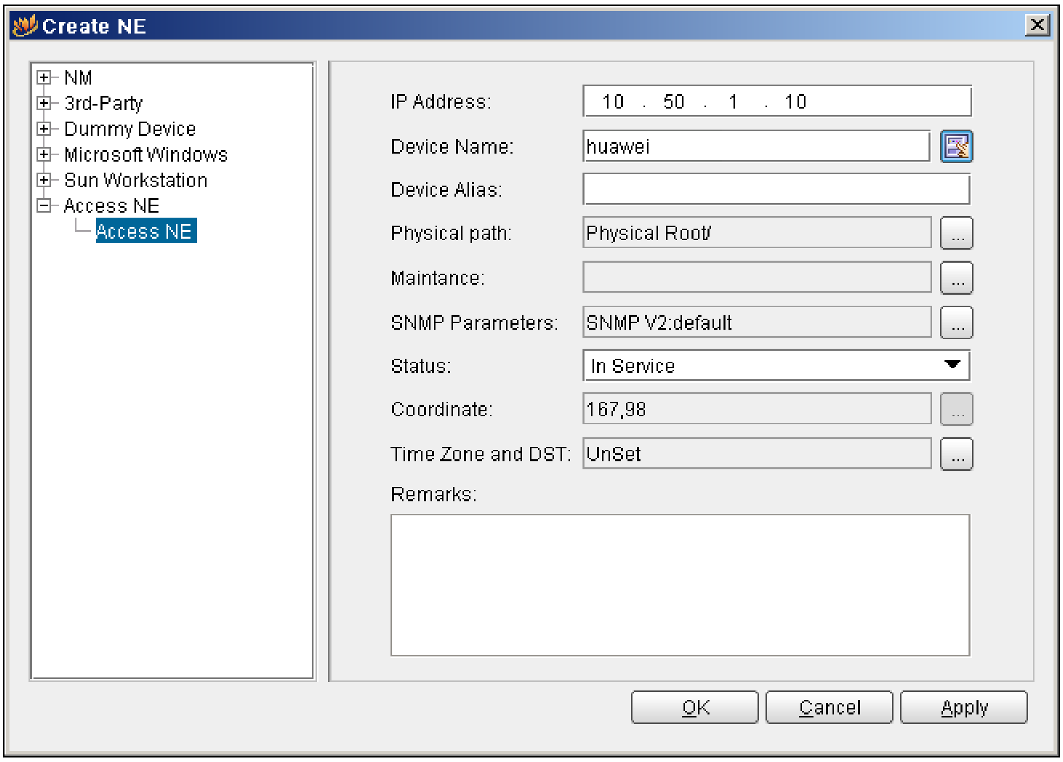
Time Zone and DST: UnSet

Remarks:

- When the SNMP V2 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V2:default**.

Figure 1-71 Add device



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V2:default
Status: In Service
Coordinate: 167,98
Time Zone and DST: UnSet
Remarks:

d. Click **OK**. The system displays a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T through the U2000.

Configuration File

The following describes the script for commissioning the inband network management on the device (SNMP V1).

```
vlan 1000 standard
port vlan 1000 0/19 0
interface vlanif 1000
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v1
```

```
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v1 securityname private

snmp-agent trap source vlanif 1000
save
```

The following describes the script for commissioning the inband network management on the device (SNMP V2).

```
vlan 1000 standard
port vlan 1000 0/19 0
interface vlanif 1000
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v2c

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v2c securityname private

snmp-agent trap source vlanif 1000
save
```

Commissioning Inband Network Management (SNMP V3)

This topic describes how to implement the inband network management on the MA5600T/MA5603T through the upstream port (inband network management port). This enables the U2000 to maintain the MA5600T/MA5603T through this management channel. In the inband network management mode, the service channel of the device is used to transmit the management information. The network is flexible and requires no additional devices, which helps save the cost for carriers. This network, however, is difficult to maintain.

Service Requirements

In the network as shown in **Figure 1-72**, the service requirements are as follows:

- The MA5600T/MA5603T provides the inband network management through the upstream port.
- The upstream port of the GIU board on the MA5600T/MA5603T is used as the inband network management port.
- A static route is used between the MA5600T/MA5603T and the U2000.
- SNMP V3 is used (more reliable than V1 and V2, providing network security and access control management functions).

Figure 1-72 Example network for the inband network management

=

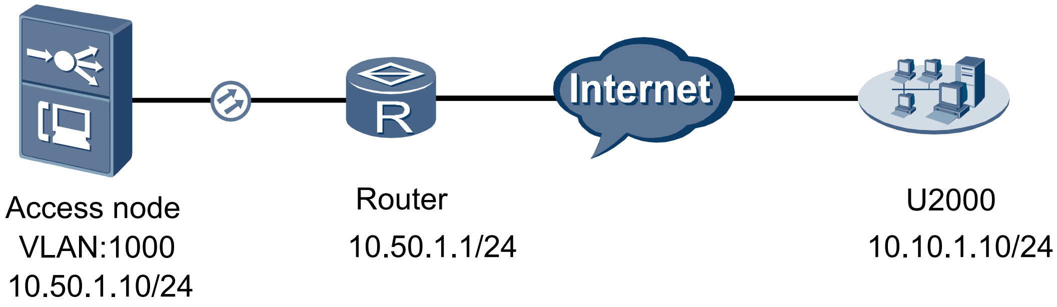
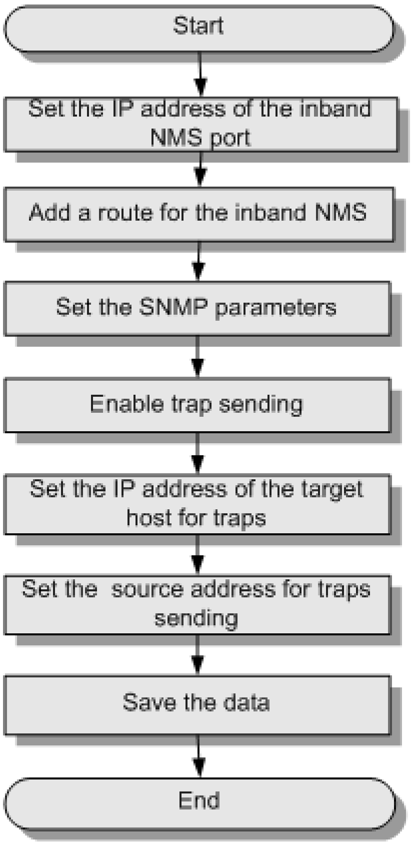


Figure 1-73 shows the flowchart for commissioning the inband network management.

Figure 1-73 Flowchart for commissioning the inband network management


Start
Set the IP address of the inband NMS port
Add a route for the inband NMS
Set the SNMP parameters
Enable trap sending
Set the IP address of the target host for traps
Set the source address for traps sending
Save the data
End

Procedure

- Commission the inband network management on the device.
  1. Configure the IP address of the inband network management port.

     The upstream port (inband network management port) is 0/19/0, the VLAN ID is 1000, the VLAN type is standard VLAN, and the IP address is 10.50.1.10/24.

     ```
     huawei(config)#vlan 1000 standard
     huawei(config)#port vlan 1000 0/19 0
     huawei(config)#interface vlanif 1000
     ```

```
huawei(config-if-vlanif1000)#ip address 10.50.1.10 255.255.255.0
huawei(config-if-vlanif1000)#quit
```

NOTE

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

2. Add a route for the inband network management.

   Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T).

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

3. Log in to the U2000.
4. Set the SNMP parameters.

   a. Configure the SNMP user, group, and view.

      The user name is **user1**, the group name is **group1**, the user authentication mode is **SHA**, the authentication password is **authkey123**, the user encryption mode is **des56**, the encryption password is **prikey123**, the read and write view names are **hardy**, and the view includes the internet subtree.

      ```
      huawei(config)#snmp-agent usm-user v3 user1 group1
      authentication-mode sha authkey123 privacy-mode des56 prikey123
      huawei(config)#snmp-agent group v3 group1 privacy read-view hardy
      write-view hardy
      huawei(config)#snmp-agent mib-view hardy include internet
      ```

   b. (Optional) Set the ID and contact means of the administrator.

      The contact means of the administrator is **HW-075528780808**.

      ```
      huawei(config)#snmp-agent sys-info contact HW-075528780808
      ```

   c. (Optional) Set the location of the device.

      The location of the device is **Shenzhen_China**.

      ```
      huawei(config)#snmp-agent sys-info location Shenzhen_China
      ```

   d. (Optional) Configure the engine ID of the SNMP entity.

      The engine ID of the SNMP entity is set to 0123456789.

      NOTE

      The context engine ID of the SNMP must be the same as that on the U2000.

      ```
      huawei(config)#snmp-agent local-engineid 0123456789
      ```

   e. Set the SNMP version.

      The SNMP version is SNMP V3.

      NOTE

      The SNMP version must be the same as the SNMP version set on the U2000.

      ```
      huawei(config)#snmp-agent sys-info version v3
      ```

5. Enable the function of sending traps.

   On the MA5600T/MA5603T, enable the function of sending traps to the U2000.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

6. Configure the IP address of the destination host for the traps.

   The host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, the SNMP version is **V3**, the parameter security name is **user1** (when the SNMP V3 is used, the parameter security name is the USM user name), and the traps are authenticated and encrypted.

```
huawei(config)#snmp-agent target-host trap-hostname huawei
address 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname
ABC v3 securityname user1 privacy
```

7. Configure the IP address of the VLAN interface as the source address for sending traps.

   Enable the forwarding of the SNMP packets from the L3 interface of VLAN 1000 of the MA5600T/MA5603T.

   ```
   huawei(config)#snmp-agent trap source vlanif 1000
   ```

8. Save the data.

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

- Commission the inband network management on the U2000.
  1. Configure the gateway of the route from the U2000 server to network segment 10.50.1.0/24 to 10.10.1.1.
     - In the Solaris OS, do as follows:

       Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

       Run the **netstat -r** command to query the information about the current routing table.
     - In the Windows OS, do as follows:

       Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

       Run the **route print** command to query the information about the current routing table.

     NOTE

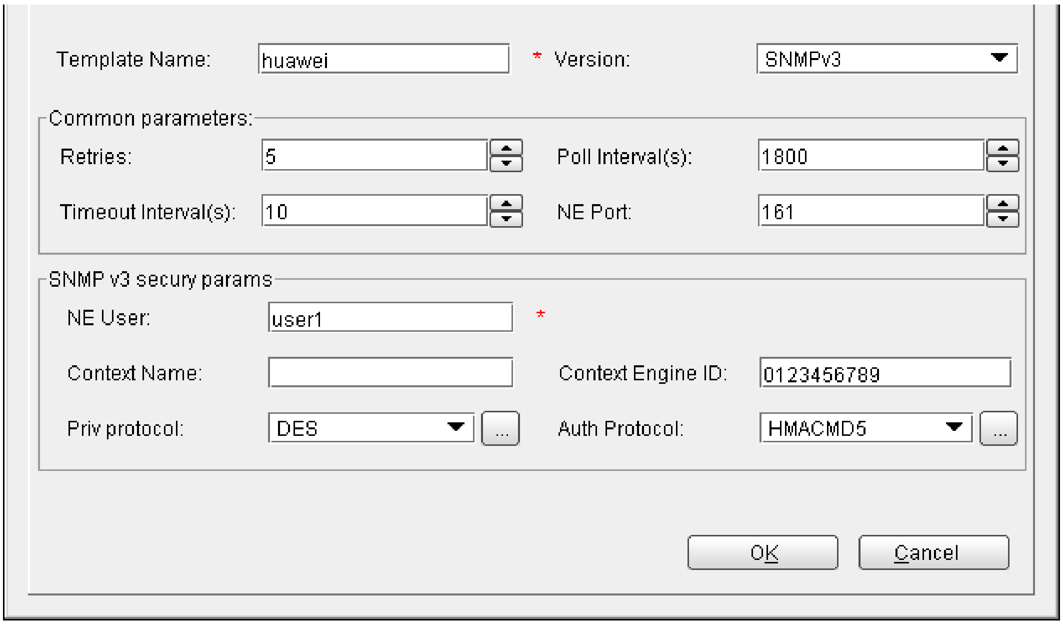
     When the IP address of the network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
  2. Set the SNMP parameters.

     a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.

     b. On the **NE Access Parameters** tab page, click **Reset**. In the dialog box that is displayed, click the corresponding tab, and then click **Add**.

     c. Choose **SNMP v3 Parameter**, set the SNMP parameters in the lower pane, as shown in **Figure 1-74**.

Figure 1-74 Set the SNMP parameters



Template Name: huawei
* Version: SNMPv3

Common parameters:

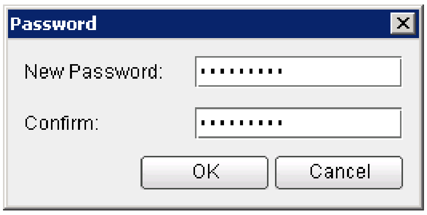
Retries: 5
Poll Interval(s): 1800
Timeout Interval(s): 10
NE Port: 161

SNMP v3 secury params

NE User: user1 *
Context Name:
Context Engine ID: 0123456789
Priv protocol: DES
Auth Protocol: HMACMD5

After selecting corresponding protocols in **Priv Protocol** and **Auth Protocol**, click ... next to the parameter, and set the passwords of data encryption protocol and authentication protocol, as shown in **Figure 1-75**.

Figure 1-75 Set the password



Password

New Password: ·········
Confirm: ·········

NOTE

NE User, **Context Engine ID**, **Priv Protocol** and password, and **Auth Protocol** and password must be the same as those configured on the MA5600T/MA5603T. You can run the **display snmp-agent usm-user** command to query the device user, data encryption protocol, and authentication protocol on the MA5600T/MA5603T and run the **display snmp-agent local-engineid** command to query the context engine ID on the MA5600T/MA5603T.

d. Click **OK**.

e. Select the added SNMP parameters. Click **OK**.

f. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

g. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

3. Add a device.

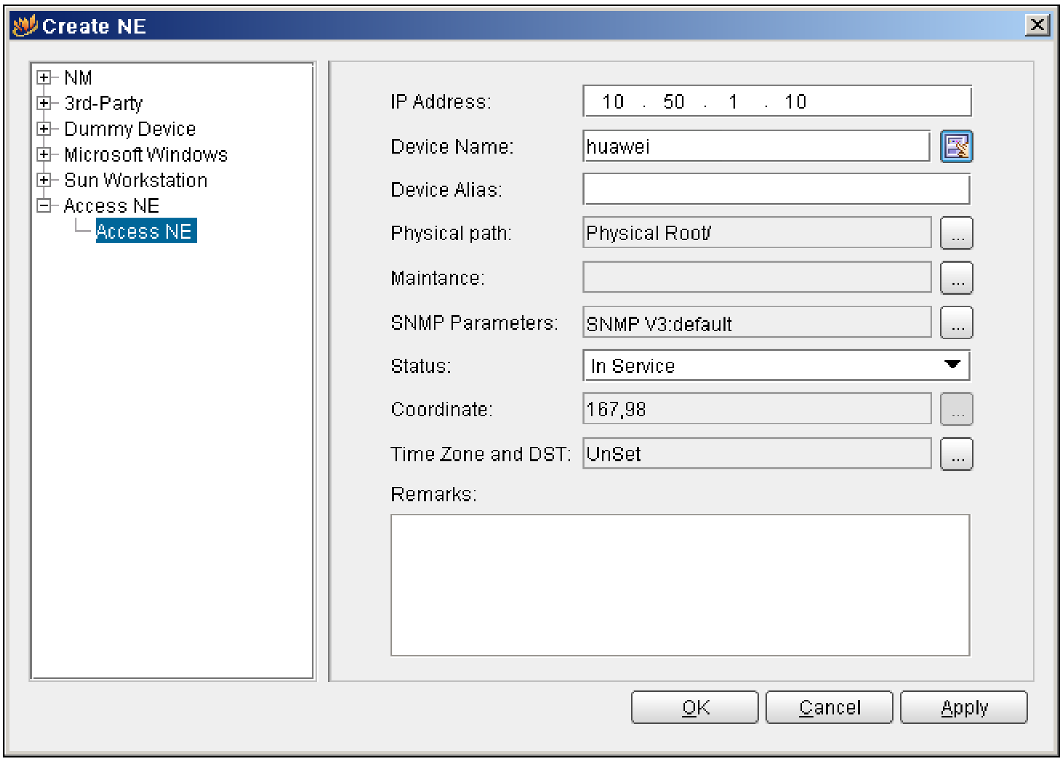
a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

c. In the dialog box that is displayed, set the required parameters, as shown in **Figure 1-76**.

IP address is **10.50.1.10**, **Device Name** is **huawei**, **SNMP Parameters** is **SNMP V3:default**.

Figure 1-76 Add device



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V3:default
Status: In Service
Coordinate: 167,98
Time Zone and DST: UnSet
Remarks:

4. Click **OK**. The system prompts a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T through the U2000.

Configuration File

The following describes the script for commissioning the inband network management on the device.

```
vlan 1000 standard
port vlan 1000 0/19 0
interface vlanif 1000
```

```
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent usm-user v3 user1 group1 authentication-mode md5 authkey123 privacy-mode
des56 prikey123
snmp-agent group v3 group1 privacy read-view hardy write-view hardy

snmp-agent mib-view hardy include internet

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v3

snmp-agent trap enable standard

snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy

snmp-agent trap source vlanif 1000
save
```

1.4.2 Commissioning the Interconnection with the Router

This topic describes how to check whether the MA5600T/MA5603T can normally communicate with the router and whether the MA5600T/MA5603T can access the upper-layer device through the router.

Service Requirements

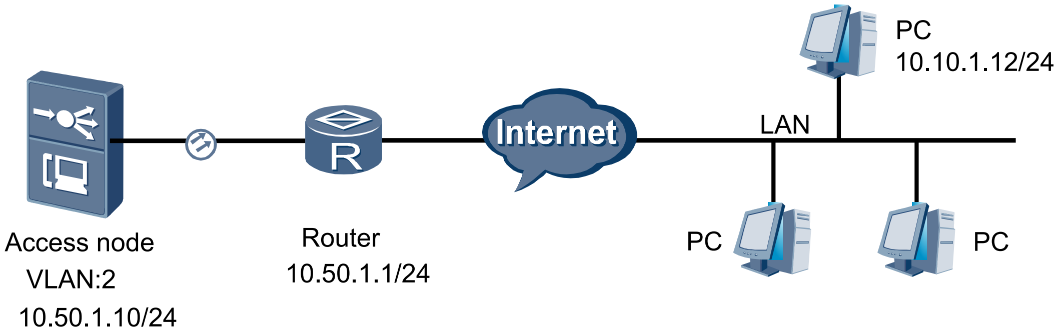
In the network as shown in **Figure 1-77**, the service requirements are as follows:

- The MA5600T/MA5603T uses the GIU board for upstream transmission.
- By interconnecting with the router, the MA5600T/MA5603T can be interconnected with the upper-layer device through configuring a static route on the MA5600T/MA5603T.

NOTE

For details about how to configure a router, see the related configuration guide.

Figure 1-77 Example network for commissioning the interconnection with the router



Procedure

Step 1 Configure a VLAN.

The VLAN ID is 2, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 2 smart
```

Step 2 Add an upstream port to the VLAN.

Upstream port 0/19/0 is added to VLAN 2.

```
huawei(config)#port vlan 2 0/19 0
```

NOTE

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

Step 3 Configure the IP address of the L3 interface.

The L3 interface IP address is 10.50.1.10/24, and this IP address must be in the same network segment as the gateway IP address (IP address of the router port that is connected to the MA5600T/MA5603T).

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.50.1.10 255.255.255.0
huawei(config-if-vlanif2)#quit
```

Step 4 Add a static route.

The destination IP address is 10.10.1.0/24, and the next-hop IP address is gateway IP address 10.50.1.1.

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

Step 5 Save the data.

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

----End

Result

After the MA5600T/MA5603T is interconnected with the router successfully, you can ping IP address 10.10.1.12 from the MA5600T/MA5603T.

Configuration File

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

save
```

1.4.3 Commissioning the Interconnection with the BRAS

This topic describes how to check whether the MA5600T/MA5603T can normally communicate with the BRAS. Working with the BRAS, the MA5600T/MA5603T can implement the authentication, accounting, and authorization (AAA) service.

Service Requirements

In the network as shown in **Figure 1-78**, the service requirements are as follows:

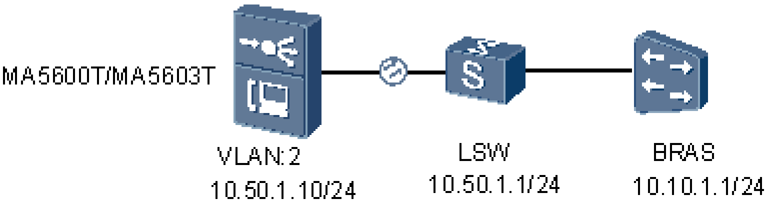
- The MA5600T/MA5603T uses the GIU board for upstream transmission.
- A static route is configured on the MA5600T/MA5603T for communicating with the BRAS.

- The requirements on the BRAS are as follows:
  - According to the authentication and accounting requirements for the users, you need to perform related configurations on the BRAS. For example, configure the access user domain (including the authentication scheme, accounting scheme, and authorization scheme that are bound to the domain) and specify the RADIUS server.
  - If the BRAS is used to authenticate users, you need to configure the user name and the password for each user on the BRAS. If the BRAS is used to allocate IP addresses, you must configure the corresponding IP address pool on the BRAS.

NOTE

For details about how to configure a LAN switch or the BRAS, see related configuration guides.

Figure 1-78 Example network for commissioning the interconnection with the BRAS



Procedure

Step 1 Configure a VLAN.

The VLAN ID is 2, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 2 smart
```

Step 2 Add an upstream port to the VLAN.

Upstream port 0/19/0 is added to VLAN 2.

```
huawei(config)#port vlan 2 0/19 0
```

NOTE

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

Step 3 Configure the IP address of the L3 interface.

The L3 interface IP address is 10.50.1.10/24, and this IP address must be in the same network segment as the gateway IP address (IP address of the router port that is connected to the MA5600T/MA5603T).

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.50.1.10 255.255.255.0
huawei(config-if-vlanif2)#quit
```

Step 4 Add a static route.

The destination IP address is 10.10.1.0/24 (the network segment of the BRAS), and the next-hop IP address is gateway IP address 10.50.1.1.

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

Step 5 Save the data.

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

----End

Result

After the MA5600T/MA5603T is interconnected with the BRAS successfully, you can ping IP address 10.10.1.1 from the MA5600T/MA5603T. After services are configured on the MA5600T/MA5603T, the authentication and accounting functions of the BRAS can be implemented.

Configuration File

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

save
```

1.4.4 Interconnection Commissioning of the MG Interface

The MG interface is a communication interface between the MA5600T/MA5603T and the MGC. Based on different control protocols between the MA5600T/MA5603T and the MGC, the MG interface can adopt the H.248 protocol or the MGCP protocol. The communication between the MA5600T/MA5603T and the MGC can be in the normal state and the services and functions can be implemented, only when the MG interface is in the normal state. This topic describes how to commission the interconnection between the MA5600T/MA5603T and the MGC.

Commissioning the Interconnection with the MG Interface(H.248)

This topic describes how to check whether the MG interface can normally communicate with the MGC through the H.248 protocol.

Service Requirements

In the network as shown in **Figure 1-79**, the service requirements are as follows:

- The MA5600T/MA5603T uses the H.248 protocol.
- The media IP address is the same as the signaling IP address, and the media stream and the signaling stream are transmitted upstream through the same Ethernet port on the GIU board.
- The media stream and the signaling stream use the default QoS policy for upstream transmission.
- Various terminals connected to the MG interface use the default TID profile, and the software parameters of the MG interface use the default settings.
- The MGC identifies the MG through the signaling IP address (IP address of the MG interface), and their communication packets do not contain any VLAN tag.

Figure 1-79 Example network for commissioning the interconnection with the MG interface (H.248)

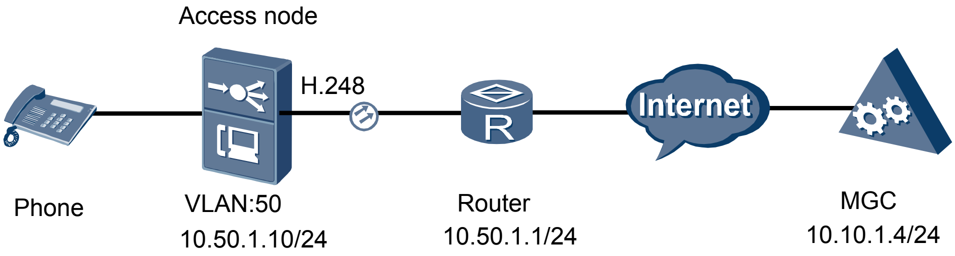
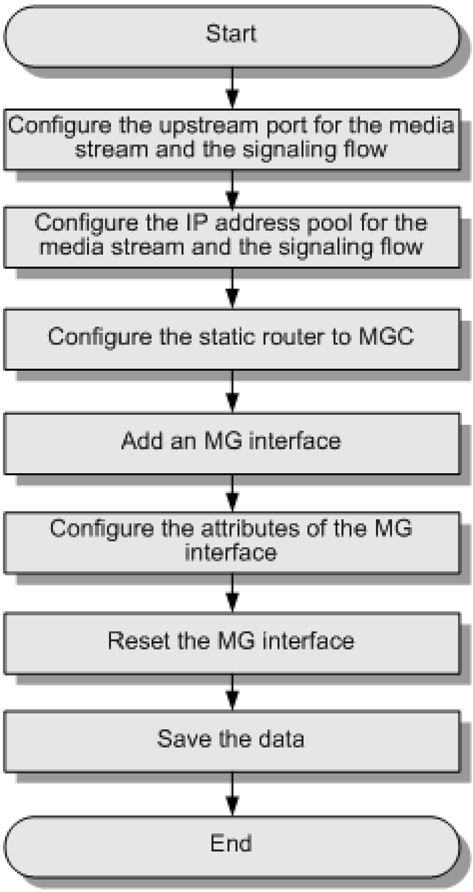


Figure 1-80 shows the flowchart for commissioning the interconnection with the MG interface (H.248).

Figure 1-80 Flowchart for commissioning the interconnection with the MG interface(H.248)


Start
Configure the upstream port for the media stream and the signaling flow
Configure the IP address pool for the media stream and the signaling flow
Configure the static router to MGC
Add an MG interface
Configure the attributes of the MG interface
Reset the MG interface
Save the data
End

Prerequisites

- The data configuration on the MGC side (corresponding to the data configuration on the MG side) must be correct.
- The current system must use the H.248 protocol.

NOTE

Run the **display protocol support** command to query the current voice protocol. If the voice protocol is not H.248, run the **protocol support** *h248* command to change it to H.248.

Procedure

Step 1 Configure the upstream VLAN interface for the media stream and the signaling stream.

The VLAN ID is 50, the VLAN type is smart VLAN, the upstream port is 0/19/0, and the IP address of the VLAN interface is 10.50.1.10/24.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
huawei(config)#interface vlanif 50
huawei(config-if-vlanif50)#ip address 10.50.1.10 24
huawei(config-if-vlanif50)#quit
```

NOTE

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

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.50.1.10/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.50.1.10 10.50.1.1
huawei(config-voip)#ip address signaling 10.50.1.10
huawei(config-voip)#quit
```

NOTE

When configuring the MG interface attributes, ensure that the media and signaling IP addresses exist in the corresponding address pools.

Step 3 Configure a static route to the MGC.

The IP address of the destination network segment of the static route to the MGC is 10.10.1.0/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 255.255.255.0 10.50.1.1
```

Step 4 Add an MG interface.

MG interface 0 that supports the H.248 protocol is added.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 5 Configure the attributes of the MG interface.

The media and signaling IP addresses of the MG interface are 10.50.1.10/24, the MG port ID is 2944, the coding mode is text, the transmission mode is UDP, the MG domain name is MA5600T/MA5603T.com, the IP address of the primary MGC is 10.10.1.4/24, the MGC port ID is 2944, and the start negotiation version of the H.248 is V2.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.50.1.10 mgport 2944 code text
transfer udp domainName
MA5600T/MA5603T.com primary-mgc-ip1 10.14.1.4 primary-mgc-port 2944 mg-media-ip1
10.50.1.10 start-negotiate-version 2
```

NOTE

The start negotiation version of the H.248 protocol for the MG interface must be the same as that on the MGC side.

Step 6 Reset the MG interface.

The MG interface is reset through cold start.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

Step 7 Save the data.

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

----End

Result

After the MG is interconnected with the MGC successfully, you can run the **display if-h248** *all* command to confirm that the MG interface is in the normal state.

```
huawei(config)#display if-h248 all
  ------------------------------------------------------------------------
  MGID   TransMode State    MGPort MGIP/DomainName MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------
  0      UDP       Normal   2944   10.50.1.10     2944    10.10.1.4
  ------------------------------------------------------------------------
```

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
interface vlanif 50
ip address 10.50.1.10 24

quit
voip
ip address media 10.50.1.10 10.50.1.1
ip address signaling 10.50.1.10
quit
ip route-static 10.10.1.0 255.255.255.0 10.50.1.1

interface h248 0
y
if-h248 attribute mgip 10.50.1.10 mgport 2944 code text transfer udp domainName
MA5600T/MA5603T.com primary-mgc-ip1 10.14.1.4 primary-mgc-port 2944 mg-media-ip1
10.50.1.10 start-negotiate-version 2

reset coldstart
y
quit
save
```

Commissioning the Interconnection with the MG Interface (MGCP)

This topic describes how to check whether the MG interface can normally communicate with the MGC through the MGCP protocol.

Service Requirements

In the network as shown in **Figure 1-81**, the service requirements are as follows:

- The MA5600T/MA5603T uses the MGCP protocol.
- The media IP address is the same as the signaling IP address (when the MGCP protocol is used, the media IP address must be the same as the signaling IP address), and the media stream and the signaling stream use the same Ethernet port on the GIU board for upstream transmission.
- The media stream and the signaling stream use the default QoS policy for upstream transmission.

- Various terminals connected to the MG interface use the default TID profile, and the software parameters of the MG interface use the default settings.
- The MGC identifies the MG through the signaling IP address (IP address of the MG interface), and their communication packets do not contain any VLAN tag.

Figure 1-81 Example network for the commissioning the interconnection with the MG interface (MGCP)

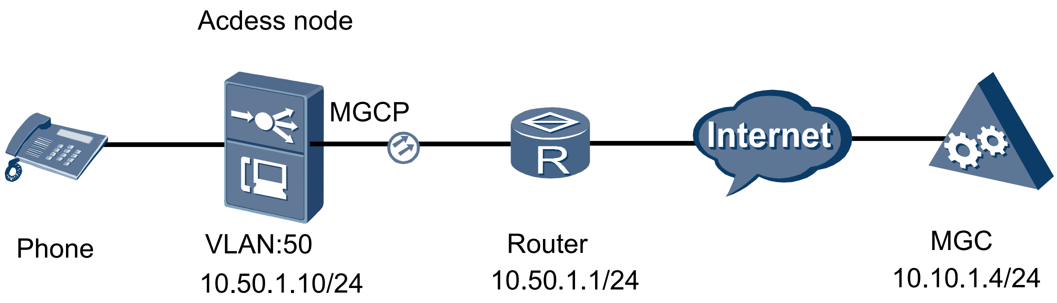
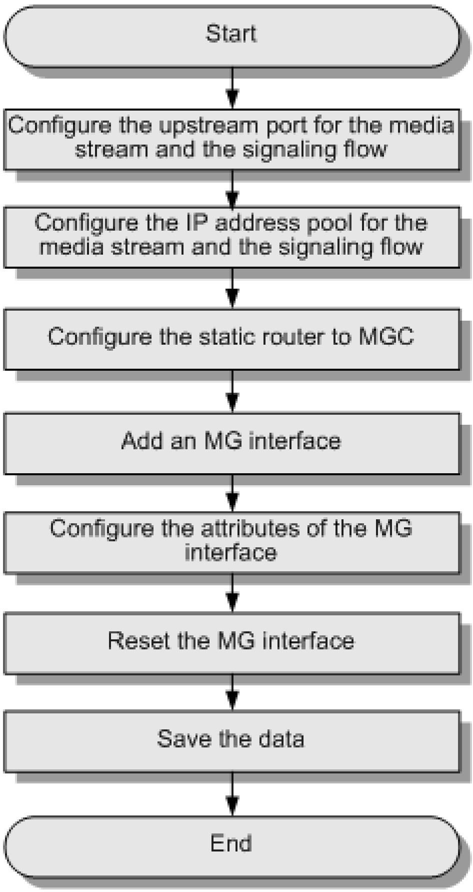


Figure 1-82 shows the flowchart for commissioning the interconnection with the MG interface (MGCP).

Figure 1-82 Flowchart for commissioning the interconnection with the MG interface (MGCP)


Start
Configure the upstream port for the media stream and the signaling flow
Configure the IP address pool for the media stream and the signaling flow
Configure the static router to MGC
Add an MG interface
Configure the attributes of the MG interface
Reset the MG interface
Save the data
End

Prerequisites

- The data configuration on the MGC side (corresponding to the data configuration on the MG side) must be correct.
- The current system must use the MGCP protocol.

  NOTE

  Run the **display protocol support** command to query the current voice protocol. If the voice protocol is not MGCP, run the **protocol support** *mgcp* command to change it to MGCP.

Procedure

Step 1 Configure the upstream VLAN interface for the media stream and the signaling stream.

The VLAN ID is 50, the VLAN type is smart VLAN, and the upstream port is 0/19/0, and the IP address of the VLAN interface is 10.50.1.10/24.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
huawei(config)#interface vlanif 50
huawei(config-if-vlanif50)#ip address 10.50.1.10 24
huawei(config-if-vlanif50)#quit
```

NOTE

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

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.50.1.10/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.50.1.10 10.50.1.1
huawei(config-voip)#ip address signaling 10.50.1.10
huawei(config-voip)#quit
```

NOTE

When configuring the MG interface attributes, ensure that the media and signaling IP addresses exist in the corresponding address pools.

Step 3 Configure a static route to the MGC.

The IP address of the destination network segment of the static route to the MGC is 10.10.1.0/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 255.255.255.0 10.50.1.1
```

Step 4 Add an MG interface.

MG interface 0 that supports the MGCP protocol is added.

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

Step 5 Configure the attributes of the MG interface.

The IP addresses of the MG interface is 10.50.1.10/24, the MG port ID is 2727, the coding mode is text (default setting), the transmission mode is UDP (default setting), the MG domain name is MA5600T/MA5603T.com, the IP address of the primary MGC is 10.10.1.4/24, and the MGC port ID is 2727.

```
huawei(config-if-mgcp-0)#if-mgcp attribute mgip 10.50.1.10 mgport 2727 domainName
MA5600T/MA5603T.com mgcip_1 10.10.1.4 mgcport_1 2727
```

Step 6 Reset the MG interface.

```
huawei(config-if-mgcp-0)#reset
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#quit
```

Step 7 Save the data.

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

----End

Result

After the MG is interconnected with the MGC successfully, you can run the **display if-mgcp** *all* command to confirm that the MG interface is in the normal state.

```
huawei(config)#display if-mgcp all
  --------------------------------------------------------------------------
  MGID     State          MGPort MGIP           MGCPort MGCIP/DomainName
  --------------------------------------------------------------------------
  0        Normal         2727   10.50.1.10     2727    10.14.1.4
  --------------------------------------------------------------------------
```

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
interface vlanif 50
ip address 10.50.1.10 24

quit
voip
ip address media 10.50.1.10 10.50.1.1
ip address signaling 10.50.1.10
quit
ip route-static 10.10.1.0 255.255.255.0 10.50.1.1

interface mgcp 0
y
if-mgcp attribute mgip 10.50.1.10 mgport 2727 domainName MA5600T/MA5603T.com
mgcip_1 10.14.1.4 mgcport_1 2727

reset
y
quit
save
```

1.4.5 Commissioning the Interconnection with the SIP Interface

This topic describes how to check whether the SIP interface can normally communicate with the IP multimedia subsystem (IMS) through the SIP protocol.

Service Requirements

In the network as shown in **Figure 1-83**, the service requirements are as follows:

- The MA5600T/MA5603T uses the SIP protocol.
- The media IP address is the same as the signaling IP address, and the media stream and the signaling stream are transmitted upstream through the same Ethernet port on the GIU board.
- The media stream and the signaling stream use the default QoS policy for upstream transmission.
- The IMS identifies the SIP interface through the signaling IP address (IP address of the SIP interface), and their communication packets do not contain any VLAN tag.

Figure 1-83 Example network for commissioning the interconnection with the SIP interface

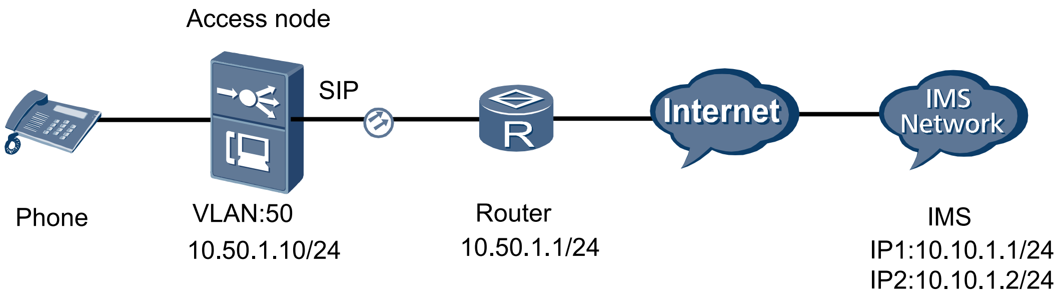
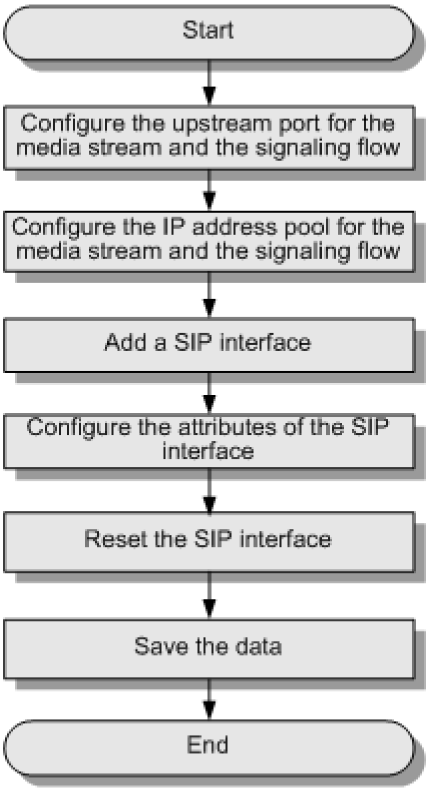


Figure 1-84 shows the flowchart for commissioning the interconnection with the SIP interface.

Figure 1-84 Flowchart for commissioning the interconnection with the SIP interface


Start
Configure the upstream port for the media stream and the signaling flow
Configure the IP address pool for the media stream and the signaling flow
Add a SIP interface
Configure the attributes of the SIP interface
Reset the SIP interface
Save the data
End

Prerequisites

- The data configuration on the IMS side (corresponding to the data configuration on the MA5600T/MA5603T side) must be correct.
- The current system must use the SIP protocol.

NOTE

Run the **display protocol support** command to query the current voice protocol. If the voice protocol is not SIP, run the **protocol support** *sip* command to change it to SIP.

Procedure

Step 1 Configure the upstream VLAN interface for the media stream and the signaling stream.

The VLAN ID is 50, the VLAN type is smart VLAN, the upstream port is 0/19/0, and the IP address of the VLAN interface is 10.50.1.10/24.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
huawei(config)#interface vlanif 50
huawei(config-if-vlanif50)#ip address 10.50.1.10 24
huawei(config-if-vlanif50)#quit
```

NOTE

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

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.50.1.10/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.50.1.10 10.50.1.1
huawei(config-voip)#ip address signaling 10.50.1.10
huawei(config-voip)#quit
```

NOTE

When configuring the SIP interface attributes, ensure that the media and signaling IP addresses exist in the corresponding address pools.

Step 3 Configure a static route to the IMS.

The IP address of the destination network segment of the static route to the IMS is 10.10.1.0/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 255.255.0.0 10.50.1.1
```

Step 4 Add a SIP interface.

SIP interface 0 is added.

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

Step 5 Configure the basic attributes of the SIP interface.

The media and signaling IP addresses of the SIP interface are 10.50.1.10/24, the signaling port ID is 5555, the transmission protocol is UDP (default setting), the IP address 1 of the primary proxy server is 10.10.1.1/24, the port ID of the primary proxy server is 5555, the IP address 1 of the secondary proxy server is 10.10.1.2/24, the port ID of the secondary proxy server is 5555, the home domain name is MA5600T/MA5603T.com, and the profile index is 0.

```
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.50.1.10 signal-ip
10.50.1.10 signal-port 5555 transfer udp primary-proxy-ip1 10.10.1.1 primary-proxy-
port 5555
secondary-proxy-ip1 10.10.1.2 secondary-proxy-port 5555 home-domain MA5600T/
MA5603T.com sipprofile-index 0
```

Step 6 Configure the optional attributes of the SIP interface.

The domain name of the SIP interface is huawei.com, and the phone context is +86755.

```
huawei(config-if-sip-0)#if-sip attribute optional mg-domain huawei.com phone-
context +86755
```

Step 7 Reset the SIP interface.

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

Step 8 Save the data.

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

----End

Result

After the SIP interface is interconnected with the IMS successfully, you can run the **display if-sip** *all* command to confirm that the SIP interface is in the normal state.

```
huawei(config)#display if-sip all
  --------------------------------------------------------
  MGID     TransMode State      SignalPort SignalIP
  --------------------------------------------------------
  0        UDP       Normal      5555       10.50.1.10
  --------------------------------------------------------
```

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
interface vlanif 50
ip address 10.50.1.10 24

quit
voip
ip address media 10.50.1.10 10.50.1.1
ip address signaling 10.50.1.10
quit
ip route-static 10.10.1.0 255.255.255.0 10.50.1.1

interface sip 0
y
if-sip attribute basic media-ip 10.50.1.10 signal-ip
10.50.1.10 signal-port 5555 transfer udp primary-proxy-ip1 10.10.1.1 primary-proxy-
port 5555
secondary-proxy-ip1 10.10.1.2 secondary-proxy-port 5555 home-domain MA5600T/
MA5603T.com sipprofile-index 0

if-sip attribute optional mg-domain huawei.com phone-context +86755

reset
y
quit
save
```

1.4.6 Commissioning the Management Channel Between the OLT and the GPON MDU

This topic describes how to commission the management channel between the MA5600T/MA5603T and the GPON MDU to ensure that you can log in to the GPON MDU using the MA5600T/MA5603T at the CO to remotely maintain and manage the GPON MDU.

Service Requirements

In the network as shown in **Figure 1-85**, the service requirements are as follows:

- A GPON port on the MA5600T/MA5603T is connected to 128 MDUs using an optical splitter.

  NOTE

  The following considers MDU 0 as an example for commissioning the management channel between the OLT and the GPON MDU.

- After the management channel between the MA5600T/MA5603T and the GPON MDU is set up, you can log in to the MDU using port 0/2/0 connected to the MDU to remotely maintain and manage the MDU.
- The DBA profile is used to limit the user rate to the fixed 10 Mbit/s bandwidth.

Figure 1-85 Example network for commissioning the management channel between the OLT and the GPON MDU

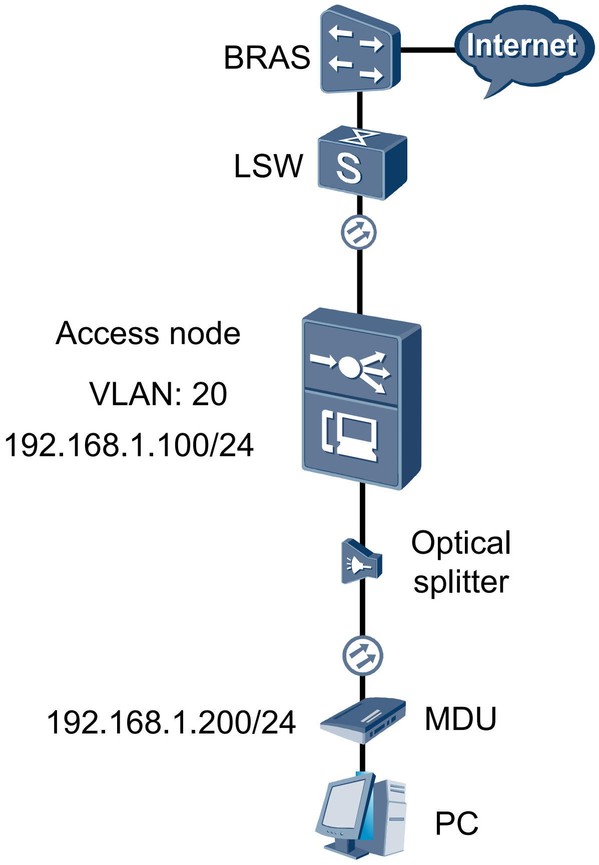
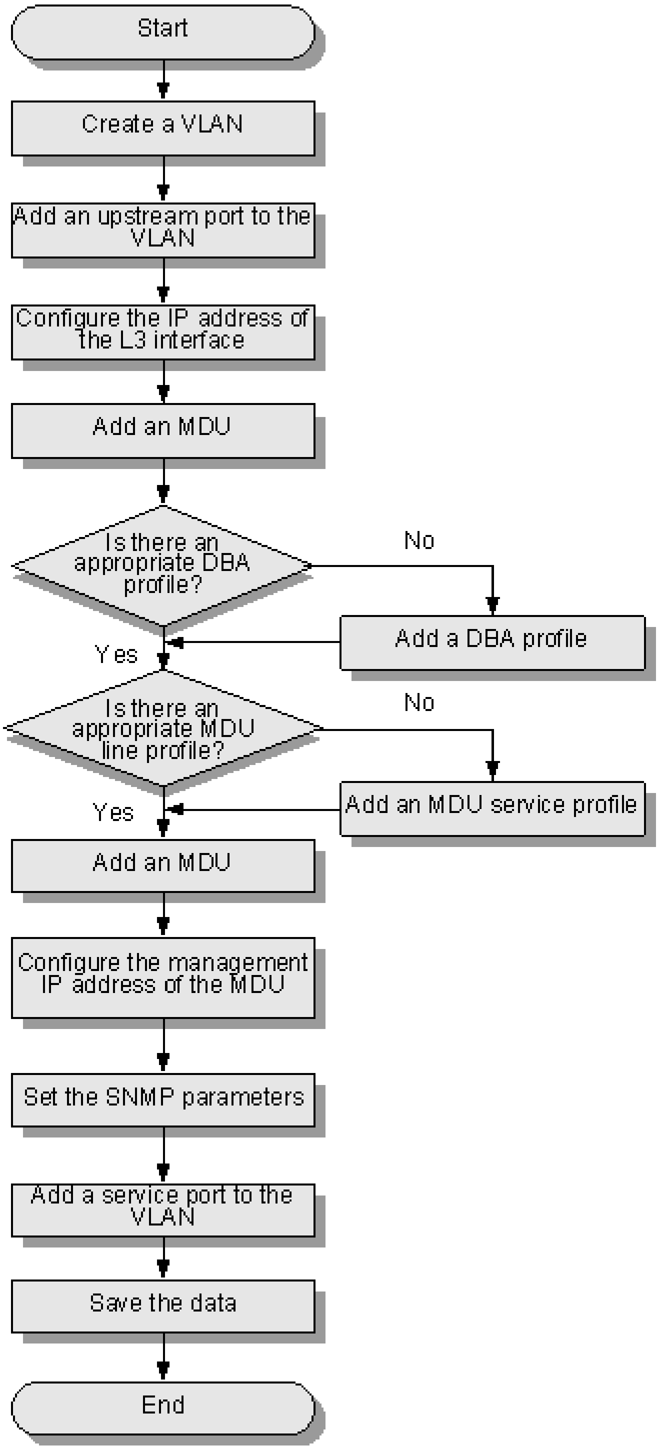


Figure 1-86 shows the flowchart for commissioning the management channel between the OLT and the GPON MDU.

Figure 1-86 Flowchart for commissioning the management channel between the OLT and the GPON MDU


Start
Create a VLAN
Add an upstream port to the VLAN
Configure the IP address of the L3 interface
Add an MDU
Is there an appropriate DBA profile?
No
Add a DBA profile
Yes
Is there an appropriate MDU line profile?
No
Add an MDU service profile
Yes
Add an MDU
Configure the management IP address of the MDU
Set the SNMP parameters
Add a service port to the VLAN
Save the data
End

Procedure

Step 1 Create a VLAN.

The VLAN ID is 20, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 20 smart
```

Step 2 Add an upstream port to the VLAN.

Upstream port 0/19/0 on the GIU board is added to VLAN 20.

```
huawei(config)#port vlan 20 0/19 0
```

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

The Layer 3 IP address is 192.168.1.100/24.

```
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 192.168.1.100 255.255.255.0
huawei(config-if-vlanif20)#quit
```

Step 4 Add a DBA profile.

The DBA profile ID is 12, the DBA profile uses the default name DBA-profile_12, the bandwidth type is type1 (fixed bandwidth), and the user rate is the fixed 10 Mbit/s bandwidth.

NOTE

- The bandwidth type and the attribute of the DBA profile must be compatible with the service to be carried.
- The system supports five DBA profile types, namely, type1 (fixed bandwidth), type2 (assured bandwidth), type3 (assured bandwidth+maximum bandwidth), type4 (maximum bandwidth), and type5 (fixed bandwidth+assured bandwidth+maximum bandwidth).
- By default, the system provides DBA profiles 1 to 9, each of which provides typical values for traffic parameters. By default, T-CONT 0 is bound with DBA profile 1.
- The value of the bandwidth you input when adding the DBA profile rounds down to the nearest integer multiple of 64. For example, if the input bandwidth value is 1022 kbit/s, the actual bandwidth is 960 kbit/s.
- You can run the **display dba-profile** command to query the information about the DBA profile.

```
huawei(config)#dba-profile add profile-id 12 type1 fix 10240
```

Step 5 Configure an MDU line profile.

The MDU line profile ID is 5, T-CONT 1 is bound with DBA profile 12, GEM port 0 is bound to T-CONT 1, the service type is ETH, and the mapping mode is VLAN mapping.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 12
huawei(config-gpon-lineprofile-5)#gem add 0 eth tcont 1
huawei(config-gpon-lineprofile-5)#gem mapping 0 0 vlan 20
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

Step 6 Add an MDU.

MDU 0 is connected to GPON port 0, the MDU authentication mode is the SN authentication, the SN is 32303131B39FD641, the management protocol is SNMP, and MDU profile 5 is bound to MDU 0.

NOTE

You can add an MDU in the following two ways: confirming an auto-discovered MDU and adding an MDU offline. Here, the method of adding an MDU offline is considered as an example.

You can also run the **port ont-auto-find** command to enable the function of auto-discovering an MDU, and then run the **ont confirm** command to confirm the auto-discovered MDU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 0 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 5
```

Step 7 Configure the management IP address of the MDU.

The management IP address is 192.168.1.200/24, and the ID of the native VLAN to which the MDU port belongs is 20.

```
huawei(config-if-gpon-0/2)#ont ipconfig 0 0 static ip-address 192.168.1.200 mask
255.255.255.0 vlan 20
huawei(config-if-gpon-0/2)#quit
```

Step 8 Set the SNMP parameters.

Configure the SNMP profile 10. That, the SNMP version is SNMP V2C, the read community name is **public**, and the write community name is **private**, the IP address of the U2000 is **10.10.1.10/24**, the port is 162, the parameter security name is **user1** (the parameter security name is the write community name), the gateway IP address is 192.168.1.101.

```
huawei(config)#snmp-profile add profile-id 10 v2c public
private 10.10.1.10 162 private
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont snmp-profile 0 0 profile-id 10
huawei(config-if-gpon-0/2)#ont snmp-route 0 0 ip-address 10.10.1.10 mask
255.255.255.0 next-hop 192.168.1.101
huawei(config-if-gpon-0/2)#quit
```

Step 9 Add a service port to the VLAN.

```
huawei(config)#service-port vlan 20 gpon 0/2/0 ont 0 gemport 0 multi-service user-
vlan 20
```

Step 10 Save the data.

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

----End

Result

After the commissioning is complete, you can remotely maintain and manage the MDU using **telnet 192.168.1.200**.

Configuration File

```
vlan 20 smart
port vlan 20 0/19 0
interface vlanif 20
ip address 192.168.1.100 255.255.255.0

quit
dba-profile add profile-id 12 type1 fix 10240

ont-lineprofile gpon profile-id 5

tcont 1 dba-profile-id 12
gem add 0 eth tcont 1

gem mapping 0 0 vlan 20

commit
quit
interface gpon 0/2
ont add 0 0 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 5

ont ipconfig 0 0 static ip-address 192.168.1.200 mask 255.255.255.0 vlan 20

quit
snmp-profile add profile-id 10 v2c public private 10.10.1.10 162 private
interface gpon 0/2
ont snmp-profile 0 0 profile-id 10
ont snmp-route 0 0 ip-address 10.10.1.10 mask 255.255.255.0 next-hop 192.168.1.101
quit
service-port vlan 20 gpon 0/2/0 ont 0 gemport 0 multi-service user-vlan 20

save
```

1.4.7 Commissioning the Management Channel Between the OLT and the GPON ONT

This topic describes how to commission the GPON OLT to ensure that the service configuration and centralized management of the GPON ONTs are performed on the GPON OLT using the ONT Management and Control Interface (OMCI) protocol.

Service Requirements

In the network as shown in **Figure 1-87**, the service requirements are as follows:

- A GPON port on the MA5600T/MA5603T is connected to 128 ONTs using an optical splitter.

  NOTE

  The following considers ONT 0 as an example for commissioning the management channel between the OLT and the GPON ONT.
- On the MA5600T/MA5603T, you can configure ONTs at different locations in a centralized manner.
- The DBA profile is used to ensure the maximum bandwidth of 10Mbit/s and the traffic profile is used to limit subscriber rates.

Figure 1-87 Example network for commissioning the management channel between the OLT and the GPON ONT

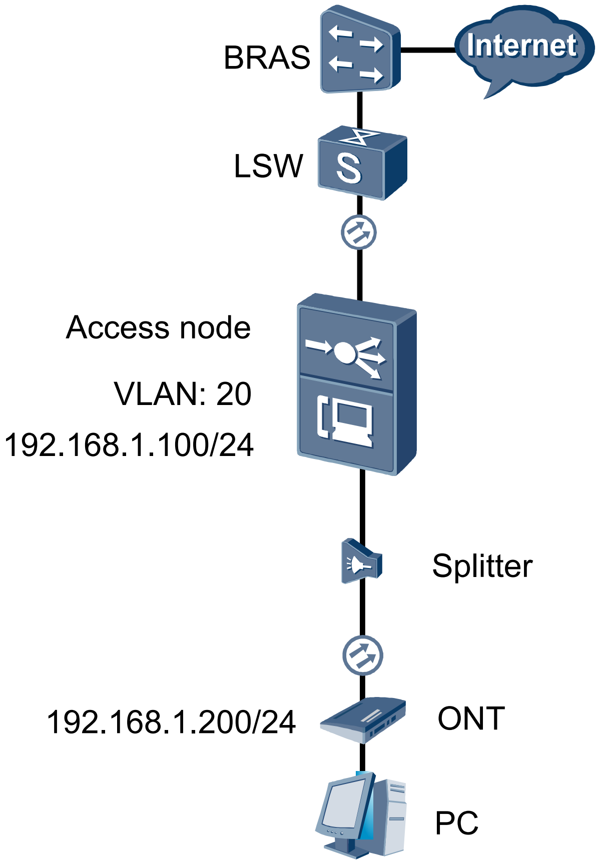
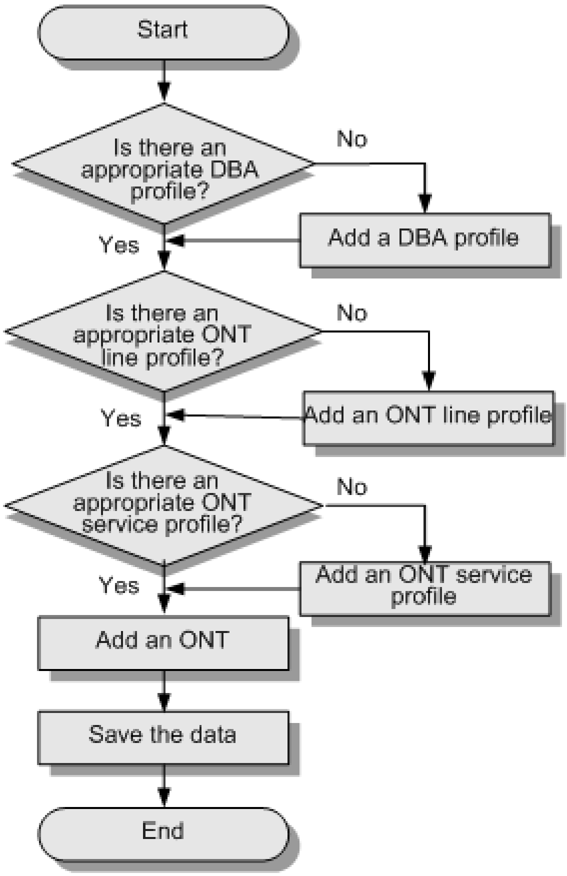


Figure 1-88 shows the flowchart for commissioning the management channel between the OLT and the GPON ONT.

Figure 1-88 Flowchart for commissioning the management channel between the OLT and the GPON ONT


Start
Is there an appropriate DBA profile?
No
Add a DBA profile
Yes
Is there an appropriate ONT line profile?
No
Add an ONT line profile
Yes
Is there an appropriate ONT service profile?
No
Add an ONT service profile
Yes
Add an ONT
Save the data
End

Procedure

Step 1 Add a DBA profile.

The DBA profile ID is 12, the DBA profile uses the default name DBA-profile_12, the bandwidth type is type1 (fixed bandwidth), and the user rate is the fixed 10 Mbit/s bandwidth.

NOTE

- The bandwidth type and the attribute of the DBA profile must be compatible with the service to be carried.
- The system supports five DBA profile types, namely, type1 (fixed bandwidth), type2 (assured bandwidth), type3 (assured bandwidth+maximum bandwidth), type4 (maximum bandwidth), and type5 (fixed bandwidth+assured bandwidth+maximum bandwidth).
- By default, the system provides DBA profiles 1 to 9, each of which provides typical values for traffic parameters. By default, T-CONT 0 is bound with DBA profile 1.
- The value of the bandwidth you input when adding the DBA profile rounds down to the nearest integer multiple of 64. For example, if the input bandwidth value is 1022 kbit/s, the actual bandwidth is 960 kbit/s.
- You can run the **display dba-profile** command to query the information about the DBA profile.

```
huawei(config)#dba-profile add profile-id 12 type1 fix 10240
```

Step 2 Add an ONT line profile.

The ONT line profile ID is 5, T-CONT 1 is bound with DBA profile 12, GEM port 0 is bound to T-CONT 1, the service type is ETH, and the mapping mode is VLAN mapping.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 12
huawei(config-gpon-lineprofile-5)#gem add 0 eth tcont 1
huawei(config-gpon-lineprofile-5)#gem mapping 0 0 vlan 20
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

Step 3 Add an ONT service profile.

The ONT service profile ID is 10, the quantity of Ethernet ports on the ONT is 4, the quantity of POTS ports on the ONT is 2, and Ethernet ports 1-4 are added to VLAN 20.

NOTE

The port capability set in the ONT service profile must be the same as the actual ONT capability set.

```
huawei(config)#ont-srvprofile gpon profile-id 10
huawei(config-gpon-srvprofile-10)#ont-port eth 4 pots 2
huawei(config-gpon-srvprofile-10)#port vlan eth 1-4 20
huawei(config-gpon-srvprofile-10)#commit
huawei(config-gpon-srvprofile-10)#quit
```

Step 4 Add an ONT.

ONT 0 is connected to GPON port 0, the ONT authentication mode is the SN authentication, the SN is 323031314D4B2041, the management protocol is OMCI, and ONT line profile 5 and ONT service profile 10 are bound to ONT 0.

NOTE

You can add an ONT in the following two ways: confirming an auto-discovered ONT and adding an ONT offline. Here, the method of adding an ONT offline is considered as an example.

You can also run the **port ont-auto-find** command to enable the function of auto-discovering an ONT, and then run the **ont confirm** command to confirm the auto-discovered ONT.

```
huawei(config)#interface gpon 0/2

huawei(config-if-gpon-0/2)#ont add 0 0 sn-auth 323031314D4B2041 omci ont-
lineprofile-id 5 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#quit
```

Step 5 Save the data.

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

----End

Result

After the commissioning is complete, you can maintain and manage the ONT on the MA5600T/MA5603T (For example, run the **ont deactivate** command to deactivate the ONT that is in the activated state).

Configuration File

```
vlan 20 smart
port vlan 20 0/19 0
interface vlanif 20
ip address 192.168.1.100 255.255.255.0

quit
dba-profile add profile-id 12 type1 fix 10240
```

```
ont-lineprofile gpon profile-id 5

tcont 1 dba-profile-id 12
gem add 0 eth tcont 1

gem mapping 0 0 vlan 20

commit
quit
interface gpon 0/2
ont add 0 0 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 5

ont ipconfig 0 0 static ip-address 192.168.1.200 mask 255.255.255.0 vlan 20

quit
service-port vlan 20 gpon 0/2/0 ont 0 gemport 0 multi-service user-vlan 20

save
```

1.4.8 Commissioning the Management Channel to the xDSL CPE

This topic describes how to commission the CPE management function of the MA5600T/MA5603T to ensure that you can log in to the CPE from the DSLAM at the CO to remotely maintain and manage the CPE.

Service Requirements

In the network as shown in **Figure 1-89**, the service requirements are as follows:

- The maintenance terminal is connected to the maintenance Ethernet port of the MA5600T/MA5603T.
- After the management channel between the DSLAM and the CPE is set up, you can log in to the CPE using port 0/2/0 connected to the CPE to remotely maintain and manage the CPE.
- The user access mode is IPoA.

Figure 1-89 Example network for managing the CPE

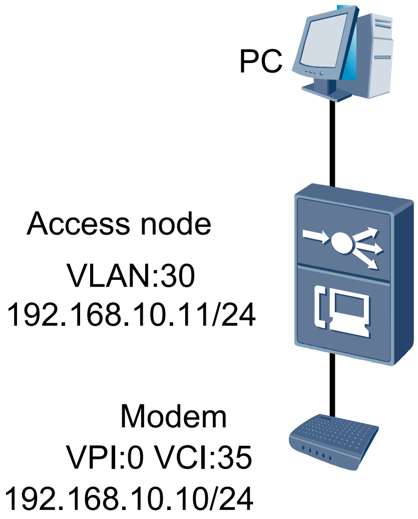
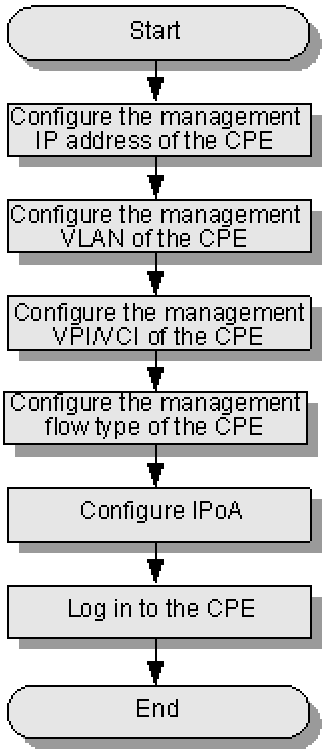


Figure 1-90 shows the flowchart for commissioning the management channel to the CPE.

Figure 1-90 Flowchart for commissioning the management channel to the CPE


Start
Configure the management IP address of the CPE
Configure the management VLAN of the CPE
Configure the management VPI/VCI of the CPE
Configure the management flow type of the CPE
Configure IPoA
Log in to the CPE
End

Prerequisites

You must be logged in to the MA5600T/MA5603T using the maintenance terminal.

Procedure

Step 1 Configure the management IP address of the CPE.

The management IP address of the CPE is 192.168.10.10/24.

```
huawei(config)#cpe-management ip-address 192.168.10.10
```

Step 2 Configure the management VLAN of the CPE.

The VLAN ID is 30, the VLAN type is smart VLAN, and the IP address of the VLAN L3 interface is 192.168.10.11/24.

```
huawei(config)#vlan 30 smart
huawei(config)#cpe-management vlan 30
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 192.168.10.11 24
huawei(config-if-vlanif30)#quit
```

Step 3 Configure the management VPI and VCI of the CPE.

The management VPI ID is 0, and the management VCI ID is 35.

```
huawei(config)#cpe-management vpi 0 vci 35
```

Step 4 Configure the management flow type of the CPE.

The management flow type is vlan-ethertype ipoe.

```
huawei(config)#cpe-management flow-type vlan-ethertype ipoe
```

Step 5 Configure IPoA.

Configure MAC address pool 0 with the start address 0000-0000-0001.

```
huawei(config)#mac-pool 0 0000-0000-0001
```

Enable the IPoA protocol conversion function.

```
huawei(config)#ipoa enable
```

Set the IPoA default gateway.

```
huawei(config)#ipoa default gateway 10.1.1.1
```

Step 6 Log in to the CPE.

```
huawei(config)#cpe-management telnet 0/2/0
```

----End

Result

You can log in to the CPE from the MA5600T/MA5603T using the maintenance terminal to maintain and manage the CPE.

Configuration File

```
cpe-management ip-address 192.168.10.10
vlan 30 smart
cpe-management vlan 30
interface vlanif 30
ip address 192.168.10.11 24
quit

cpe-management vpi 0 vci 35
cpe-management flow-type vlan-ethertype ipoe
mac-pool 0 0000-0000-0001

ipoa enable
ipoa default gateway 10.1.1.1
cpe-management telnet 0/2/0
```

1.5 Maintenance and Management Commissioning

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

1.5.1 Configuring the System Energy-Saving Function

This topic describes how to power off a board that is not configured with any services for a long time to reduce the system power and therefore to reduce the system energy consumption.

Prerequisites

NOTE

Only the MA5600T supports this operation.

The board must support the power-off mode and the energy-saving mode.

Context

Energy-saving modes include the manual energy-saving mode and automatic energy-saving mode.

- Manual energy-saving mode (powering off a board manually). You can manually power off an unused board in the subrack according to the plan for the energy-saving purpose. When the service is provisioned from the OSS server to a board that is powered off, the system prompts that the board is currently powered off. In this case, you can manually power on the board according to the prompt.
- Automatic energy-saving mode (automatically powering off a board). When the automatic energy-saving mode is enabled, the system supports a series of energy-saving measures according to the referenced energy-saving profile. These measures include the following: battery energy saving, shutting down unused boards, putting unused xDSL ports to sleep mode and shutting down the laser on unused xPON ports. An energy-saving profile is a set of energy-saving measures. The system provides three typical energy-saving profiles. You can query the profiles but cannot modify, rename, or delete them. The three typical profiles are as follows:
  - Standard energy-saving profile **standard**, with ID 1. It is the default energy-saving profile in the system. In this profile, all the energy-saving measures are disabled.
  - Basic energy-saving profile **basic**, with ID 2. In this profile, some energy-saving measures that do not affect the current services are enabled, such as:
    - Shutting down unused boards
    - Shutting down the laser on unused xPON ports and putting unused xDSL ports to sleep mode
  - Deep energy-saving profile **deep**, with ID 3. In this profile, all the energy-saving measures are enabled, and the battery energy saving may affect the service running.
- To power on a board that is powered off manually, you must run the **board power-on** command to manually power it on.
- You can recover the power supply of the board that is automatically powered off in the following two ways:
  - Run the **board power-on** command to power on the board.
  - Remove the board from the slot that is automatically powered off, and the system determines that the board is offline and then recovers the power supply of the slot. After the power supply is recovered, reinstall the board.

Procedure

- Set the manual energy-saving mode.
  1. Run the **board power-off** command to manually power off a board.
- Set the automatic energy-saving mode.
  1. Run the spm-profile command to create an energy-saving profile. By default, the system uses the standard energy-saving profile. That is, the energy-saving mode is disabled by default. You can enable the required energy-saving measure according to actual requirements.
     - Run the battery energy-saving command to set the status of the mains monitoring module and battery energy saving.
     - Run the unused-port shutdown command to set energy saving for unused ports.
     - Run the unused-slot shutdown command to set energy saving for unused boards.

2. Run the **system energy-saving mode** command to set the used energy-saving profile.
3. Run the **display system energy-saving mode** command to query the used energy-saving profile.

----End

Result

The system is referenced to an energy-saving profile (that is, the unused board is shut down). If a board is not used 15 minutes after it is confirmed and functions properly, the board is powered off automatically.

Example

To reference energy-saving profile 4 to enable the system energy-saving function, do as follows: Assume that battery energy saving is enabled and energy saving for unused boards is enabled.

```
huawei(config)#spm-profile profile-id 4
huawei(config-spm-prof-4)#unused-slot shutdown enable
huawei(config-spm-prof-4)#battery energy-saving ac-monitor emuid 1 digitalid 6
huawei(config-spm-prof-4)#battery energy-saving enable
huawei(config-spm-prof-4)#quit
huawei(config)#system energy-saving mode profile-id 4
huawei(config)#display system energy-saving mode
  Current spm-profile id  : 4
  Current spm-profile name: spm_profile_4
```

1.5.2 Checking Alarms and Events

This topic describes how to check the alarm and event reporting function of the device.

Verifying the Alarm and Event Function

This topic describes how to verify the alarm and event function by triggering various alarms and events through the related operations.

Verifying Operation

Table 1-47 lists the operations for verifying the alarm and event function.

Table 1-47 Operations for verifying the alarm and event function

Operation	Description
Remove a service board.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the service board back into the slot.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Remove the optical fiber connected to an optical port.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the optical fiber back into the optical port.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.

Operation	Description
Remove the optical fiber connected to an optical port when an ONT is online.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the optical fiber back into the optical port.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Open the cabinet door.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Close the cabinet door.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Remove the fan tray from the shelf.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the fan tray back into the shelf.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Perform the active/standby switchover of the control boards.	Log in to the system, and run the **display event history** command to check whether the active/standby switchover event history exists.

Querying Alarms and Events

This topic describes how to query history alarms and events through the maintenance terminal.

Context

Up to 1001 latest fault alarms and recovery alarms, and 901 event alarms can be saved in the system. If the record table is full, and a new alarm or event is generated, the new alarm or event overwrites the oldest record in the record table. You can query the records that have been overwritten in the NMS database.

The CLI provides multiple ways to query history alarms and events.

Table 1-48 lists the commands for querying history alarms.

Table 1-48 Commands for querying history alarms

To...	Run the Command...
Query alarms by alarm SN	**display alarm history alarmsn** *sn* [**detail** | **list**]
Query alarms by alarm ID	**display alarm history alarmid** *id* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm type	**display alarm history alarmtype** *type* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm class	**display alarm history alarmclass** *class* [**detail** | **list** | **start-number** *number*]

To...	Run the Command...
Query alarms by alarm level	**display alarm history alarmlevel** *level* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm time	**display alarm history alarmtime start** *start-date start-time* **end** *end-date end-time* [*start-number number*] [**detail** | **list** | **start-number** *number*]
Query alarms by alarm parameter	**display alarm history alarmparameter** { *frameid/slotid/portid* | *frameid/slotid* | *frameid* | **vlanif** *vlanif* } [**detail** | **list**]
Query all the latest alarms	**display alarm history all** [**detail** | **list**]

Table 1-49 lists the commands for querying history events.

Table 1-49 Commands for querying history events

To...	Run the Command...
Query events by event SN	**display event history eventsn** *sn* [**detail** | **list**]
Query events by event ID	**display event history eventid** *id* [**detail** | **list** | **start-number** *number*]
Query events by event type	**display event history eventtype** *type* [**detail** | **list** | **start-number** *number*]
Query events by event class	**display event history eventclass** *class* [**detail** | **list** | **start-number** *number*]
Query events by event level	**display event history eventlevel** *level* [**detail** | **list** | **start-number** *number*]
Query events by event time	**display event history eventtime start** *start-date start-time* **end** *end-date end-time* [*start-number number*] [**detail** | **list** | **start-number** *number*]
Query events by event parameter	**display event history eventparameter** { *frameid/slotid/portid* | *frameid/slotid* | *frameid* | **vlanif** *vlanif* } [**detail** | **list**]
Query all the latest events	**display event history all** [**detail** | **list**]

Procedure

Step 1 Perform an operation (such as inserting and removing a board) to generate an alarm or event.

Step 2 Run the **display alarm history** command to query history alarms.

Step 3 Run the **display event history** command to query history events.

----End

Result

You can query the alarm or event triggered by the operation you have performed.

Example

To query the history environment alarms by alarm type, do as follows:

```
huawei>display alarm history alarmtype
{ type<E><communication,service,process,equipment,environment> }:environment
{ <cr>|detail<K>|list<K>|start-number<U><1,1900>||<K> }:list
{ <cr>||<K> }:

  Command:
          display alarm history alarmtype environment list
  ----------------------------------------------------------------------
  AlarmSN  Date&Time                Alarm Name/Para
  ----------------------------------------------------------------------
  777      2009-08-21 10:18:29      The system resources usage recovers from
                                    the overload state to the normal state
                                    Resource Name: CPU, Current Percent: 70
  765      2009-08-21 10:17:29      The system resources usage exceeds the
                                    threshold
                                    Resource Name: CPU, Current Percent: 86
  764      2009-08-21 10:17:29      The system resources usage recovers from
                                    the overload state to the normal state
                                    Resource Name: CPU, Current Percent: 86
  714      2009-08-20 15:04:35      The system resources usage recovers from
                                    the overload state to the normal state
                                    Resource Name: CPU, Current Percent: 72
  705      2009-08-20 15:03:35      The system resources usage exceeds the
                                    threshold
                                    Resource Name: CPU, Current Percent: 86
  704      2009-08-20 15:03:35      The system resources usage recovers from
                                    the overload state to the normal state
---- More ( Press 'Q' to break ) ----
```

To query the history events by event date, and the start date is 2009-08-24, the star time is 16:00:00, the end date is 2009-08-24, and the end time is 18:00:00, do as follows:

```
huawei>display event history
{ all<K>|eventclass<K>|eventid<K>|eventlevel<K>|eventparameter<K>|eventsn<K>|eve
nttime<K>|eventtype<K> }:eventtime
{ start<K> }:start
{ start-date<D><yyyy-mm-dd> }:2009-08-24
{ start-time<T><hh:mm:ss> }:16:00:00
{ end<K> }:end
{ end-date<D><yyyy-mm-dd> }:2009-08-24
{ end-time<T><hh:mm:ss> }:18:00:00
{ <cr>|detail<K>|list<K>|start-number<U><1,1900>||<K> }:list
{ <cr>||<K> }:

  Command:
          display event history eventtime start 2009-08-24 16:00:00 end 2009-08-
24 18:00:00 list
  ----------------------------------------------------------------------
  EventSN  Date&Time                Event Name/Para
  ----------------------------------------------------------------------
  35346    2009-08-24 17:59:40      Backing up files fails from the host to
                                    the maintenance terminal
                                    FrameID: 0, SlotID: 9, Position: -1,
                                    Backup type: Host data, Backup Object:
                                    Active control board, Failure cause: Failed
                                    to transfer the file
  35345    2009-08-24 17:58:52      Change of Maintenance User's State
                                    User name: test01, Log mode: Telnet, IP:
                                    10.71.42.55, State: Log on
  35344    2009-08-24 17:58:47      Change of Maintenance User's State
                                    User name: test01, Log mode: Telnet, IP:
                                    10.71.42.55, State: Log off
  35343    2009-08-24 17:58:24      Backing up files starts from the host to
                                    the maintenance terminal
                                    FrameID: 0, SlotID: 9, Position: -1,
                                    Backup type: Host data, Backup Object:
---- More ( Press 'Q' to break ) ----
```

1.5.3 Checking the Log

If a fault occurs on the device, you can locate the fault by querying the log.

Procedure

Step 1 Perform an operation (such as adding a board) through the CLI.

Step 2 In the user mode, run the **display log** command to query the records in the log.

----End

Result

You can query the log record generated by the operation you have performed.

Example

To query the log records of all users within the period from 10:00:00 on 2009-08-24 to 18:00:00 on 2009-08-24, do as follows:

```
huawei>display log
{ all<K>|cli<K>|failure<K>|index<K>|memory<K>|name<K>|snmp<K> }:all
{ <cr>|start-date<D><yyyy-mm-dd> }:2009-08-24
{ -<K>|<cr>|start-time<T><hh:mm:ss> }:10:00:00
{ -<K>|<cr> }:-
{ end-date<D><yyyy-mm-dd> }:2009-08-24
{ <cr>|end-time<T><hh:mm:ss> }:18:00:00

  Command:
          display log all 2009-08-24 10:00:00 - 2009-08-24 18:00:00
  ---------------------------------------------------------------------------
  No.   UserName                                Domain           IP-Address
    65  test03                                  --               10.71.42.55
  Time: 2009-08-24 17:14:48
  Cmd:  switch language-mode
  ---------------------------------------------------------------------------
  No.   UserName                                Domain           IP-Address
    64  private                                 --               10.78.217.35
  Time: 2009-08-24 17:08:08
  Cmd:
  Index1: hwFrameIndex: 0
  Index2: hwSlotIndex: 9
  hwBackupServerIpAddr: 10.78.217.35
  hwBackupMode: 3
  hwBackupFileName: /bmsuser/7341374.poz
  hwBackupContent: 68
  hwBackupUserNam  ...
  ---------------------------------------------------------------------------
  No.   UserName                                Domain           IP-Address
    63  private                                 --               10.78.217.35
---- More ( Press 'Q' to break ) ----
```

1.5.4 Checking the System Switchover

After the active/standby switchover is performed, the services of the active control board are switched to the standby control board. This ensures that the services run in the normal state.

Prerequisites

- An active control board and a standby control board must be configured on the device, and the cables must be connected correctly on the boards.
- The patch status of the active and standby control boards must be consistent with the hardware environment.

Precautions

- If the data of the active and standby control boards is not completely synchronized, the system prohibits the active/standby switchover.

  NOTE

  Run the **display data sync state** command to query the data synchronization status of the active and standby control boards.
- When the communication between the active and standby control boards fails or the standby control board is faulty, the system prohibits the active/standby switchover.
- When the data is being loaded, saved, or backed up, the system prohibits the active/standby switchover.

Context

Classification of the active/standby switchover:

According to the status of the data synchronization, the active/standby switchover is classified into the normal switchover and forced switchover.

- Normal switchover: Refers to the active/standby switchover that is performed when the data is synchronized sufficiently. A normal switchover does not cause links to break or boards to reset.
- Forced switchover: Refers to the active/standby switchover that is performed when the data is not synchronized sufficiently.

  The following data might be synchronized insufficiently:

  - Configuration data.

    When the configuration data is not fully synchronized, the system prohibits performing forced switchover by running the active/standby switchover command. Other forced switching methods, such as manually resetting the active control board or removing the active control board, cause loss of basic data or the system to reset.

    Therefore, when the configuration data is not fully synchronized, it is recommended that you do not perform the forced switchover. You can choose to reset the system. In this manner, the system can return to the normal state in a short period.
  - Basic data.

    When the basic data is not fully synchronized, the system prohibits performing forced switchover by running the active/standby switchover command. Other forced switching methods, such as manually resetting the active board or removing the active control board, neither reset the system nor affect the database, but they may cause service boards to reset.

- Dynamic data.

  When certain dynamic data is not fully synchronized, the system permits performing forced switchover by running the active/standby switchover command. After the switchover, the on-going services continue to run in the normal state, and the original connections, alarms, and logs are not lost.

Procedure

Step 1 Run the **save** command to save the data.

Step 2 Run the **system switch-over** command to perform the active/standby switchover.

----End

Result

When the ACT LED on the original standby control board is on, log in to the system through this control board. It is found that the system runs in the normal state.

Example

After the data is saved, perform the active/standby switchover.

```
huawei#save
{ <cr>|configuration<K>|data<K> }:

  Command:
          save

huawei#
  It will take several minutes to save configuration file, please wait...

huawei#
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated

huawei#
  The data is being saved, please wait a moment...
huawei(config)#system switch-over
  Are you sure to switch over? (y/n)[n]:y
```

1.6 Supplementary Information

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

1.6.1 Script Making

Before the commissioning, you can collect the information such as the data plan according to **1.2.4 Planning Data** to make a commissioning script. Then, configure the basic data of the device by loading the script. This ensures that the device works in the normal state, which facilitates the commissioning of the basic functions and services of the device.

Script Overview

The basic configuration through the script includes but is not limited to the following items:

- Adding the power board
- Configuring the environment monitoring unit (including the FAN and the ESC)
- Configuring the route protocol

NOTE

For details about how to load the script, see **1.3.7 Loading a Configuration Script**.

Example Script

Table 1-50 lists the data plan of an example script. After the example script is configured, you can log in to the MA5600T/MA5603T through the maintenance terminal in the management center to commission the basic functions of the device.

Table 1-50 Script data plan

Item	Data
PRTE power board	Slot IDs: 0/21 and 0/22
FAN	● SN: 0 ● Sub-node ID: 1 (default) ● Name: FAN ● Fan speed adjustment mode: automatic
ESC	● SN: 1 ● Sub-node ID: 15 (default) ● Name: H801ESC
Route protocol	● Upstream port: 0/19/0 ● Management VLAN ID: 100; type: Standard VLAN ● IP address of the L3 interface of the management VLAN: 10.50.1.10/24 ● Gateway address: 10.50.1.1/24 ● IP address of the target network segment: 10.10.1.10/24

The following displays the commands that need to be included in the script according to the preceding data plan.

CAUTION

Each command in the script must end with a carriage return (CR).

```
enable
config
board add 0/21 H801PRTE
board add 0/22 H801PRTE
emu add 0 FAN 0 1 FAN
interface emu 0
fan speed mode automatic
```

```
quit
emu add 1 H801ESC 0 15 H801ESC
vlan 100 standard
port vlan 100 0/19 0
interface vlanif 100
ip address 10.50.1.10 24

quit
ip route-static 10.10.1.0 24 10.50.1.1


save
```

1.6.2 Configuring the File Transfer Mode

This topic describes how to configure the file transfer mode of the FTP,SFTP, Xmodem and TFTP. You are advised to use SFTP mode.

Configuring the FTP Transfer Mode

This topic describes how to configure the FTP transfer mode for transferring (uploading or downloading) files through the inband or outband Ethernet port of the MA5600T/MA5603T. After the configuration, the FTP server and the MA5600T/MA5603T can communicate to transfer files in the FTP mode.

Prerequisites

- The Ethernet port of the FTP server is directly connected to the inband or outband Ethernet port of the MA5600T/MA5603T.
  - Connect to the inband Ethernet port (Upstream port) through the crossover cable.
  - Connect to the outband Ethernet port (Maintenance port) through the direct cable.
- You have logged in to the MA5600T/MA5603T through Telnet from the console (maintenance terminal), and have entered the global config mode.

Tools, Meters, and Materials

- Crossover cable
- Direct cable

Impact on System

None

Precautions

Make sure that the crossover cable is used to directly connect the FTP server to the MA5600T/MA5603T. In other cases, a straight through cable is used.

Procedure

Step 1 On the FTP server, configure the IP address of its Ethernet port.

Configure the Ethernet port IP address of the FTP server according to the IP address planning in the specific networking, and ensure that the Ethernet port of the FTP server and the inband or outband Ethernet port of the MA5600T/MA5603T can ping each other.

For example, if the Ethernet port of the FTP server is directly connected to the MA5600T/MA5603T, the IP address of this Ethernet port and the IP address of the inband or outband Ethernet port of the MA5600T/MA5603T must be in the same subnet.

Step 2 On the FTP server, run the FTP application and set related parameters.

After running the FTP application, set the path for saving the file, FTP user name, and password.

Step 3 (This is step is used for setting the FTP user attributes for the manual file transfer.) On the MA5600T/MA5603T, run the **ftp set** command to set the FTP user name and password.

```
huawei(config)#ftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
```

NOTE

By default, the FTP user name is **anonymous** and the password is **anonymous@huawei.com** in the MA5600T/MA5603T system.

Step 4 (Optional; this step is required when the function of database file auto-backup is used.) On the MA5600T/MA5603T, run the **file-server auto-backup data** command to configure the FTP user name, password, and port ID.

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 ftp path test user
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
```

----End

Reference

- Any PC that runs the FTP software can serve as an FTP server.
- In the FTP file transfer mode, the user name and the password must be authenticated. Apart from setting the user name and password on the FTP server, you also need to set the FTP user name and password on the FTP client (such as the MA5600T/MA5603T), and make sure that the settings at both ends are the same.

Configuring the SFTP Transfer Mode

This topic describes how to configure the SFTP transfer mode for transferring (uploading or downloading) files through the inband or outband Ethernet port of the MA5600T/MA5603T. After the configuration, the SFTP server and the MA5600T/MA5603T can communicate to transfer files in the SFTP mode.

Prerequisites

- The Ethernet port of the SFTP server is directly connected to the inband or outband Ethernet port of the MA5600T/MA5603T.
  - Connect to the inband Ethernet port (Maintenance port) through the crossover cable.
  - Connect to the outband Ethernet port (Upstream port) through the direct cable.
- You have logged in to the MA5600T/MA5603T through Telnet from the console (maintenance terminal), and have entered the global config mode.

Tools, Meters, and Materials

- Crossover cable
- Direct cable

Impact on System

None

Precautions

Make sure that the crossover cable is used to directly connect the SFTP server to the MA5600T/MA5603T. In other cases, a straight through cable is used.

Procedure

Step 1 On the SFTP server, configure the IP address of its Ethernet port.

Configure the Ethernet port IP address of the SFTP server according to the IP address planning in the specific networking, and ensure that the Ethernet port of the SFTP server and the inband or outband Ethernet port of the MA5600T/MA5603T can ping each other.

For example, if the Ethernet port of the SFTP server is directly connected to the MA5600T/MA5603T, the IP address of this Ethernet port and the IP address of the inband or outband Ethernet port of the MA5600T/MA5603T must be in the same subnet.

Step 2 On the SFTP server, run the SFTP application and set related parameters.

After running the SFTP application, set the path for saving the file, SFTP user name, password, and port ID. The port ID is 22 by default.

Step 3 (This is step is used for setting the SFTP user attributes for the manual file transfer.) On the MA5600T/MA5603T, run the **ssh sftp set** command to set the SFTP user name, password, and port ID.

```
huawei(config)#ssh sftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
  Listening Port(0--65535):22
```

NOTE

The MA5600T/MA5603T system does not have default SFTP user name, password, or port ID.

Step 4 (Optional; this step is required when the function of database file auto-backup is used.) On the MA5600T/MA5603T, run the **file-server auto-backup data** command to configure the SFTP user name, password, and port ID.

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 sftp path test port
22 user
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
```

NOTE

The MA5600T/MA5603T system does not have default SFTP user name, password, or port ID.

----End

Reference

- Any PC that runs the SFTP software can serve as an SFTP server.
- In the SFTP file transfer mode, the user name and the password must be authenticated. Apart from setting the user name, password, and port ID on the SFTP server, you also need to set the SFTP user name, password, and port ID on the SFTP client (such as the MA5600T/MA5603T), and make sure that the settings at both ends are the same.

Configuring Xmodem File Transfer Mode

This topic describes how to configure the Xmodem file transfer mode. To upload or download files through the maintenance serial port on the MA5600T/MA5603T, configure the Xmodem file transfer mode according to this operation guide. Then, the console and the MA5600T/MA5603T can communicate with each other normally and transfer files in Xmodem mode.

Prerequisites

You must be logged in to the MA5600T/MA5603T from the console (also called maintenance terminal) through the serial port, and must enter the global config mode.

Tools, Meters, and Materials

RS-232 serial port cable (used for logging in to the MA5600T/MA5603T from the console through the serial port)

Impact on the System

None

Precautions

NOTE

- The speed of transferring files in Xmodem mode through the serial port is limited. Therefore, the system does not support file transfer in the Xmodem mode for large-size files such as program packet files and configuration files.
- It is recommended to transfer files through other modes as much as possible, such as TFTP, even if file transfer in the Xmodem mode is supported.

- The baud rate of the serial port on the MA5600T/MA5603T must be the same as the baud rate of the serial port on the console.
- The Xmodem transfer mode is applicable to only the active control board.
- Telnet users are prohibited from transferring files in Xmodem mode.

Procedure

Step 1 Query the baud rate of the serial port on the MA5600T/MA5603T.

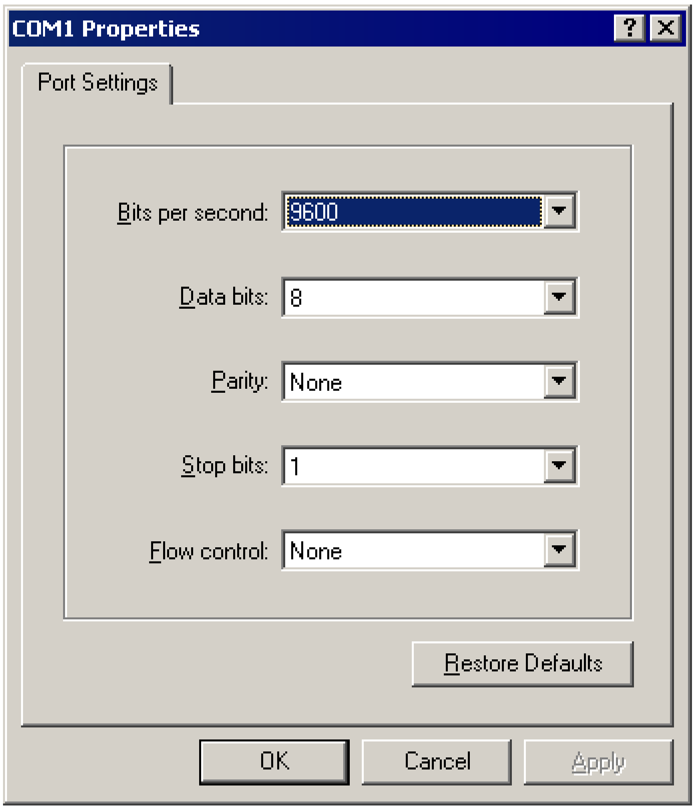
```
huawei(config)#display baudrate
  Current active serial baudrate: 9600 bps
```

Step 2 (This step is optional but is required when you reconfigure the baud rate of the serial port.) Run the **baudrate** command on the MA5600T/MA5603T to configure the baud rate of the serial port on the MA5600T/MA5603T. The high baud rate can increase the transmission speed.

For example, reconfigure the baud rate on the MA5600T/MA5603T to 9600 bit/s:

```
huawei(config)#baudrate 9600
```

Step 3 Open the HyperTerminal on the console to configure the baud rate of the serial port on the console to be the same as the baud rate on the MA5600T/MA5603T.



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

----End

Configuring the TFTP Transfer Mode

This topic describes how to configure the TFTP transfer mode for transferring (uploading or downloading) files through the inband or outband Ethernet port of the MA5600T/MA5603T. After the configuration, the TFTP server and the MA5600T/MA5603T can communicate to transfer files in the TFTP mode.

Prerequisites

- The Ethernet port of the TFTP server is directly connected to the inband or outband Ethernet port of the MA5600T/MA5603T.
  - Connect to the inband Ethernet port (Maintenance port) through the crossover cable.
  - Connect to the outband Ethernet port (Upstream port) through the direct cable.
- You have logged in to the MA5600T/MA5603T through Telnet from the console (maintenance terminal), and have entered the global config mode.

Tools, Meters, and Materials

- Crossover cable
- Direct cable

Impact on System

None

Precautions

Make sure that the crossover cable is used to directly connect the TFTP server to the MA5600T/MA5603T. In other cases, a straight through cable is used.

Procedure

Step 1 On the TFTP server, configure the IP address of its Ethernet port.

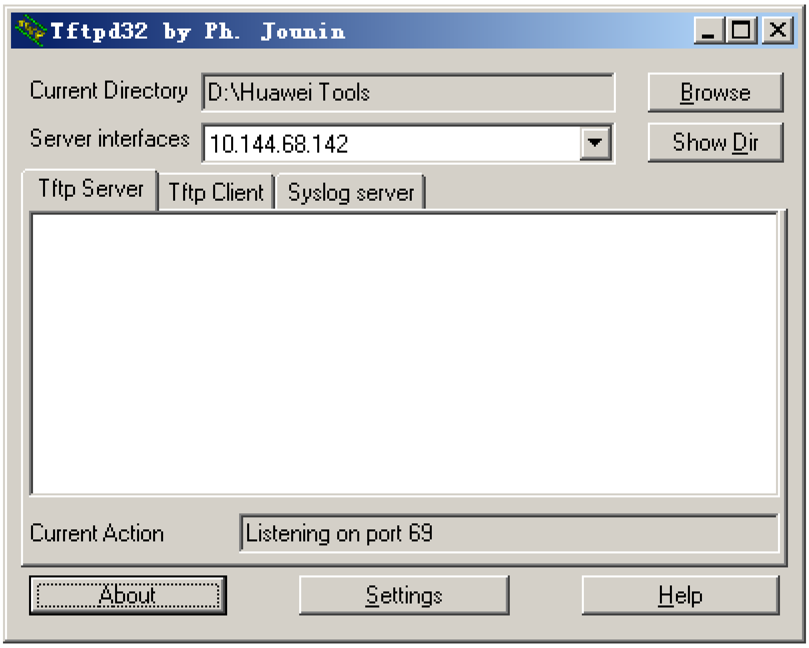
Configure the Ethernet port IP address of the TFTP server according to the IP address planning in the specific networking, and ensure that the Ethernet port of the TFTP server and the inband or outband Ethernet port of the MA5600T/MA5603T can ping each other.

For example, if the Ethernet port of the TFTP server is directly connected to the MA5600T/MA5603T, the IP address of this Ethernet port and the IP address of the inband or outband Ethernet port of the MA5600T/MA5603T must be in the same subnet.

Step 2 On the TFTP server, run the TFTP application and set related parameters.

1. After the TFTP application is run on the TFTP server, an interface as shown in **Figure 1-91** is displayed. In the **Server interfaces** drop-down list, select the IP address that is set in step 1.

Figure 1-91 TFTP main interface



Tftpd32 by Ph. Jounin

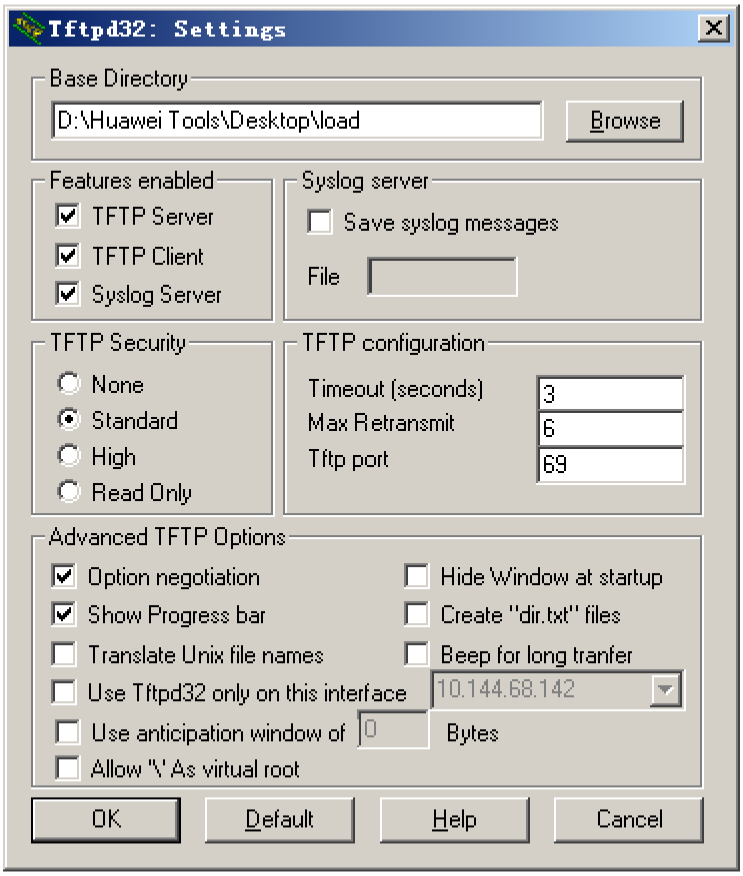
Current Directory: D:\Huawei Tools

Server interfaces: 10.144.68.142

Current Action: Listening on port 69

2. In the interface as shown in **Figure 1-91**, click **Settings**.
3. In the dialog box that is displayed, click **Browse** to select the path for saving the file, as shown in **Figure 1-92**.

Figure 1-92 Setting TFTP parameters



Tftpd32: Settings

Base Directory: D:\Huawei Tools\Desktop\load

Features enabled:
- ☑ TFTP Server
- ☑ TFTP Client
- ☑ Syslog Server

Syslog server:
- ☐ Save syslog messages
- File:

TFTP Security:
- ○ None
- ● Standard
- ○ High
- ○ Read Only

TFTP configuration:
- Timeout (seconds): 3
- Max Retransmit: 6
- Tftp port: 69

Advanced TFTP Options:
- ☑ Option negotiation
- ☐ Hide Window at startup
- ☑ Show Progress bar
- ☐ Create "dir.txt" files
- ☐ Translate Unix file names
- ☐ Beep for long tranfer
- ☐ Use Tftpd32 only on this interface: 10.144.68.142
- ☐ Use anticipation window of 0 Bytes
- ☐ Allow '\' As virtual root

----End

Reference

- Any PC that runs the TFTP software can serve as a TFTP server.
- The IP address in the **Server interfaces** drop-down list is the IP address of the TFTP server. The TFTP application can identify the IP address automatically. If the TFTP server has multiple IP addresses, select the correct one.
- If the TFTP file transfer fails, check the following items:
  - Whether the selected IP address of the TFTP server is correct.
  - Whether the TFTP server can ping the inband or outband Ethernet port of the MA5600T/MA5603T (run the **Ping** command).
  - Whether the TFTP application is run on the TFTP server.
  - Whether the path is correctly set in the TFTP application.
  - Whether the TFTP file transfer function has been enabled through the command.
  - Whether the entered name of the file to be transferred is correct.

1.6.3 Software Package Settings

This topic provides the default software package settings of the MA5600T/MA5603T.

Factory Default of the xDSL Line Profile

The following **Table 1-51**, **Table 1-52**, **Table 1-53** list the factory defaults of the xDSL line profile on the MA5600T/MA5603T.

Table 1-51 ADSL line profile

Profile Index	Profile	Parameter	Factory Default

1	DEFVAL	Transmission mode	T1.413
			ETSI
			G.992.1(Annex A/B/C)
			G.992.2(Annex A/C)
			G.992.3(Annex A/B/I/J/L/M)
			G.992.4(Annex A/I)
			G.992.5(Annex A/B/I/J/M)

		Trellis mode	Enable
		Bit swap downstream	Enable
		Bit swap upstream	Enable
		Form of transmit rate adaptation downstream	AdaptAtStartup
		Form of transmit rate adaptation upstream	AdaptAtStartup
		Target SNR margin downstream (0.1dB)	60
		Minimum SNR margin downstream (0.1dB)	0
		Maximum SNR margin downstream(0.1dB)	160
		Target SNR margin upstream (0.1dB)	60
		Minimum SNR margin upstream (0.1dB)	0
		Maximum SNR margin upstream (0.1dB)	160
		Allow transition to idle	not allowed
		Allow transition to low power	not allowed
		L0 time(second)	255
		Layer 2 time(second)	30

<table>
<tr><th>Profile Index</th><th>Profile</th><th colspan="2">Parameter</th><th>Factory Default</th></tr>
<tr><td rowspan="13"></td><td rowspan="13"></td><td colspan="2">Layer 3 time(second)</td><td>255</td></tr>
<tr><td colspan="2">Maximum aggregate transmit power reduction(dB)</td><td>3</td></tr>
<tr><td colspan="2">Total maximum aggregate transmit power reduction(dB)</td><td>9</td></tr>
<tr><td colspan="2">INM inter arrival time offset downstream(symbol):</td><td>3</td></tr>
<tr><td colspan="2">INM inter arrival time step downstream</td><td>0</td></tr>
<tr><td colspan="2">INM cluster continuation value downstream(symbol)</td><td>0</td></tr>
<tr><td colspan="2">INM equivalent INP mode downstream</td><td>0</td></tr>
<tr><td rowspan="5"><defmode></td><td>Maximum nominal transmit PSD downstream(-0.1dBm)</td><td>400</td></tr>
<tr><td>Maximum nominal transmit PSD upstream (-0.1dBm)</td><td>380</td></tr>
<tr><td>Maximum nominal aggregate transmit power downstream(0.1dBm)</td><td>200</td></tr>
<tr><td>Maximum nominal aggregate transmit power upstream(0.1dBm)</td><td>125</td></tr>
<tr><td>Upstream PSD mask selection</td><td>ADLU-32/EU-32</td></tr>
<tr><td colspan="2">Network timing reference clock mode</td><td>FreeRun</td></tr>
</table>

Table 1-52 VDSL line profile

Profile Index	Profile	Parameter	Factory Default

1	DEFVAL	Transmission mode	T1.413
			G.992.1(Annex A/B/C)
			G.992.2(Annex A/C)
			G.992.3(Annex A/B/I/J/L/M)
			G.992.4(Annex A/I)
			G.992.5(Annex A/B/I/J/M)
			G.993.2(Annex A/B/C)

		Bit swap downstream	Enable
		Bit swap upstream	Enable
		Form of transmit rate adaptation downstream	AdaptAtStartup
		Form of transmit rate adaptation upstream	AdaptAtStartup
		Target SNR margin downstream(0.1dB)	60
		Minimum SNR margin downstream(0.1dB)	0
		Maximum SNR margin downstream (0.1dB)	300
		Target SNR margin upstream(0.1dB)	60
		Minimum SNR margin upstream(0.1dB)	0
		Maximum SNR margin upstream(0.1dB)	300
		UPBO US1 band reference PSD parameters [a, b]	1650,1020
		UPBO US2 band reference PSD parameters [a, b]	1650,615
		UPBO US3 band reference PSD parameters [a, b]	0,0
		UPBO US4 band reference PSD parameters [a, b]	0,0
		UPBO Boost Mode	Enable
		UPBO US1 band reference electrical length	0
		UPBO US2 band reference electrical length	0

Profile Index	Profile	Parameter		Factory Default
		UPBO US3 band reference electrical length		0
		UPBO US4 band reference electrical length		0
		UPBO use of electrical length to compute UPBO		Auto
		Allow transition to idle		not allowed
		Allow transition to low power		not allowed
		L0 time(second)		255
		Layer 2 time(second)		30
		Layer 3 time(second)		255
		Maximum aggregate transmit power reduction(dB)		3
		Total maximum aggregate transmit power reduction(dB)		9
		<defmode>	G.993.2 profile	Profile12a
			VDSL2 PSD class mask	AnnexB998-M2x-B (B8-6)
			VDSL2 link use of U0	Unused
			Maximum nominal aggregate transmit power downstream (0.1dBm)	145
			Maximum nominal aggregate transmit power upstream (0.1dBm)	145
			Upstream PSD mask selection	ADLU-32/EU-32
			Virtual noise mode downstream	Disable
			Virtual noise mode upstream	Disable
		Network timing reference clock mode		FreeRun
		INM inter arrival time offset downstream (symbol)		3
		INM inter arrival time step downstream		0
		INM cluster continuation value downstream (symbol)		0
		INM equivalent INP mode downstream		0

Profile Index	Profile	Parameter	Factory Default
		INM inter arrival time offset upstream (symbol)	3
		INM inter arrival time step upstream	0
		INM cluster continuation value upstream (symbol)	0
		INM equivalent INP mode upstream	0
		SOS time Window downstream(64ms)	0
		Minimum percentage of degraded tones downstream	0
		Minimum number of normalized CRC anomalies downstream(0.02)	65535
		Maximum number of SOS downstream	0
		SNR margin offset of ROC downstream (0.1dB)	0
		Minimum impulse noise protection of ROC downstream	0
		SOS time Window upstream(64ms)	0
		Minimum percentage of degraded tones upstream	0
		Minimum number of normalized CRC anomalies upstream(0.02)	65535
		Maximum number of SOS upstream	0
		SNR margin offset of ROC upstream (0.1dB)	0
		Minimum impulse noise protection of ROC upstream	0

Table 1-53 SHDSL line profile

Profile Index	Profile	Parameter	Factory Default
1	DEFVAL	Path mode	ATM
		G.SHDSL interface mode of line	two wire
		G.SHDSL minimum line rate (unit:kbps)	2048

Profile Index	Profile	Parameter	Factory Default
		G.SHDSL maximum line rate (unit:kbps)	2048
		PSD	symmetric
		Transmission mode	all
		Remote enable	enabled
		Probe enable	disabled
		Downstream current target SNR margin	6
		Downstream worst target SNR margin	0
		Upstream current target SNR margin	6
		Upstream worst target SNR margin	0
		Target SNR margin used bitmap	0x5
		Reference times	0

Factory Defaults of the xDSL Alarm Profile

The following **Table 1-54**, **Table 1-55**, **Table 1-56** list the factory defaults of the xDSL alarm profile on the MA5600T/MA5603T.

Table 1-54 ADSL alarm profile

Profile Index	Profile	Parameter		Factory Default
1	DEFVAL	CO	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
		CPE	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0

Profile Index	Profile	Parameter		Factory Default
			The number of unavailable seconds	0
			The number of failed full initialization	0
			The number of failed short initialization	0

Table 1-55 VDSL alarm profile

Profile Index	Profile	Parameter		Factory Default
1	DEFVAL	CO	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
		CPE	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
		The number of failed full initialization		0
		The number of full initialization		0

Table 1-56 SHDSL alarm profile

Profile Index	Profile	Parameter	Factory Default
1	DEFVAL	Loop attenuation threshold (unit:dB)	0
		SNR margin threshold (unit:dB)	0
		ES threshold (unit:second)	0

Profile Index	Profile	Parameter	Factory Default
		SES threshold (unit:second)	0
		CRC anomaly threshold	0
		LOSWS threshold (unit:second)	0
		UAS threshold (unit:second)	0
		Dying gasp alarm switch	Enable
		Reference status	Unused

Default settings of the system parameters

The following table lists the default settings of the system parameters on the MA5600T/MA5603T.

Table 1-57 System parameters

Index	Description	Default
0	Sending howler tone flag, 0:not send, 1:send	1
1	Overseas version flag, 0:China, 1:HongKong, 2:Brazil, 3:Egypt, 4:Singapore, 5:Thailand, 6:France, 7:Britain MSFUK, 8:Britain ETSI, 9:Bulgaria	0
2	Stop initial ringing flag, 0:not send, 1:send	0
3	The mode of voicemail, 0:high voltage, 1:FSK and ring, 2:FSK no ring	1
4	Global digitmap support flag 0:Not support, 1:Support	1
5	Transfer mode of media stream in a device, 0:Device internal forwarding, 1:Device external forwarding	0
6	RTP 2833 Payload Type	97

Default settings of the overseas parameters

The following table lists the default settings of the overseas parameters on the MA5600T/MA5603T.

Table 1-58 Overseas parameters

Index	Description	Default
0	Hooking upper threshold(ms), reference: China:350, HongKong:800	350
1	Hooking lower threshold(ms), reference: China:100, HongKong:100	100
2	Flag of applying PARKED LINE FEED or not when user port is locked, 0:not apply, 1:apply	0

Factory Defaults of a DBA Profile

The following table lists the factory defaults of a DBA profile on the MA5600T/MA5603T.

Table 1-59 DBA profile

Profile Index	Profile Name	Default	
1	Profile-name	dba-profile_1	
	Profile-ID	1	
	type	1	
	Bandwidth compensation	No	
	Fix(kbps)	5120	
	Assure(kbps)	0	
	Max(kbps)	0	
	2	Profile-name	dba-profile_2
Profile-ID		2	
type		1	
Bandwidth compensation		No	
Fix (kbps)		1024	
Assure (kbps)		0	

Profile Index	Profile Name	Default	
Max (kbps)		0	
3		Profile-name	dba-profile_3
	Profile-ID	3	
	type	4	
	Bandwidth compensation	No	
	Fix(kbps)	0	
	Assure(kbps)	0	
	Max(kbps)	32768	
	4	Profile-name	dba-profile_4
Profile-ID		4	
type		1	
Bandwidth compensation		No	
Fix (kbps)		1024000	
Assure (kbps)		0	
Max (kbps)		0	
5		Profile-name	dba-profile_5
	Profile-ID	5	
	type	1	
	Bandwidth compensation	No	
	Fix(kbps)	32768	
	Assure(kbps)	0	
	Max(kbps)	0	
	6	Profile-name	dba-profile_6

Profile Index	Profile Name	Default	
Profile-ID		6	
type		1	
Bandwidth compensation		No	
Fix (kbps)		102400	
Assure (kbps)		0	
Max (kbps)		0	
7		Profile-name	dba-profile_7
	Profile-ID	7	
	type	2	
	Bandwidth compensation	No	
	Fix(kbps)	0	
	Assure(kbps)	32768	
	Max(kbps)	0	
	8	Profile-name	dba-profile_8
Profile-ID		8	
type		2	
Bandwidth compensation		No	
Fix (kbps)		0	
Assure (kbps)		102400	

Profile Index	Profile Name	Default	
Max (kbps)		0	
9		Profile-name	dba-profile_9
	Profile-ID	9	
	type	3	
	Bandwidth compensation	No	
	Fix(kbps)	0	
	Assure(kbps)	32768	
	Max(kbps)	65536	

Default settings of the GPON ONT line profile

The following table lists the default settings of the GPON ONT line profile on the MA5600T/ MA5603T.

Table 1-60 GPON ONT line profile

Parameter Name	Default
FEC upstream switch	Disable
Qos mode	PQ
Mapping mode	VLAN
<T-CONT 0>	DBA Profile-ID:1

Default settings of the GPON ONT service profile

The following table lists the default settings of the GPON ONT service profile on the MA5600T/ MA5603T.

Table 1-61 GPON ONT service profile

Parameter Name		Default	
Port-type	POTS	Port-number	0
	ETH		0
	TDM		0

Parameter Name		Default	
	MOCA		0
	CATV		0
TDM port type		E1	
TDM service type		TDMoGem	
MAC learning function switch		Enable	
ONT transparent function switch		Disable	
Multicast forward mode		Unconcern	
Multicast forward VLAN		-	
Multicast mode		Unconcern	
Upstream IGMP packet forward mode		Unconcern	
Upstream IGMP packet forward VLAN		-	

Factory Defaults of a GPON ONT Alarm Profile

The following table lists the factory defaults of a GPON ONT alarm profile on the MA5600T/MA5603T.

Table 1-62 GPON ONT alarm profile

Profile Index	Profile	Parameter	Factory Default
1	alarm-profile_1	GEM port loss of packets threshold	0
		GEM port misinserted packets threshold	0
		GEM port impaired blocks threshold	0
		Ethernet FCS errors threshold	0
		Ethernet excessive collision count threshold	0
		Ethernet late collision count threshold	0
		Too long Ethernet frames threshold	0
		Ethernet buffer (Rx) overflows threshold	0

Profile Index	Profile	Parameter	Factory Default
		Ethernet buffer (Tx) overflows threshold	0
		Ethernet single collision frame count threshold	0
		Ethernet multiple collisions frame count threshold	0
		Ethernet SQE count threshold	0
		Ethernet deferred transmission count threshold	0
		Ethernet internal MAC Tx errors threshold	0
		Ethernet carrier sense errors threshold	0
		Ethernet alignment errors threshold	0
		Ethernet internal MAC Rx errors threshold	0
		PPPOE filtered frames threshold	0
		MAC bridge port discarded frames due to delay threshold	0
		MAC bridge port MTU exceeded discard frames threshold	0
		MAC bridge port received incorrect frames threshold	0
		CES general error time threshold	0
		CES severely time threshold	0
		CES bursty time threshold	0
		CES controlled slip time threshold	0
		CES unavailable time threshold	0
		Drop events threshold	0
		Undersize packets threshold	0
		Fragments threshold	0
		Jabbers threshold	0
		Failed signal of ONU threshold (Format:1e-x)	3

Profile Index	Profile	Parameter	Factory Default
		Degraded signal of ONU threshold (Format:1e-x)	4

Default settings of the environment monitoring units

Tables Table 1-63, Table 1-64 list the default settings of the environment monitoring units on the MA5600T/MA5603T.

Table 1-63 Default settings of the H801ESC board

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

Parameter	Default
	Definition of user-defined alarm indexes 1: AC voltage; 2: AC switch; 3: battery voltage; 4: battery fuse; 5: load fuse; 6: rectifier unit; 7: secondary power supply; 8: door status of the cabinet; 9: door status of the equipment room; 10: window; 11: theft; 12: MDF; 13: fan; 14: fire; 15: smoke; 16: water; 17: diesel; 18: abnormal smell 19: air conditioner; 20: lightning arrester; 21: user-defined alarms of digital parameters

Table 1-64 Default settings of the FAN

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

Table 1-65 Default settings of the TCU

Parameter	Default
Sub-node	7

2 Basic Configurations

About This Chapter

Basic configurations mainly include certain common configurations, public configurations, and pre-configurations in service configurations. There is no obvious logical relation between basic configurations. You can perform basic configurations according to actual requirements.

2.1 Configuring Alarms
Alarm management includes the following functions: alarm record, alarm setting, and alarm statistics. These functions help you to maintain the device and ensure that the device works efficiently.

2.2 Configuring the Clock
On a digital network comprising the MA5600T and other devices, the primary problem to be solved is clock synchronization for carrying the traditional TDM service. To ensure the system clock synchronization of each device in the digital network, a system clock source must be specified.

2.3 Configuring the Network Time
Configure the NTP protocol to keep the time of all devices in the network synchronized, so that the MA5600T/MA5603T implements various service applications based on universal time, such as the network management system and the network accounting system.

2.4 Adding Port Description
This topic describes how to add port description.

2.5 Configuring the Attributes of an Upstream Ethernet Port
This topic describes how to configure the attributes of a specified Ethernet port so that the system communicates with the upstream device in the normal state.

2.6 Configuring a VLAN
Configuring VLAN is a prerequisite for configuring a service. Hence, before configuring a service, make sure that the VLAN configuration based on planning is complete.VLAN configuration is divided into three parts: creating a VLAN, configuring VLAN attributes, and configuring the VLAN forwarding policy. The system provides default values for VLAN configuration steps.

2.7 Configuring the User Security

Configuring the security mechanism can protect operation users and access users against user account theft and roaming or from the attacks from malicious users.

2.8 Configuring System Security
This topic describes how to configure the network security and protection measures of the system to protect the system from malicious attacks.

2.9 Configuring the ACL
This topic describes the type, rule, and configuration of the access control list (ACL) on the MA5600T/MA5603T.

2.10 Configuring QoS
This topic describes how to configure quality of service (QoS) on the MA5600T/MA5603T.

2.11 Configuring AAA
This topic describes how to configure the AAA on the MA5600T/MA5603T, including configuring the MA5600T/MA5603T as the local and remote AAA servers.

2.12 Configuring ANCP
Access Node Control Protocol (ANCP) is used to implement the functions such as topology discovery, line configuration, and L2C OAM on the user ports. The MA5600T/MA5603T establishes an ANCP session according to the GSMP communication IP address configured in the network access server (NAS).

2.1 Configuring Alarms

Alarm management includes the following functions: alarm record, alarm setting, and alarm statistics. These functions help you to maintain the device and ensure that the device works efficiently.

Context

An alarm refers to the notification of the system after a fault is detected. After an alarm is generated, the system broadcasts the alarm to the terminals, mainly including the NMS and command line interface (CLI) terminals.

Alarms are classified into fault alarm and recovery alarm. After a fault alarm is generated at a certain time, the fault alarm lasts till the fault is rectified to clear the alarm.

You can modify the alarm settings according to your requirements. The settings are alarm severity, alarm output mode through the CLI and alarm statistics switch.

When managing alarms on the GUI through the NMS, you can set filtering criteria to mask unimportant alarms and events. Such filtering function facilitates the focus of the important alarms and eliminates the load of the NMS.

Procedure

- Clear alarms.

  You can run the **alarm active clear** command to clear the alarms that are not recovered in the system.

  - When an active alarm lasts a long time, you can run this command to clear the alarm.
  - Before clearing an alarm, you can run the **display alarm active** command to query the currently active alarms.

- Configure alarm level.

  Run the **alarm alarmlevel** command to configure the alarm level.

  - Alarm levels are critical, major, minor, and warning.
  - Parameter **default** indicates restoring the alarm level to the default setting.
  - You can run the **display alarm list** command to query the alarm level.
  - The system specifies the default (also recommended) alarm level for each alarm. Use the default alarm level unless otherwise required.

- Configure alarm jitter-proof.

  Run the **alarm jitter-proof** command to configure the alarm jitter-proof function and the jitter-proof period.

  - To prevent a fault alarm and its recovery alarm from being displayed frequently, you can enable the alarm jitter-proof function to filter alarms in the system.
  - After the alarm jitter-proof function is enabled, the alarm in the system is not reported to the NMS immediately but is reported to the NMS after an alarm jitter-proof period.
  - If an alarm is recovered in an alarm jitter-proof period, the alarm is not reported to the NMS.

  - You can run the **display alarm jitter-proof** command to check whether the alarm jitter-proof function is enabled and whether the alarm jitter-proof period is set.
  - By default, the alarm jitter-proof function is disabled. You can determine whether to enable the function according to the running of the device.

- Set or shield the output of alarms.

  Run the **(undo) alarm output** command to set or shield the output of alarms to the CLI terminal.

  - Setting the output mode of alarms does not affect the generating of alarms. The alarms generated by the system are still recorded. You can run the **display alarm history** command to query the alarms that are shielded.
  - When the new output mode of an alarm conflicts with the previous mode, the new output mode takes effect.
  - The output mode of the recovery alarm is the same as the output mode of the fault alarm. When the output mode of the fault alarm is set, the system automatically synchronizes the output mode of its recovery alarm. The reverse is also applicable.

- Set alarm statistics period.

  Run the **alarm-event statistics period** command to set the alarm statistics collection period.

  - You can use the statistical result of alarms and events to locate a problem in the system.
  - You can run the **display alarm statistics** command to query the alarm statistical record.

- Filter alarms reporting to NMS.

  Run the **trap filter alarm condition** command to filter alarms that the device reports to the NMS through traps.

  The filtering criteria can be alarm ID, alarm severity, alarm type, subrack ID, subrack ID/slot ID, subrack ID/slot ID/port ID, VLAN interface, and NE.

  To reduce alarms and avoid alarm storms, the system does not send alarms of some ONTs to the NMS. To query the filtering criteria of alarms and events in the system, run the **display trap filter** command.

- Query alarm configuration and alarm statistics.

  Run the **display alarm configuration** command to query the alarm configuration according to the alarm ID. The alarm configuration that you can query includes the alarm ID, alarm name, alarm class, alarm type, alarm level, default alarm level, number of parameters, CLI output flag, conversion flag, and detailed alarm description.

  Run the **display alarm statistics** command to query the alarm statistical record.

  - When you need to know the frequency in which one alarm occurs within a time range, and to know the working conditions of the device and analyze the fault that may exist, run this command.
  - Currently, you can query the alarm statistics in the current period and previous period in the system.

- (Optional) Configure alarm policy for ONT.

  In FTTH scenarios, you can configure the ONT alarm policy profile to configure alarms for different service policies.

  1. Create an ONT alarm policy profile.

     Run the **ont-alarm-policy** command to create an ONT alarm policy profile.

The system supports a maximum number of 16 alarm policy profiles. The default alarm policy profile is profile 0.

It is recommended that you configure different alarm policies for VIP and common users.

2. Configure attributes of the ONT alarm policy profile.

   Run the **alarm filter** command to configure the control function of each alarm of the profile.

   Run the **commit** command to save the configuration.

   Run the **display ont-alarm-policy** command to query attributes of the ONT alarm policy profile.

3. Bind the ONT to the ONT alarm policy profile.

   Run the **ont alarm-policy** command to bind the ONT to the ONT alarm policy profile so that the PON board can control whether to send the ONT alarm information.

   During ONT adding or confirmation, the system binds the ONT to the default ONT alarm policy profile 0.

----End

Example

Assume the following configurations: The output of all alarms at level **warning** is shielded to the CLI terminal, the alarm jitter-proof function is enabled, the alarm jitter-proof period is set to 15s, the level of alarms with IDs 0x0a310021 and 0x2e314021 are modified to **critical**, do as follows:

```
huawei(config)#undo alarm output alarmlevel warning
huawei(config)#alarm jitter-proof on
huawei(config)#alarm jitter-proof 15
huawei(config)#alarm alarmlevel 0x0a310021 critical
huawei(config)#alarm alarmlevel 0x2e314021 critical
```

To mask the activation and deactivation alarm events of the ADSL port (event IDs 0x0a300013 and 0x0a300015) so that normal operations are not affected by too many alarms, do as follows:

```
huawei(config)#undo event output eventid 0x0a300013
huawei(config)#undo event output eventid 0x0a300015
```

To create ONT alarm policy profile 10, filter the following alarms, and bind this profile to GPON ONT 1 connected to port 0/3/0, do as follows:

- 0x2e112003 (The signal degrade of ONTi (SDi) occurs)
- 0x2e112004 (The signal fail of ONTi (SFi) occurs)
- 0x2e112006 (The loss of frame of ONTi (LOFi) occurs)
- 0x2e313015 (The hardware of the ONT is faulty)
- 0x2e313016 (The ONT switches to the standby battery)
- 0x2e313017 (The standby battery of the ONT is lost)
- 0x2e313018 (The standby battery of the ONT cannot be charged)
- 0x2e313019 (The voltage of the standby battery of the ONT is too low)
- 0x2e31301a (The shell of the ONT is opened)
- 0x2e313024 (The loss of signals occurs on the ethernet port of the ONT)

- 0x2e313025 (No signal is received in the video UNI of the ONT)
- 0x2e31302a (The E1/T1 port loss of signal (LOS) occurs at the ONT)

```
huawei(config)#ont-alarm-policy policy-id 10
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e112003
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e112004
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e112006
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313015
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313016
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313017
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313018
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313019
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e31301a
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313024
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313025
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e31302a
huawei(config-ont-alarm-policy-10)#commit
huawei(config-ont-alarm-policy-10)#quit
huawei(config)#interface gpon 0/3
hauwei(config-if-gpon-0/3)#ont alarm-policy 0 1 policy-id 10
```

2.2 Configuring the Clock

On a digital network comprising the MA5600T and other devices, the primary problem to be solved is clock synchronization for carrying the traditional TDM service. To ensure the system clock synchronization of each device in the digital network, a system clock source must be specified.

Context

IP-based solution is the trend of future network and service development, so is the trend of the bearer network. Difficulties, however, currently exist in the transition from the SDH-based traditional network to the IP-based Ethernet bearer network. One key technology involved is how to carry traditional TDM service on the new network. Traditional TDM service has two major applications: voice service and clock synchronization service. 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.

To ensure clock synchronization among devices, relevant clock synchronization methods are adopted based on the clock source solution provided by an upper-layer device.

Table 2-1 Clock configuration method

Configuration Method	Configuration Principle
Configuring the system clock based on the priority	This configuration method is similar to the basic configuration of the clock. If a device has multiple clock sources and the precision of the clock sources is provided, the clock source with the highest precision is generally configured with the highest priority.

Configuration Method	Configuration Principle
Configuring the system clock based on the SSM clock source selection mode	This configuration method is adopted if the clock transmitted from an upper-layer device contains SSM information and all clock sources are selected based on the SSM clock source selection mode.
Configuring external clock	This configuration method is adopted to output an independent clock signal from the CITD BITS OUT interface to serve as the clock source of a lower-layer device.

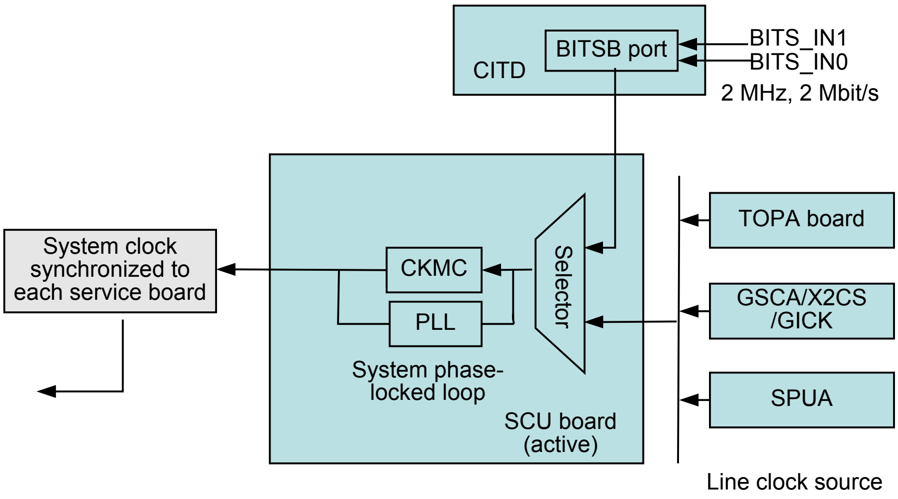
2.2.1 Configuring the System Clock Based on the Priority

If a device has multiple clock sources and the precision of the clock sources is provided, you need to configure the priorities of the clock sources. Generally, the higher the precision is, the higher the priority is.

Context

A clock source can be an external BITS clock or a line clock from the upper-layer node. The clock module automatically judges the types of the specified clock sources (BITS, TDM, or SDH), and sends them according to their priorities to the clock module, serving as clock sources for phase lock, as shown in **Figure 2-1**.

Figure 2-1 Configuring the system clock based on the priority



NOTE

- Only the MA5600T supports this configuration.
- When the SSM signal is used as the input clock signal and the system selects the clock source based on the SSM signal, see **2.2.2 Configuring the System Clock Based on the SSM Clock Source Selection Mode**.

Procedure

Step 1 Run the **clock source sourceid { frameid/slotid/portid [bits-clktype bits-impedance]** command to configure the system clock source.

Specify the clock signals extracted from a certain port as the system clock source.

- The system supports 10 clock sources in total.
- Only the external clock sources on the physical entities are added by running this command and the external clock sources are numbered. To enable the relevant external clock source, you need to run the **clock priority** command to determine whether the relevant clock source is available.
- The system clock cannot serve as the system clock source.

Step 2 Run the **clock priority system p0/p1/p2/p3/p4/p5/p6/p7/p8/p9** command to configure the priority of the system clock source.

- The system supports 10 clock source priorities. The highest priority is p0 and the lowest priority is p9.
- When the clock source is selected based on the priority, the system does not check the quality of the clock source. Therefore, you must configure the clock source of high quality with a high priority.
- After the priority of the clock source is configured, the system selects the clock source with the highest priority and in the normal state as the system clock source.
- When the clock source with the highest priority is faulty, the system automatically switches to the clock source with the second highest priority.
- When the clock source with the highest priority recovers, the system switches back to this clock source.

----End

Example

Assume the following configurations: On the MA5600T, obtain three clock sources from port BITS on the CITD board and ports 0/5/0 and 0/5/1 of the TOPA board as the clock source 0, clock source 1, and clock source 2 of the system. Configure clock source 0 with the highest priority and configure clock source 2 with the lowest priority. To perform the preceding configurations, do as follows:

```
huawei(config)#clock source 0 0/0/0 2MHz 120ohm
huawei(config)#clock source 1 0/5/0
huawei(config)#clock source 2 0/5/1
huawei(config)#clock priority system 0/1/2
```

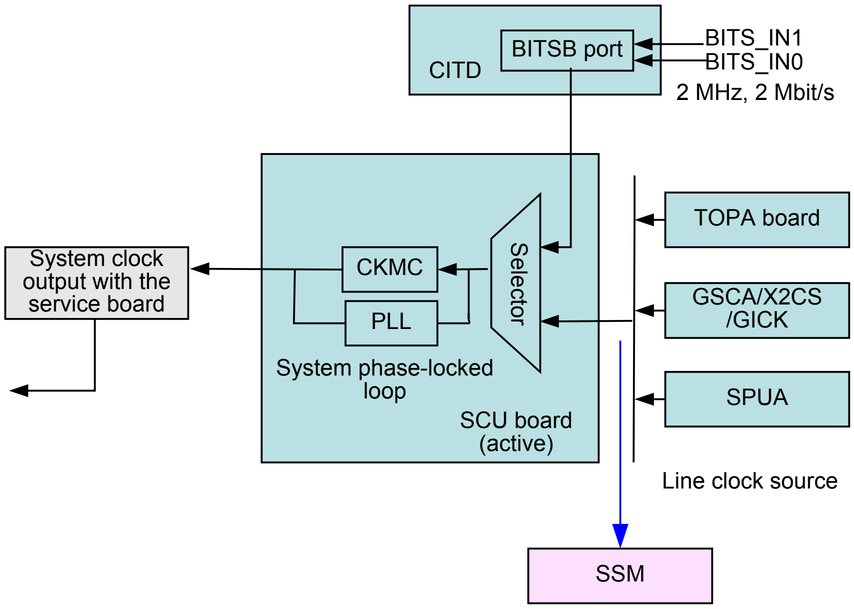
2.2.2 Configuring the System Clock Based on the SSM Clock Source Selection Mode

If the clock transmitted from an upper-layer device contains a synchronization status message (SSM) and all clock sources are selected based on the SSM, you need to configure the system clock based on the SSM clock source selection mode.

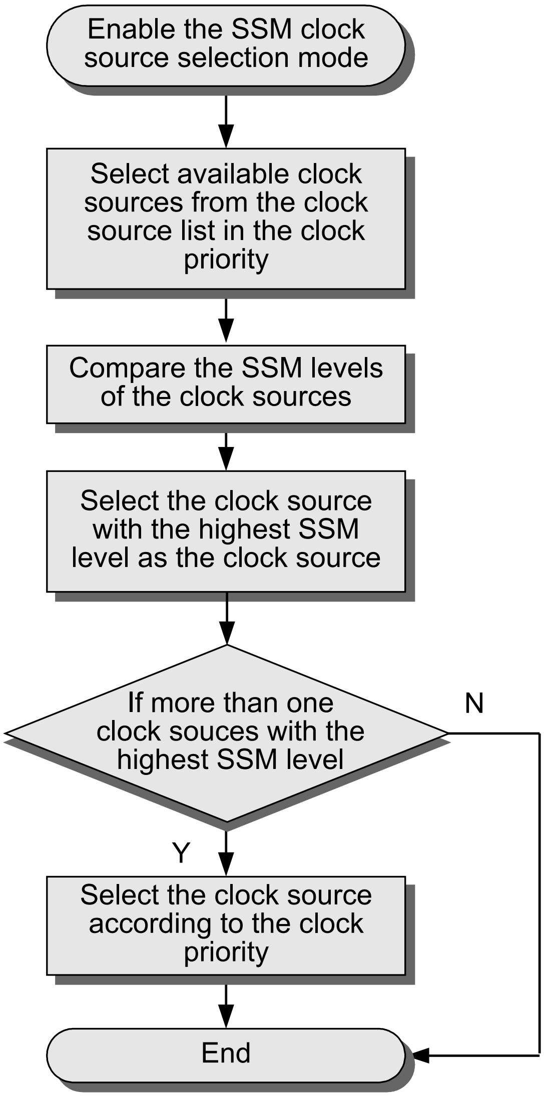
Context

By default, the SSM clock source selection mode is disabled. That is, the system selects the clock source based on the priority. The system enables the SSM clock source selection mode only after the system determines that the clock source contains an SSM and the entire system are based on the SSM clock source selection mode, as shown in **Figure 2-2**.

Figure 2-2 Configuring the system clock based on the SSM clock source selection mode



For the detailed SSM clock source selection process, see the following flowchart.


Enable the SSM clock source selection mode
Select available clock sources from the clock source list in the clock priority
Compare the SSM levels of the clock sources
Select the clock source with the highest SSM level as the clock source
If more than one clock souces with the highest SSM level
N
Y
Select the clock source according to the clock priority
End

Procedure

Step 1 Enable the SSM clock source selection mode.

Run the **clock ql-mode enable** command to enable the SSM clock source selection mode.

Step 2 Run the **clock source sourceid { frameid/slotid/portid [bits-clktype bits-impedance]** command to configure the system clock source.

Step 3 Run the **clock priority system p0/p1/p2/p3/p4/p5/p6/p7/p8/p9** command to configure the clock source range based on the SSM clock source selection mode and the priority sequence of the corresponding clock sources if the SSM quality levels are the same.

Step 4 (Optional) Run the **clock ql sourceid clock-ql** command to configure the SSM quality level for the clock source. If the SSM clock source selection mode is enabled, but a clock source does not support the output of an SSM, you need to manually configure the SSM quality level for the clock source. After the SSM quality level is configured, the device no longer matches the received SSM.

NOTE

- When the SSM clock source selection mode of the system is disabled, the SSM quality level of the clock source cannot be set.
- When the system selects the clock source based on the SSM quality level, the system selects the clock sources based on the priority and then compares the SSM of the clock sources. Finally, the system selects the clock source with the highest SSM quality level as the system clock source. If there are multiple clock sources with the same SSM qualify level, the system selects the clock source based on the priority.

Step 5 (Optional) Run the **clock ql input lower-limit** command to configure the lowest synchronization status message (SSM) quality level threshold of the clock source. When the SSM quality level of the clock source of the upper-layer device is higer than or equal to that of the device, the clock of the upper-layer device is traced. Otherwise, the clock of the device is in the holdover state and switched to the free-run state after 24 hours elapses.

Step 6 (Optional) Run the **clock ql output** command to configure whether the specified port sends the SSM quality level.

----End

Example

Example 1:

Assume the following configurations: Configure the SSM clock source selection mode as the system clock source selection mode. Obtain three clock sources from ports 0/20/0 and 0/20/1 of the X2CS board and port 0/19/0 of the GICK board as the clock source 0, clock source 1, and clock source 2 with the SSM. Configure clock source 0 with the highest priority and configure clock source 2 with the lowest priority. To perform the preceding configurations, do as follows:

```
huawei(config)#clock ql-mode enable
huawei(config)#clock source 0 0/20/0
huawei(config)#clock source 1 0/20/1
huawei(config)#clock source 2 0/19/0
uawei(config)#clock priority system 0/1/2
```

Example 2:

Assume the following configurations: Configure the SSM clock source selection mode as the system clock source selection mode. Obtain clock sources with SSM from ports 0/19/0 and 0/19/1 of the GICK board as clock source 0 and clock source 1; and obtain a clock source that does not support SSM from port 0/0/0 of the CITD board as clock source 2. Configure clock source 0 with the highest priority and configure clock source 2 with the lowest priority.

Set manually the SSM of clock source 2 to QL-SSU-A.

Send SSM from port 0/3/1. To perform the preceding configurations, do as follows:

```
huawei(config)#clock ql-mode enable
huawei(config)#clock source 0 0/19/0
huawei(config)#clock source 1 0/19/1
huawei(config)#clock source 2 0/0/0 2MHz 120ohm
huawei(config)#clock ql 2 QL-SSU-A
huawei(config)#clock priority system 0/1/2
huawei(config)#clock ql output 0/3/1 enable
```

2.2.3 Configuring External Clock

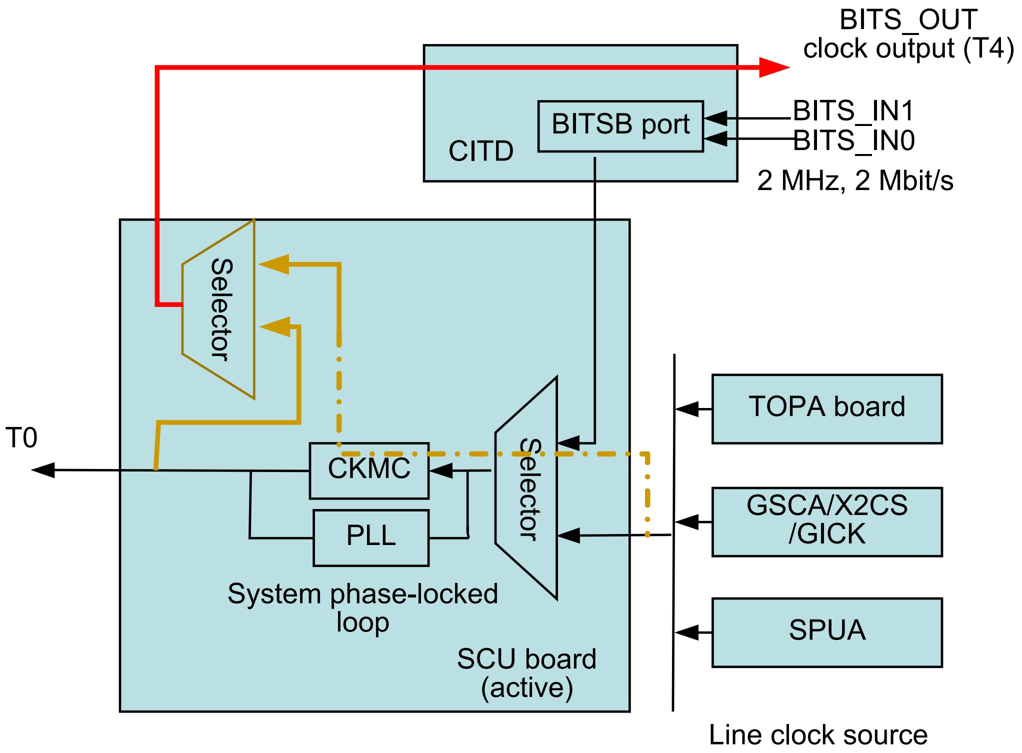
The MA5600T can select a system clock output or export the line clock as the clock source of another device.

Context

As shown in **Figure 2-3**, the external clock output of the MA5600T supports the selection of the following two benchmark clocks.

- Select the system clock as the output benchmark clock.
- Select the line clock as the output benchmark clock.

Figure 2-3 External clock output



Procedure

Step 1 Run the **clock external mode** command to configure the switch mode of the output clock.

In the auto-trace mode, enable the output clock or disable the output clock depending on the system.

- In the case of the SSM clock source selection mode, if the SSM quality level of the input clock is not lower than the threshold, the output clock port (T4) is enabled; otherwise, the output clock port is disabled.
- In the case of the priority clock source selection mode, the output clock is enabled if there is a clock source serving as the current source of the output clock. Otherwise, the output clock is disabled.

In the fix-trace mode, the system clock is output fixedly.

In the no-trace mode, the output clock is manually disabled.

NOTE

The system defaults to the fix-trace mode.

Step 2 Run the **clock external bits-type { 2MHz |2Mbps }** command to set the signal type of the BITS port on the CITD board to 2 MHz or 2 Mbit/s.

NOTE

The system defaults to 2 Mbit/s.

Step 3 Configuring the clock source of the external clock

1. Run the **clock source sourceid { system | { frameid/slotid/portid [1588 | bits-clktype bits-impedance]** command to configure the clock sources of the external clock.

   NOTE

   The CITD port does not support clock sources of the external clock.

2. Run the **clock priority external p0/p1/p2/p3/p4/p5/p6/p7/p8/p9** command to configure the clock sources and their priorities.

Step 4 (Optional) Run the **clock external output threshold clock-ql** command to configure the threshold of the SSM quality level for the output clock.

- If the output clock is in the auto-trace mode and its SSM quality level is lower than the threshold, the output clock is disabled automatically.
- The threshold takes effect only when the clock source mode is the SSM clock source selection mode. To configure the threshold, see **2.2.2 Configuring the System Clock Based on the SSM Clock Source Selection Mode**.

----End

Example

To obtain synchronization Ethernet clock sources from port 0/19/0 of the GICK board and port 0/20/1 of the X2CA board as system clock source 1 and system clock source 2, configure their priorities, and set the output clock to auto-trace, do as follows:

```
huawei(config)#clock external mode auto-trace
huawei(config)#clock source 1 0/19/0
huawei(config)#clock source 2 0/20/1
huawei(config)#clock priority external 2/1
```

2.3 Configuring the Network Time

Configure the NTP protocol to keep the time of all devices in the network synchronized, so that the MA5600T/MA5603T implements various service applications based on universal time, such as the network management system and the network accounting system.

Context

Introduction to the NTP Protocol:

- The Network Time Protocol (NTP) is an application layer protocol defined in RFC 1305, which is used to synchronize the times of the distributed time server and the client. The RFC defines the structures, arithmetics, entities and protocols used in the implementation of NTP.
- NTP is developed from the time protocol and the ICMP timestamp message protocol, with special design on the aspects of accuracy and robustness.
- NTP runs over UDP with port number as 123.

- Any local system that runs NTP can be time synchronized by other clock sources, and also act as a clock source to synchronize other clocks. In addition, mutual synchronization can be done through NTP packets exchanges.

NTP is applied to the following situations where all the clocks of hosts or routers in a network need to be consistent:

- In the network management, an analysis of log or debugging information collected from different routers needs time for reference.
- The charging system requires the clocks of all devices to be consistent.
- Completing certain functions, for example, timing restart of all the routers in a network requires the clocks of all the routers be consistent.
- When several systems work together on the same complicate event, they have to take the same clock for reference to ensure a correct implementation order.
- Incremental backup between the backup server and clients requires clocks on them be synchronized.

When all the devices on a network need to be synchronized, it is almost impossible for an administrator to manually change the system clock by using a command line. This is because the work load is heavy and clock accuracy cannot be ensured. NTP can quickly synchronize the clocks of network devices and ensure their precision.

There are four NTP modes: server/client, peer, broadcast and multicast modes. The MA5600T/MA5603T supports all these modes.

Default Configuration

Table 2-2 provides the default configuration for NTP.

Table 2-2 Default configuration for NTP

Parameter	Default Value
NTP-service authentication function	Disable
NTP-service authentication key	None
The maximum allowed number of sessions	100
Clock stratum	16

2.3.1 (Optional) Configuring NTP Authentication

This topic describes how to configure NTP authentication to improve the network security and prevent unauthorized users from modifying the clock.

Prerequisites

Before configuring the NTP client/server mode, make sure that the network interface and the routing protocol of the MA5600T/MA5603T are configured so that the server and the client are reachable to each other at the network layer.

Context

In certain networks that have strict requirements on security, enable NTP authentication when running the NTP protocol. Configuring NTP authentication is classified into configuring NTP authentication on the client and configuring NTP authentication on the server.

Precautions

- If NTP authentication is not enabled on the client, the client can synchronize with the server, regardless of whether NTP authentication is enabled on the server.
- If NTP authentication is enabled, a reliable key should be configured.
- The configuration of the server must be the same as that of the client.
- When NTP authentication is enabled on the client, the client can pass the authentication if the server is configured with the same key as that of the client. In this case, you do not need to enable NTP authentication on the server or declare that the key is reliable.
- The client synchronizes with only the server that provides the reliable key. If the key provided by the server is unreliable, the client does not synchronize with the server.
- The flow of configuring NTP authentication is as follows: start->enable NTP authentication->configure the reliable NTP authentication key->declare the reliable key->end.

Procedure

Step 1 Run the **ntp-service authentication enable** command to enable NTP authentication.

Step 2 Run the **ntp-service authentication-keyid** command to set an NTP authentication key.

Step 3 Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.

----End

Example

To enable NTP authentication, set the NTP authentication key as **aNiceKey** with the key number 42, and then define key 42 as a reliable key, do as follows:

```
huawei(config)#ntp-service authentication enable
huawei(config)#ntp-service authentication-keyid 42 authentication-mode md5 aNice
Key
huawei(config)#ntp-service reliable authentication-keyid 42
```

2.3.2 Configuring the NTP Broadcast Mode

This topic describes how to configure the MA5600T/MA5603T for clock synchronization in the NTP broadcast mode. After the configuration is completed, the server periodically broadcasts clock synchronization packets through a specified port, and the client listens to the broadcast packets sent from the server and synchronizes the local clock according to the received broadcast packets.

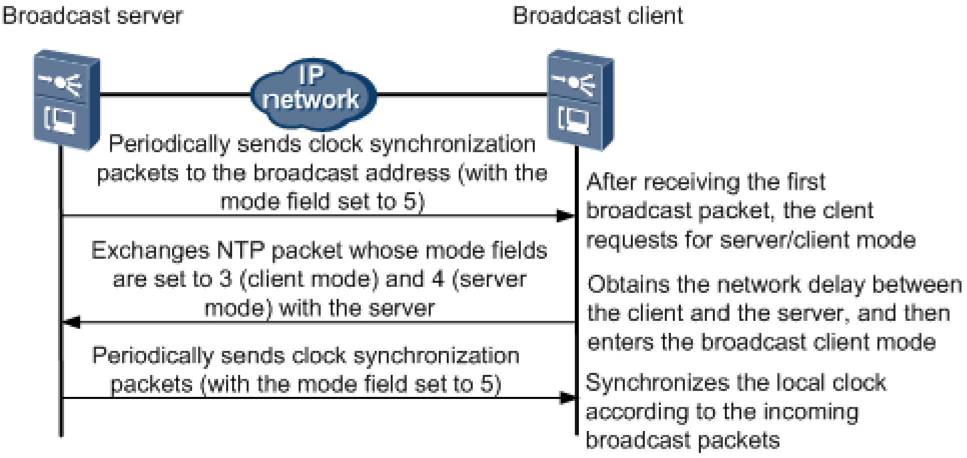
Prerequisites

Before configuring the NTP broadcast mode, make sure that the network interface and the routing protocol of the MA5600T/MA5603T are configured so that the server and the client are reachable to each other at the network layer.

Context

In the broadcast mode, the server periodically sends clock synchronization packets to the broadcast address 255.255.255.255, with the mode field set to 5 (indicating the broadcast mode). The client listens to the broadcast packets sent from the server. After receiving the first broadcast packet, the client exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server to estimate the network delay between the client and the server. The client then enters the broadcast client mode, continues to listen to the incoming broadcast packets, and synchronizes the local clock according to the incoming broadcast packets, as shown in **Figure 2-4**.

Figure 2-4 NTP broadcast mode


Broadcast server
Broadcast client
IP network
Periodically sends clock synchronization packets to the broadcast address (with the mode field set to 5)
Exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server
Periodically sends clock synchronization packets (with the mode field set to 5)
After receiving the first broadcast packet, the clent requests for server/client mode
Obtains the network delay between the client and the server, and then enters the broadcast client mode
Synchronizes the local clock according to the incoming broadcast packets

Precautions

1. In the broadcast mode, you should configure both the NTP server and the NTP client.
2. The clock stratum of the synchronizing device must be higher than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

- Configure the NTP broadcast server host.
  1. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
  2. (Optional) Configure NTP authentication.

     In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

   a. Run the **ntp-service authentication enable** command to enable NTP authentication.
   b. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
   c. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
3. Add a VLAN Layer 3 interface.
   a. Run the **vlan** command to create a VLAN.
   b. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
   c. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLAN interface mode to configure the Layer 3 interface.
   d. Run the **ip address** command to configure the IP address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
4. Run the **ntp-service broadcast-server** command to configure the NTP broadcast server mode of the host, and specify the key ID for the server to send packets to the client.

- Configure the NTP broadcast client host.
  1. (Optional) Configure NTP authentication.

     In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

     a. Run the **ntp-service authentication enable** command to enable NTP authentication.
     b. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
     c. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
  2. Add a VLAN Layer 3 interface.
     a. Run the **vlan** command to create a VLAN.
     b. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
     c. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLAN interface mode to configure the Layer 3 interface.
     d. Run the **ip address** command to configure the IP address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
  3. Run the **ntp-service broadcast-client** command to configure a host as the NTP broadcast client.

----End

Example

Assume the following configurations: MA5600T/MA5603T_S uses the local clock as the master NTP clock on stratum 2 and works in the NTP broadcast mode, broadcasting clock synchronization packets periodically through IP address 10.10.10.10/24 of the Layer 3 interface of VLAN 2, and MA5600T/MA5603T_C functions as the NTP client, listening to the broadcast packets sent from the server through IP address 10.10.10.20/24 of the Layer 3 interface of VLAN 2 and synchronizing with the clock on the broadcast server. To perform these configurations, do as follows:

1. On MA5600T/MA5603T_S:

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service broadcast-server
huawei(config-if-vlanif2)#quit
```

2. On MA5600T/MA5603T_C:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service broadcast-client
huawei(config-if-vlanif2)#quit
```

2.3.3 Configuring the NTP Multicast Mode

This topic describes how to configure the MA5600T/MA5603T for clock synchronization in the NTP multicast mode. After the configuration is completed, the server periodically multicasts clock synchronization packets through a specified port, and the client listens to the multicast packets sent from the server and synchronizes the local clock according to the received multicast packets.

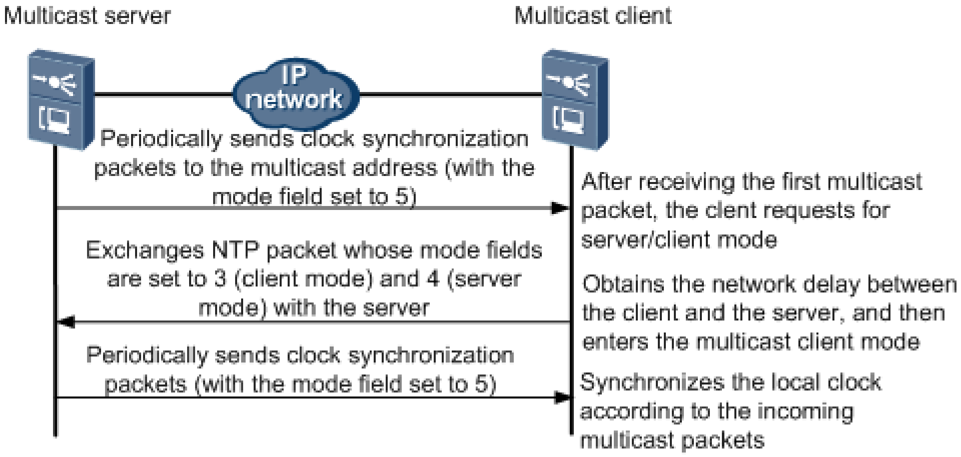
Prerequisites

Before configuring the NTP multicast mode, make sure that the network interface and the routing protocol of the MA5600T/MA5603T are configured so that the server and the client are reachable to each other at the network layer.

Context

In the multicast mode, the server periodically sends clock synchronization packets to the multicast address configured by the user. The default NTP multicast address 224.0.1.1 is used if the multicast address is not configured. The mode field of clock synchronization packet is set to 5 (multicast mode). The client listens to the multicast packets sent from the server. After receiving the first multicast packet, the client exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server to estimate the network delay between the client and the server. The client then enters the multicast client mode, continues to listen to the incoming multicast packets, and synchronizes the local clock according to the incoming multicast packets, as shown in **Figure 2-5**.

Figure 2-5 NTP multicast mode


Multicast server
Multicast client
IP network
Periodically sends clock synchronization packets to the multicast address (with the mode field set to 5)
After receiving the first multicast packet, the clent requests for server/client mode
Exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server
Obtains the network delay between the client and the server, and then enters the multicast client mode
Periodically sends clock synchronization packets (with the mode field set to 5)
Synchronizes the local clock according to the incoming multicast packets

Precautions

1. In the multicast mode, you should configure both the NTP server and the NTP client.
2. The clock stratum of the synchronizing device must be higher than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

- Configure the NTP multicast server host.
  1. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
  2. (Optional) Configure NTP authentication.

     In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

     a. Run the **ntp-service authentication enable** command to enable NTP authentication.

     b. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.

     c. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
  3. Add a VLAN Layer 3 interface.

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

     b. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.

     c. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLAN interface mode to configure the Layer 3 interface.

   d. Run the **ip address** command to configure the IP address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.

4. Run the **ntp-service multicast-server** command to configure the NTP multicast server mode of the host, and specify the key ID for the server to send packets to the client.

- Configure the NTP multicast client host.
  1. (Optional) Configure NTP authentication.

     In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

     a. Run the **ntp-service authentication enable** command to enable NTP authentication.

     b. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.

     c. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
  2. Add a VLAN Layer 3 interface.

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

     b. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.

     c. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLAN interface mode to configure the Layer 3 interface.

     d. Run the **ip address** command to configure the IP address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
  3. Run the **ntp-service multicast-client** command to configure a host as the NTP multicast client.

----End

Example

Assume the following configurations: MA5600T/MA5603T_S uses the local clock as the master NTP clock on stratum 2 and works in the NTP multicast mode, multicasting clock synchronization packets periodically through IP address 10.10.10.10/24 of the Layer 3 interface of VLAN 2, and MA5600T/MA5603T_C functions as the NTP client, listening to the multicast packets sent from the server through IP address 10.10.10.20/24 of the Layer 3 interface of VLAN 2 and synchronizing with the clock on the multicast server. To perform these configurations, do as follows:

1. On MA5600T/MA5603T_S:

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service multicast-server
huawei(config-if-vlanif2)#quit
```

2. On MA5600T/MA5603T_C:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service multicast-client
huawei(config-if-vlanif2)#quit
```

2.3.4 Configuring the Unicast NTP Client

This topic describes how to configure the MA5600T/MA5603T as the NTP client to synchronize with the NTP server in the network.

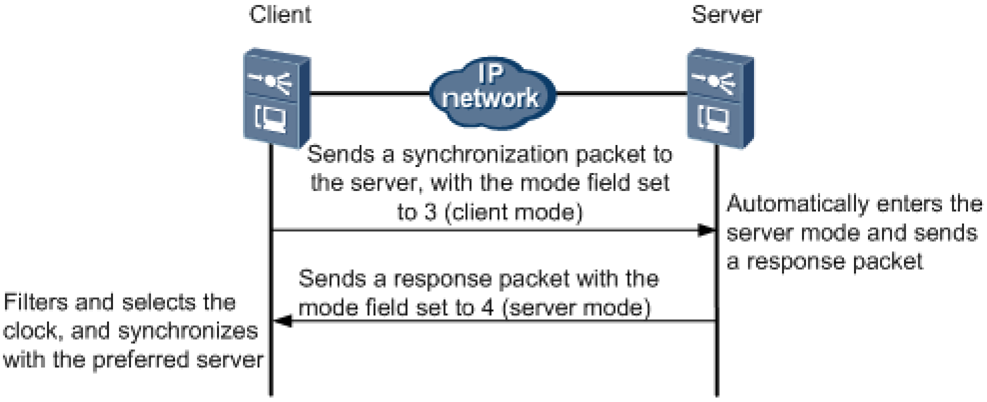
Prerequisites

Before configuring the NTP client/server mode, make sure that the network interface and the routing protocol of the MA5600T/MA5603T are configured so that the server and the client are reachable to each other at the network layer.

Context

In the client/server mode, the client sends a synchronization packet to the server, with the mode field set to 3 (client mode). After receiving the packet, the server automatically enters the server mode and sends a response packet with the mode field set to 4 (server mode). After receiving the response from the server, the client filters and selects the clock, and synchronizes with the preferred server, as shown in **Figure 2-6**.

Figure 2-6 NTP client/server mode


Client
Server
IP network
Sends a synchronization packet to the server, with the mode field set to 3 (client mode)
Automatically enters the server mode and sends a response packet
Sends a response packet with the mode field set to 4 (server mode)
Filters and selects the clock, and synchronizes with the preferred server

Precautions

1. In the client/server mode, you need to configure only the client, and do not need to configure the server.
2. The clock stratum of the synchronizing device must be lower than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

Step 1 Add a VLAN Layer 3 interface.

1. Run the **vlan** command to create a VLAN.
2. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
3. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLAN interface mode to configure the Layer 3 interface.
4. Run the **ip address** command to configure the IP address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.

Step 2 Run the **ntp-service unicast-server** command to configure the NTP unicast server mode, and specify the IP address of the remote server that functions as the local timer server and the interface for transmitting and receiving NTP packets.

NOTE

- In this command, *ip-address* is a unicast address, which cannot be a broadcast address, a multicast address, or the IP address of a local clock.
- After the source interface of the NTP packets is specified by *source-interface*, the source IP address of the NTP packets is configured as the primary IP address of the specified interface.
- A server can function as a time server to synchronize other devices only after its clock is synchronized.
- When the clock stratum of the server is higher than or equal to that of the client, the client does not synchronize with the server.
- You can run the **ntp-service unicast-server** command for multiple times to configure multiple servers. Then, the client selects the best server according to clock priorities.

Step 3 (Optional) Configure the ACL rules.

Filter the packets that pass through the Layer 3 interface. Only the IP packet from the clock server is allowed to access the Layer 3 interface. Other unauthorized packets are not allowed to access the Layer 3 interface. It is recommended to use the ACL rules for the system that has high requirements on security.

1. Run the **acl** *adv-acl-numbe* command to create an ACL.
2. Run the **rule** command to classify traffic according to the source IP address, destination IP address, type of the protocol over IP, and features or protocol of the packet, allowing or forbidding the data packets that meet related conditions to pass.
3. Run the **packet-filter** command to configure an ACL filtering rule for a specified port, and make the configuration take effect.

----End

Example

Assume the following configurations: One MA5600T/MA5603T functions as the NTP server (IP address: 10.20.20.20/24), the other MA5600T/MA5603T (IP address of the Layer 3 interface of VLAN 2: 10.10.10.10/24, gateway IP address: 10.10.10.1) functions as the NTP client, the NTP client sends the clock synchronization request packet through the VLAN Layer 3 interface to the NTP server, the NTP server responds to the request packet, and ACL rules are configured to allow only IP packets from the clock server to access the Layer 3 interface. To perform these configurations, do as follows:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.10.10
 0.0.0.0
```

```
huawei(config-acl-adv-3050)#rule permit ip source 10.20.20.20 0.0.0.0 destination
 10.10.10.10 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
```

2.3.5 Configuring the NTP Peer

This topic describes how to configure the MA5600T/MA5603T for clock synchronization in the NTP peer mode. In the peer mode, configure only the active peer, and the passive peer does not need to be configured. In the peer mode, the active peer and the passive peer can synchronize with each other. The peer with a higher clock stratum is synchronized by the peer with a lower clock stratum.

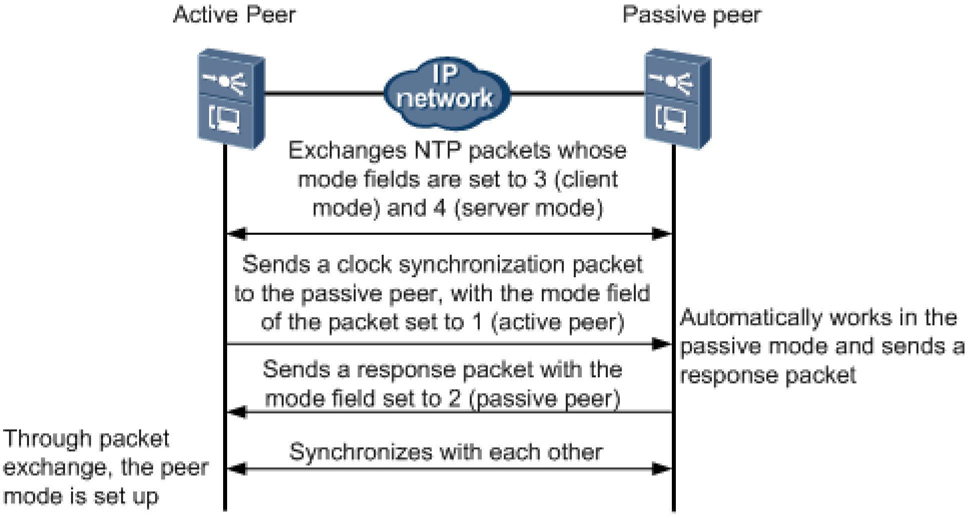
Prerequisites

Before configuring the NTP peer mode, make sure that the network interface and the routing protocol of the MA5600T/MA5603T are configured so that the server and the client are reachable to each other at the network layer.

Context

In the peer mode, the active peer and the passive peer exchange NTP packets whose mode fields are set to 3 (client mode) and 4 (server mode). Then, the active peer sends a clock synchronization packet to the passive peer, with the mode field of the packet set to 1 (active peer). After receiving the packet, the passive peer automatically works in the passive mode and sends a response packet with the mode field set to 2 (passive peer). Through packet exchange, the peer mode is set up. The active peer and the passive peer can synchronize with each other. If both the clock of the active peer and that of the passive peer are synchronized, the clock on a lower stratum is used, as shown in **Figure 2-7**.

Figure 2-7 NTP peer mode


Active Peer
Passive peer
IP network
Exchanges NTP packets whose mode fields are set to 3 (client mode) and 4 (server mode)
Sends a clock synchronization packet to the passive peer, with the mode field of the packet set to 1 (active peer)
Automatically works in the passive mode and sends a response packet
Sends a response packet with the mode field set to 2 (passive peer)
Through packet exchange, the peer mode is set up
Synchronizes with each other

Precautions

1. In the peer mode, you need to configure the NTP mode only on the active peer.

2. The peers determine clock synchronization according to the clock stratum instead of according to whether the peer is an active peer.

Procedure

Step 1 Configure the NTP active peer.

1. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
2. Run the **ntp-service unicast-peer** command to configure the NTP peer mode, and specify the IP address of the remote server that functions as the local timer server and the interface for transmitting and receiving NTP packets.

NOTE

- In this command, *ip-address* is a unicast address, which cannot be a broadcast address, a multicast address, or the IP address of a reference clock.
- After the source interface of the NTP packets is specified by *source-interface*, the source IP address of the NTP packets is configured as the primary IP address of the specified interface.

Step 2 Add a VLAN Layer 3 interface.

1. Run the **vlan** command to create a VLAN.
2. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
3. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLAN interface mode to configure the Layer 3 interface.
4. Run the **ip address** command to configure the IP address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.

----End

Example

Assume the following configurations: One MA5600T/MA5603T functions as the NTP active peer (IP address of the Layer 3 interface of VLAN 2: 10.10.10.10/24) and works on clock stratum 4, the other MA5600T/MA5603T (IP address: 10.10.10.20/24) functions as the NTP passive peer, the active peer sends a clock synchronization request packet through the VLAN Layer 3 interface to the passive peer, the passive peer responds to the request packet, and the peer with a higher clock stratum is synchronized by the peer with a lower clock stratum. To perform these configurations, do as follows:

```
huawei(config)#ntp-service refclock-master 4
huawei(config)#ntp-service unicast-peer
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
```

2.4 Adding Port Description

This topic describes how to add port description.

Prerequisites

A board must be added to the system.

Context

After the description of a physical port on the board is added, the description facilitates information query in system maintenance.

Procedure

Step 1 In the global config mode, run the **port desc** command to add port description.

Port description is a character string, used to identify a port on a board in a slot of a subrack.

Step 2 Run the **display port desc** command to query port description.

----End

Example

Plan the format of user port description as "community ID-building ID-floor ID/subrack ID-slot ID-port ID". "Community ID-building ID-floor ID" indicates the physical location where the user terminal is deployed, and subrack ID-slot ID-port ID" indicates the physical port on the local device that is connected to the user terminal. This plan can present the user terminal location and the connection between the user terminal and the device, which facilitates query in maintenance. Assume that the user terminal that is connected to port 0/2/0 of the MA5600T/MA5603T is deployed in floor 1, building 01 of community A. To add port description according to the plan, do as follows:

```
huawei(config)#port desc 0/2/0 description A-01-01/0-2-0
huawei(config)#display port desc 0/2/0
  ------------------------------------------------------------
   F/ S/ P   IMA Group   Port Description
  ------------------------------------------------------------
   0/ 2/ 0   -           A-01-01/0-2-0
  ------------------------------------------------------------
```

2.5 Configuring the Attributes of an Upstream Ethernet Port

This topic describes how to configure the attributes of a specified Ethernet port so that the system communicates with the upstream device in the normal state.

Prerequisites

The board in the GIU slot must be in position and must work in the normal state.

Context

The MA5600T/MA5603T should be interconnected with the upstream device through the Ethernet port. Therefore, pay attention to the consistency of port attributes.

Default Configuration

Table 2-3 lists the default settings of the attributes of an Ethernet port.

Table 2-3 Default settings of the attributes of an Ethernet port

Parameter	Default Setting (Optical Port)	Default Setting (Electrical Port)
Auto-negotiation mode of the port	Disabled	Enabled
Port rate	● FE optical port: 100 Mbit/s ● GE optical port: 1000 Mbit/s ● 10GE optical port: 10000 Mbit/s	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the port rate.
Duplex mode	Full-duplex, read only	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the duplex mode.
Network cable adaptation mode	Not supported	● FE electrical port: auto ● GE electrical port: normal
Flow control	Disabled	Disabled

Procedure

- Configure the physical attributes of an Ethernet port.
  1. (Optional) Set the auto-negotiation mode of the Ethernet port.

     Run the **auto-neg** command to set the auto-negotiation mode of the Ethernet port. You can enable or disable the auto-negotiation mode:

     - After the auto-negotiation mode is enabled, the port automatically negotiates with the peer port for the rate and working mode of the Ethernet port.
     - After the auto-negotiation mode is disabled, the rate and working mode of the port are in the forced mode (adopt default values or are set through command lines).
  2. (Optional) Set the rate of the Ethernet port.

     Run the **speed** command to set the rate of the Ethernet port. After the port rate is set successfully, the port works at the set rate. Pay attention to the following points:

     - Make sure that the rate of the Ethernet port is the same as that of the interconnected port on the peer device. This prevents communication failure.
     - The auto-negotiation mode should be disabled.
  3. (Optional) Set the duplex mode of the Ethernet port.

     Run the **duplex** command to set the duplex mode of the Ethernet port. The duplex mode of an Ethernet port can be full-duplex, half-duplex, or auto negotiation. Pay attention to the following points:

     - Make sure that the ports of two interconnected devices work in the same duplex modes. This prevents communication failure.
     - The auto-negotiation mode should be disabled.
  4. (Optional) Configure the network cable adaptation mode of the Ethernet port.

Run the **mdi** command to configure the network cable adaptation mode of the Ethernet port to match the actual network cable. The network adaptation modes are as follows:

  - **normal**: Specifies the adaptation mode of the network cable as straight-through cable. In this case, the network cable connecting to the Ethernet port must be a straight-through cable.
  - **across**: Specifies the adaptation mode of the network cable as crossover cable. In this case, the network cable connecting to the Ethernet port must be a crossover cable.
  - **auto**: Specifies the adaptation mode of the network cable as auto-sensing. The network cable can be a straight-through cable or crossover cable.

Pay attention to the following points:

  - The Ethernet optical port does not support the network cable adaptation mode.
  - If the Ethernet electrical port works in forced mode (auto-negotiation mode disabled), the network cable type of the port cannot be configured to **auto**.

- Configure flow control on the Ethernet port.

  Run the **flow-control** command to enable flow control on the Ethernet port. When the flow of an Ethernet port is heavy, run this command to control the flow to prevent network congestion, which may cause the loss of data packets. Flow control should be supported on both the local and peer devices. Pay attention to the following points:

  - If the peer device does not support flow control, generally, enable flow control on the local device.
  - If the peer device supports flow control, generally, disable flow control on the local device.

  By default, flow control is disabled.

- Mirror the Ethernet port.

  Run the **mirror port** command to mirror the Ethernet port. When the system is faulty, copy the traffic of a certain port to the other port and output the traffic for traffic observation, network fault diagnosis, and data analysis.

----End

Example

Ethernet port 0/19/0 is an electrical port. The attribute is as follows: The port rate is 1000 Mbit/s in duplex mode, with supporting flow control, not supporting auto-negotiation function. Do as follows:

```
huawei(config)#interface 0/19
huawei(config-if-0/19)#auto-neg 0 disable
huawei(config-if-0/19)#speed 0 1000
huawei(config-if-0/19)#duplex 0 full
huawei(config-if-0/19)#flow-control 0
```

2.6 Configuring a VLAN

Configuring VLAN is a prerequisite for configuring a service. Hence, before configuring a service, make sure that the VLAN configuration based on planning is complete.VLAN configuration is divided into three parts: creating a VLAN, configuring VLAN attributes, and configuring the VLAN forwarding policy. The system provides default values for VLAN configuration steps.

2.6.1 Creating a VLAN

Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see **Table 2-4**.

Table 2-4 VLAN planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN type: smart
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S+C.	
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	

Default Configuration

Table 2-5 lists the default parameter settings of VLAN.

Table 2-5 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart VLAN	You can run the **defaultvlan modify** command to modify the VLAN type but cannot delete the VLAN.
Reserved VLAN of the system	VLAN ID range: 4079-4093	You can run the **vlan reserve** command to modify the VLAN reserved by the system.

Prerequisite

- The VLAN to be added should not exist in the system.
- Service VLAN cannot be reserve VLAN.

Procedure

Step 1 Create a VLAN.

Run the **vlan** to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 2-6 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the **vlan** ***vlanid*** **standard** command.	Standard VLAN. Ethernet ports in a standard VLAN are interconnected with each other but Ethernet ports in different standard VLANs are isolated from each other.	Only available to Ethernet ports and specifically to network management and subtending.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Smart VLAN	To add a smart VLAN, run the **vlan** ***vlanid*** **smart** command.	One VLAN may contain multiple xDSL service ports or xPON service ports. The traffic streams of these ports, however, are isolated from each other. In addition, the traffic streams of different VLANs are also isolated. One smart VLAN provides access for multiple users and therefore saves VLAN resources.	Smart VLANs can be applied in residential communities to provide xDSL or xPON service access.
MUX VLAN	To add a MUX VLAN, run the **vlan** ***vlanid*** **mux** command.	One MUX VLAN contains only one xDSL service port or xPON service port. The traffic streams in different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. Hence, a MUX VLAN can identify an access user.	MUX VLANs are applicable to xDSL or xPON service access. For example, MUX VLANs can be used to distinguish users.
Super VLAN	To add a super VLAN, run the **vlan** ***vlanid*** **super** command.	The super VLAN is based on Layer 3. One super VLAN contains multiple sub-VLANs. Through an ARP proxy, the sub-VLANs in a super VLAN can be interconnected at Layer 3.	Super VLANs save IP addresses and improve the utilization of IP addresses. For a super VLAN, sub-VLANs must be configured. You can run the **supervlan** command to add a sub-VLAN to a specified super VLAN. A sub-VLAN must be a smart VLAN or MUX VLAN.

NOTE

- To add VLANs with consecutive IDs in batches, run the **vlan *vlanid* to *end-vlanid*** command.
- To add VLANs with inconsecutive IDs in batches, run the **vlan *vlan-list*** command.

----End

Example

Create VLAN 50 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 50 smart
```

Create VLAN 55-60 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 55 to 60 smart
```

Create VLAN 65, 73 and 52 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 65,73,52 smart
```

2.6.2 Configuring the VLAN attribute

Configuring the VLAN attribute is a prerequisite for configuring a VLAN. Hence, before configuring a service, make sure that the VLAN attribute configuration based on planning is complete.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see **Table 2-7**.

Table 2-7 VLAN attribute planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN attribute: common
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S +C.	Attribute: stacking

User Type	Application Scenario	VLAN Planning
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	VLAN attribute: QinQ

Default Configuration

Table 2-8 lists the default parameter settings of VLAN.

Table 2-8 Default attribute settings of VLAN

Parameter	Default Setting
Default attribute of a new VLAN	Common

Prerequisite

- The VLAN to be configured should have been created.
- The VLAN attribute must be planned properly according to the application scenarios.

Procedure

Step 1 Configure the VLAN attribute.

The default attribute for a new VLAN is "common". You can run the **vlan attrib** command to configure the attribute of the VLAN.

Configure the attribute according to VLAN planning.

Table 2-9 VLAN attributes and application scenarios

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
Common	The default attribute for a new VLAN is "common".	The VLAN with this attribute can be a standard VLAN, smart VLAN, MUX VLAN, or super VLAN.	A VLAN with the common attribute can function as a common Layer 2 VLAN or function for creating a Layer 3 interface.	Applicable to the N:1 access scenario.

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
QinQ VLAN	To configure QinQ as the attribute of a VLAN, run the **vlan attrib *vlanid* q-in-q** command.	The VLAN with this attribute can be a standard VLAN, smart VLAN or MUX VLAN. The attribute of a sub VLAN, the VLAN with a Layer 3 interface, and the default VLAN of the system cannot be set to QinQ VLAN.	The packets from a QinQ VLAN contain two VLAN tags, that is, inner VLAN tag from the private network and outer VLAN tag from the MA5600T/ MA5603T. Through the outer VLAN, a Layer 2 VPN tunnel can be set up to transparently transmit the services between private networks.	Applicable to the enterprise private line scenario.

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
VLAN Stacking	To configure stacking as the attribute of a VLAN, run the **vlan attrib** ***vlanid*** **stacking** command.	The VLAN with this attribute can only be a smart VLAN or MUX VLAN. The attribute of a sub VLAN, the VLAN with a Layer 3 interface, and the default VLAN of the system cannot be set to VLAN stacking.	The packets from a stacking VLAN contain two VLAN tags, that is, inner VLAN tag and outer VLAN tag from the MA5600T/ MA5603T. The upper-layer BRAS authenticates the access users according to the two VLAN tags. In this manner, the number of access users is increased. On the upper-layer network in the Layer 2 working mode, a packet can be forwarded directly by the outer VLAN tag and MAC address mode to provide the wholesale service for ISPs.	Applicable to the 1:1 access scenario for the wholesale service or extension of VLAN IDs. In the case of a stacking VLAN, to configure the inner tag of the service port, run the **stacking label** command.

NOTE

- To configure attributes for the VLANs with consecutive IDs in batches, run the **vlan attrib** ***vlanid*** **to** ***end-vlanid*** command.
- To configure attributes for the VLANs with inconsecutive IDs in batches, run the **vlan attrib** ***vlan-list*** command.

----End

Example

To configure the attribute of VLAN 50 to **stacking** for extending VLAN IDs, do as follows:

```
huawei(config)#vlan attrib 50 stacking
```

To configure the attributes of VLANs 55-60 (used for enterprise users) to **QinQ**, do as follows:

```
huawei(config)#vlan attrib 55 to 60 q-in-q
```

To configure the attributes of service VLANs 65, 73, and 52 to **stacking**, do as follows:

```
huawei(config)#vlan attrib 65,73,52 stacking
```

2.6.3 Configuring the VLAN S+C forwarding policy

The configuration of VLAN forwarding policies is the foundation of the VLAN configuration, and is also an important step to ensure that services are forwarded correctly. Before the service configuration, make sure that VLAN forwarding policies have been configured properly according to the actual planning.

VLAN forwarding policy refers to the Layer 2 forwarding mechanism of packets. It can be **vlan-connect** or **vlan-mac**. In the **vlan-connect** mode, the system forwards packets based on S+C. This mode ensures higher security by solving the problems of insufficient MAC address space, MAC address aging, MAC address spoofing, and MAC address attacks. In the **vlan-mac** mode, the system forwards the packets based on the VLAN and MAC address of packets.

S+C forwarding is to forward packets on the service board based on S+C and forward packets on the control board based on VLAN+MAC; Strict S+C forwarding is to forward packets on the service board and control board based on S+C; Only the SCUN/SCUH control board supports strict S+C forwarding.

Application Context

Different users have different requirements of VLAN forwarding modes. **Table 2-10** lists detailed application scenarios of VLAN forwarding modes.

Table 2-10 VLAN application and planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN forwarding mode: by VLAN+MAC
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S+C.	VLAN forwarding mode: by S+C

User Type	Application Scenario	VLAN Planning
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	VLAN forwarding mode: by VLAN+MAC or S+C.

Default Configuration

Table 2-11 lists the default forwarding policy settings of VLAN.

Table 2-11 Default parameter settings of VLAN

Parameter	Default Setting
VLAN forwarding mode	VLAN+MAC

Prerequisite

- VLAN IDs are created correctly.
- VLAN attributes are configured properly.

You can configure the VLAN forwarding policy in either the global config mode or VLAN service profile mode.

- If you only need to configure the forwarding policy for one VLAN, it is recommended that you use the first configuration method, which is simple.
- If all service profile parameters are the same for multiple VLANs, it is recommended that you use the second configuration method to bulk configure the same forwarding policy for these VLANs using service profiles.

Procedure

Step 1 Configure the VLAN forwarding policy.

- In the global config mode, to configure the VLAN forwarding policy, run the **vlan forwarding** command. The default VLAN forwarding mode is VLAN+MAC in the system.
- In the VLAN service profile mode, to configure the VLAN forwarding policy, do as follows:
  1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
  2. Run the **forwarding** command to configure the VLAN forwarding policy. The default VLAN forwarding mode is VLAN+MAC in the system.
  3. Run the **commit** command to validate the profile configuration. The configuration of the VLAN service profile takes effect only after execution of this command.
  4. Run the **quit** command to quit the VLAN service profile mode.
  5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile.

NOTE

Configure the traffic stream that uses strict S+C forwarding. The procedure is as follows:

1. Run the **vlan** command to add a VLAN.
2. Run the **vlan attrib** command to modify the VLAN attribute to QinQ or stacking.
3. Run the **mac-address learning** command to disable the MAC address learning function of the control board.
4. Run the **vlan forwarding** or **forwarding** command to configure the VLAN forwarding policy.
5. Run the **port vlan** command to associate the upstream port, SVLAN, and CVLAN.
6. Run the **service-port** command to create a service port.

----End

Example

To configure the forwarding policy of VLAN 50 to S+C, do as follows:

```
huawei(config)#vlan forwarding 50 vlan-connect
```

To configure the forwarding policy of VLAN 60 to S+C using the VLAN service profile, do as follows:

```
huawei(config)#vlan service-profile profile-id 10
huawei(config-vlan-srvprof-10)#forwarding vlan-connect
huawei(config-vlan-srvprof-10)#commit
huawei(config-vlan-srvprof-10)#quit
huawei(config)#vlan bind service-profile 60 profile-id 10
```

Assuming that the SCUN control board is used, VLAN 65 is a service VLAN, and VLAN 73 is an enterprise VLAN, to configure the forwarding policy of VLAN 65 to S+C and disable the MAC address learning function, do as follows:

```
huawei(config)#vlan 65 smart
huawei(config)#vlan attrib 65 stacking
huawei(config)#mac-address learning fabric all disable
huawei(config)#vlan service-profile profile-id 200
huawei(config-vlan-srvprof-200)#mac-address learning fabric disable
huawei(config-vlan-srvprof-200)#forwarding vlan-connect
huawei(config-vlan-srvprof-200)#commit
huawei(config-vlan-srvprof-200)#quit
huawei(config)#vlan bind service-profile 65 profile-id 200
huawei(config)#port vlan 65 inner-vlan-list 73 0/19 0
huawei(config)#service-port 100 uplink-port 0/19/0 vlan 65 gpon 0/2/0 ont 1
gemport
2 multi-service user-vlan 73 rx-cttr 10 tx-cttr 10
```

2.6.4 Configuring a VLAN Service Profile

A VLAN service profile is a collection of service-related parameters for VLAN attributes. After a VLAN is bound to a VLAN service profile, the VLAN has all the VLAN attributes defined in the VLAN service profile. Binding a VLAN service profile is an efficient way of configuring a VLAN.

Application Context

VLAN, as a basic and also important concept of access equipment, involves discrete configurations of many parameters. These parameters include forwarding mode, security feature, protocol enabling/disabling, transparent transmission of protocol packets, and packet forwarding policy. Service parameters are related to specific VLANs and in actual usage there are a lot of VLANs, causing complex configuration. Against this backdrop, the VLAN service profile is introduced to achieve simplified and highly-efficient configuration. A VLAN service profile is abstracted from specific VLANs and supports centralized configuration of VLAN-related service parameters. Different VLANs of the same attribute can flexibly be bound to (or unbound from) a VLAN service profile to possess (or release) the attributes defined in the VLAN service profile.

Prerequisite

The VLAN to which the VLAN service profile is bound must be created.

Configuration Process

1. Create a VLAN service profile.
2. Configure the following service parameters according to service requirements:
   - Forwarding mode
   - Forwarding policy
   - Protocol switch
   - Transparent transmission function
   - Security function
3. Commit to save the current parameters.
4. Bind the VLAN service profile to the VLAN.

Procedure

Step 1 Create a VLAN service profile.

Run the **vlan service-profile** command to create a VLAN service profile or enter the configuration mode of the VLAN service profile. When the profile does not exist, running this command means to create a VLAN service profile and enter the configuration mode of the service profile. If the profile exists, running this command means to directly enter the configuration mode of this service profile.

Step 2 Configure the VLAN forwarding mode.

Forwarding mode refers to the Layer 2 packet forwarding mechanism, including VLAN+MAC forwarding (default) and SVLAN+CVLAN (or S+C) forwarding. In VLAN+MAC forwarding, the system needs to dynamically learn the mapping relationship between VLAN, source MAC address, and port. In S+C forwarding, the system does not need to dynamically learn MAC addresses but determines the forwarding entry according to SVLAN and CVLAN. Because S +C forwarding does not depend on MAC address learning, it has the following advantages:

1. Saving MAC addresses
2. Preventing occurrence of unknown unicast packets caused by aging of dynamic MAC addresses Broadcasting unknown unicast packets threatens the security of the device
3. Ensuring security by solving problems such as MAC spoofing and attack

- Run the **forwarding** command to configure the VLAN forwarding policy.
- Run the **user-bridging** command to configure the bridging function of the VLAN service profile. After the bridging function is enabled, two users in the same VLAN can directly communicate with each other at Layer 2.

NOTE

The bridging function is visible only to the SCUN and SCUH control board. It conflicts with S+C forwarding.

- Run the **mac-address learning** command to configure MAC address learning on the control board.

Step 3 Configure the VLAN forwarding policy.

Forwarding policy refers to the discard policy of packets such as downstream broadcast, downstream unknown unicast, and unknown multicast packets.

- Run the **packet-policy** command to configure the forwarding policy for the downstream broadcast packets, downstream unknown unicast packets, and unknown multicast packets in the VLAN. Two policies namely forward and discard are supported.
- Run the **igmp mismatch** command to configure the mismatch IGMP policy of the VLAN, supports the transparent and discard policies.

Step 4 Configure the VLAN protocol switch.

Protocol switch refers to whether to enable certain types of protocols or certain functions of a protocol. VMAC aging and PPPoE MAC conflict with S+C forwarding.

- Run the **dhcp mode** command to configure the DHCPv4 forwarding mode, that is, to switch between the DHCP Layer 2 forwarding mode and the DHCP Layer 3 forwarding mode.
- Run the **dhcpv6 mode** command to configure the DHCPv6 forwarding mode, that is, to switch between the DHCP Layer 2 forwarding mode and the DHCP Layer 3 forwarding mode.
- Run the **pppoe mac-mode** command to configure the MAC address allocation mode for PPPoE users. Two modes namely, single-mac and multi-mac are supported.
- Run the **pppoa mac-mode** command to configure the MAC address allocation mode for PPPoA users. Two modes namely, single-mac and multi-mac are supported.
- Run the **vmac aging-mode** command to configure the VMAC aging mode, which can be common aging or DHCP-based aging.
- Run the **pitp** command to configure the PITP function to implement authentication of bound user account and access port.
- Run the **dhcp option82** command to configure the DHCPv4 option 82 feature.
- Run the **dhcpv6 option82** command to enable or disable the DHCPv6 option 82 feature.
- Run the **dhcp proxy** command to configure the DHCP proxy function. After the DHCP proxy function is enabled, the server ID proxy function and lease time proxy function will be enabled.

Step 5 Configure the VLAN transparent transmission function.

In transparent transmission, the system does not process specified types of protocol packets but transparently transmits them.

- Run the **bpdu tunnel** command to configure the BPDU transparent transmission switch. After transparent transmission is enabled, the Layer 2 BPDUs of the private network can be transmitted transparently over the public network.
- Run the **vtp-cdp tunnel** command to configure the VTP/CDP packet transparent transmission switch. After the switch is enabled, VTP/CDP packets are transparently transmitted based on the VLAN.

- Run the **rip tunnel** command to configure the RIP Layer 2 transparent transmission switch. After the transparent transmission switch is enabled, RIP packets can be transparently transmitted at Layer 2 based on VLAN on the device without running the RIP protocol.
- Run the **ospf tunnel** command to configure the OSPF Layer 2 transparent transmission switch. After the transparent transmission switch is enabled, OSPF packets can be transparently transmitted at Layer 2 based on VLAN on the device without running the OSPF protocol.
- Run the **l3-protocol tunnel** command to configure the L2 transparent transmission for the L3 protocol packets except RIP and OSPF packets. After this function is enabled, the L3 protocol packets can be transparently transmitted at Layer 2 based on VLAN on the device without running the L3 protocol.
- Run the **ipv6 dad proxy** command to configure the DAD proxy (duplicate address detect proxy). DAD proxy prevents repeated LLA configuration on the user side.

Step 6 Configure the VLAN security function.

The security function is used to prevent malicious users from attacking the system by forging the IP address or MAC address of an authorized user. VMAC and anti-MAC spoofing conflict with S+C forwarding.

- Run the **security anti-ipspoofing** command to configure the anti-IPv4 spoofing function. After the anti-IPv4 spoofing function is enabled, the system automatically and dynamically binds the IPv4 address to the user. The packet can be transmitted upstream through the device only when the source IPv4 address of the packet is the same as the bound IPv4 address. Otherwise, the packet is discarded.
- Run the **security anti-ipv6spoofing** command to configure the anti-IPv6 spoofing function. After the anti-IPv6 spoofing function is enabled, the system automatically and dynamically binds the IPv6 address to the user. The packet can be transmitted upstream through the device only when the source IPv6 address of the packet is the same as the bound IPv6 address. Otherwise, the packet is discarded.
- Run the **security anti-macspoofing** command to configure the anti-MAC spoofing function. After the anti-MAC spoofing function is enabled, the system automatically and dynamically binds the MAC address to the traffic stream. When the source MAC address of the traffic stream is the same as the bound MAC address, the traffic stream can be upstream transmitted through the device. Otherwise, the packets are discarded.
- Run the **security arp-reply** command to enable the network-side ARP proxy response function. If the network-side ARP proxy response function is enabled, the system searches for user's going online information based on the destination IP address and VLAN after it receives network-side ARP request packets. If there is an online user, the system performs proxy response. If there is no online user, the system discards or forwards the ARP request packets based on the setting in the **security arp-reply unknown-policy** command. This prevents ARP request packets from being sent to user ports and reduces system resources.
- Run the **security ns-reply** command to enable the network-side NS proxy response function. If network-side NS proxy reply is enabled, the system searches for user's going online information based on the destination IP address and VLAN after it receives network-side NS packets. If there is an online user, the system performs proxy response. If there is no online user, the system discards or forwards the NS packets based on the setting in the **security ns-reply unknown-policy** command. This prevents NS packets from being sent to user ports and reduces system resources.
- Run the **security bind-route-nd** command to configure the function of binding route with neighbor entry. After the function of binding route with neighbor entry is enabled, the system automatically generates the route and neighbor entry of a DHCPv6 user based on the user

information recorded when the user goes online. This function reduces the effort of configuring static routes manually, prevents neighbor packets from being sent to the user side, and enhances system security.

- Run the **vmac** command to enable or disable VMAC. By default, VMAC is disabled.

Step 7 Commit to save the current parameters.

Run the **commit** command to commit the current parameter configuration of the VLAN service profile. After the configuration is completed, do run the **commit** command to make the configuration take effect.

Step 8 Bind the VLAN service profile to the VLAN.

Run the **vlan bind service-profile** command to bind the configured VLAN service profile to a specified VLAN. After the binding, the VLAN-level feature control switch is based on the configuration of the VLAN service profile. Independent configuration commands for VLAN-based features are no longer effective.

----End

Result

You can query the configuration of the VLAN service profile by the **display vlan service-profile** command.

After a VLAN service profile is bound to a VLAN, regarding the parameters whose **Committed** state is **NotConfig**, the configuration commands that are independent of the VLAN take effect; other parameters adopt the control parameters of the profile. Modifying the feature parameters relevant to the VLAN does not take effect.

Example

Add VLAN service profile 3 and bind it to VLAN 100. The profile parameters are planned as follows:

- VLAN forwarding mode VLAN+MAC address (vlan-mac)
- BPDU transparent transmission: enabled
- Unknown multicast packet: discarded

Adopt the default values for other parameters.

```
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#forwarding vlan-mac
huawei(config-vlan-srvprof-3)#bpdu tunnel enable
huawei(config-vlan-srvprof-3)#packet-policy multicast discard
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
huawei(config)#vlan bind service-profile 100 profile-id 3
```

2.7 Configuring the User Security

Configuring the security mechanism can protect operation users and access users against user account theft and roaming or from the attacks from malicious users.

Context

The user security mechanism includes:

- PITP: The purpose of the PITP feature is to provide the user physical location information for the upper-layer authentication server. After the BRAS obtains the user physical location information, the BRAS binds the information to the user account for authentication, protecting the user account against theft and roaming.
- DHCP option 82: The user physical location information is added to the option 82 field in the DHCP request sent by the user. The information is used by the upper-layer authentication server for authenticating the user, protecting the user account against theft and roaming.
- IP address binding: The IP address of the user is bound to the corresponding service port for authenticating the user, ensuring the security of the authentication.
- MAC address binding: The MAC address is bound to the service port, preventing the access of illegal users.
- Anti-MAC spoofing: It is a countermeasure taken by the system to prevent a user from attacking the system with a forged MAC address.
- Anti-IP spoofing: It is a countermeasure taken by the system to prevent a user from attacking the system with a forged IP address.

Table 2-12 lists the default settings of the user security mechanism.

Table 2-12 Default settings of the user security mechanism

Parameter	Default Setting	Remarks
PITP	Global function: disabled Port-level function: enabled VLAN-level function: enabled Service-port-level function: enabled	The PITP function can be enabled only when the functions at all levels are enabled.
DHCP option 82	Global function: disabled Port-level function: enabled VLAN-level function: enabled Service-port-level function: enabled	The DHCP option 82 function can be enabled only when the functions at all levels are enabled.
Anti-IP spoofing	Global function: disabled Service-port-level function: enabled VLAN-level function: enabled	The anti-IP spoofing function can be enabled only when the functions at all levels are enabled.
Anti-MAC spoofing	Global function: disabled VLAN-level function: disabled Service-port-level status: enabled By default, up to eight MAC addresses can be bound.	The anti-MAC spoofing function can be enabled only when the functions at all levels are enabled.

2.7.1 Configuring Anti-Theft and Roaming of User Account Through PITP

Policy Information Transfer Protocol (PITP) is mainly used for the user PPPoE dialup access. It is a protocol defined for transferring policy information between the access device and the

Broadband Remote Access Server (BRAS) through Layer 2 P2P communication. PITP can be used for transferring the user physical port information and protecting the user account against theft and roaming.

Application Context

PITP is used for providing the user port information for the BRAS. After the BRAS obtains the user port information, the BRAS binds the user account to the user port, protecting the user account against theft and roaming. PITP has two modes, the PPPoE+ mode (also called the PITP P mode) and the VBAS mode (also called the PITP V mode).

PITP is applicable to the networking of a standalone MA5600T/MA5603T and the networking of subtended MA5600T/MA5603Ts.

- In the networking of a standalone MA5600T/MA5603T: Two PCs (PC1 and PC2) are connected to different ports of the MA5600T/MA5603T for the dialup access.
- In the networking of subtended MA5600T/MA5603Ts: Two PCs (PC1 and PC2) are connected to different MA5600T/MA5603Ts (PC1 is connected to the MA5600T/MA5603T, and PC2 is connected to the MA5600T/MA5603T through a subtended device) for the dialup access.

The principles in the two scenarios are similar. The user dials up from PC1 by using the corresponding user account. The BRAS binds the user account to the user's physical port information reported by the MA5600T/MA5603T. When the user of PC2 dials up by using the user account of PC1, the BRAS discovers that the user account does not match the physical port information and therefore rejects the dialup access request of PC2.

Default Configuration

Table 2-13 lists the default settings related to PITP.

Table 2-13 Default settings related to PITP

Parameter	Default Setting
PITP function	Global function: disabled Port-level function: enabled VLAN-level function: enabled Service-port-level function: enabled
PITP sub-option 90	Disabled
User-side PPPoE packet carrying the vendor tag information	Disabled

Procedure

Step 1 Configure the relay agent information option (RAIO). Before using the PITP function, you must configure RAIO.

NOTE

You can configure RAIO in the global config mode or RAIO profile mode. If an RAIO profile is bound to a VLAN, the RAIO configuration in the RAIO profile mode takes effect. If the RAIO profile is not bound to any VLAN, the RAIO configuration in the global config mode takes effect.

- Run the **raio-mode** ***mode*** **pitp-pmode** command to configure the RAIO mode in the PITP P mode.
- Run the **raio-mode** ***mode*** **pitp-vmode** command to configure the RAIO mode in the PITP V mode.

The PITP P mode supports all the RAIO modes; the PITP V mode currently supports only the common, cntel, and userdefine modes. When the auto-sensing traffic stream is configured, fill in 8191.35 as the VPI/VCI of the tag, regardless of whether the traffic stream has learned the VPI/VCI or not.

user-defined: indicates the user-defined mode. In this mode, you need to run the **raio-format** command to configure the RAIO format. Select a corresponding keyword for configuring the RAIO format according to the PITP mode.

- In the PITP P mode, run the **raio-format pitp-pmode** command to configure the RAIO format.
- In the PITP V mode, run the **raio-format pitp-vmode** command to configure the RAIO format.

In the case of the user-defined RAIO format, configure the circuit ID (CID) and the remote ID (RID). If the access mode is not selected, the configured format applies to all access modes. If the access mode is selected, the configured format applies to only this access mode. The CID format and RID format in the PITP V mode are the same:

- CID: identifies the attribute information about the device.
- RID: identifies the access information about the user.

Step 2 Configure the PITP function.

The PITP function can be enabled or disabled at four levels. The PITP function is enabled only when it is enabled at all the four levels. The global PITP function has higher priority over the port-level and service-port-level PITP functions.

1. Global PITP function: Run the **pitp enable pmode** command to enable global PITP P mode. By default, the global PITP function is disabled.

   In the PITP V mode, run the **pitp vmode ether-type** command to set the Ethernet protocol type to be the same as that of the BRAS. Then, run the **pitp enable vmode** command to enable global PITP V mode.

   NOTE

   The Ethernet protocol type of the PITP V mode must be configured when the PITP V mode is disabled.
2. Port-level PITP function: Run the **pitp port** or **pitp board** command to configure the port-level PITP function. By default, the port-level PITP function is enabled.
3. VLAN-level PITP function:
   a. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
   b. Run the **pitp enable** command to enable the PITP function of the VLAN. By default, the PITP function of the VLAN is enabled.

c. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after this command is executed.

d. Run the **quit** command to quit the VLAN service profile mode.

e. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile configured.

4. Service-port-level PITP function: Run the **pitp service-port** command to enable the service-port-level PITP function. By default, the service-port-level PITP function is enabled.

Step 3 Configure the optional attributes of PITP.

- Run the **pitp permit-forwarding service-port** command to set whether the service port allows the user-side PPPoE packet carrying the vendor tag information. By default, this function is disabled, that is, the user-side PPPoE packet carrying the vendor tag information is not allowed.

  The system adds a tag containing the device name, subrack ID, slot ID, and port ID to the PPPoE+ upstream PADI and PADR packets to generate new packets. If this function is enabled, tagged packets are forwarded. If this function is disabled, tagged packets are discarded.

  When the PITP function is applied to the OLT+ONU network, pay attention to the following points:

  1. When the PITP function is enabled only on the OLT, the tag of the PADI packet contains only the information about the PON port of the OLT.
  2. When the PITP function is enabled only on the ONU, the tag of the PADI packet contains only the information about the user port of the ONU.
  3. If the PITP function is enabled on both the OLT and the ONU, a function (through the **pitp permit-forwarding service-port** command) is used to choose which tag the PADI packet carries.
     - When this function is enabled, the tag of the PADI packet contains only the information about the PON port of the OLT.
     - When this function is disabled, subscribers connected to the ONU fail to dial the number. That is, the PADI packet (PITP P mode) cannot be transmitted.

  The PON board of the OLT can be connected to the terminals such as the ONT and the ONU. Generally, the PITP function is enabled on the OLT in the global mode. Certain PON ports are connected to ONUs. For example, in the FTTB application, however, the MDUs are connected to multiple subscribers. For the OLT, an MDU is one subscriber, regardless of how many subscribers are connected to the MDU. In this case, to differentiate subscribers connected to the MDU, you need to enable the PITP function on the MDU.

- Run the **pitp sub-option90** command to configure PITP sub-option 90. By default, PITP sub-option 90 is disabled.

  The PPPoE+ mode supports reporting the sub-option 90 line parameters, including the activation bandwidth. Enable or disable PITP sub-option 90 according to actual requirements. The configuration of PITP sub-option 90 takes effect only in the PITP P mode; the PITP V mode does not support reporting the line parameters.

----End

Example

Assume the following configuration:

- RAIO mode: user-defined mode
- CID format for the ATM access mode: subrack ID/slot ID/port ID:VPI.VCI
- CID format for the Ethernet access mode: subrack ID/slot ID/port ID:VLAN ID
- CID format for the xPON access mode: subrack ID/slot ID/port ID:ONT ID.VLAN ID
- RID format is the label of the subscriber port.

To enable the PITP P mode of service port 1 under port 0/2/0, do as follows:

```
huawei(config)#raio-mode user-defined pitp-pmode
huawei(config)#raio-format pitp-pmode cid atm anid atm frame/slot/port:vpi.vci
huawei(config)#raio-format pitp-pmode cid eth anid eth frame/slot/port:vlanid
huawei(config)#raio-format pitp-pmode cid xpon anid xpon frame/slot/
port:ontid.vlanid
huawei(config)#raio-format pitp-pmode rid atm plabel
huawei(config)#raio-format pitp-pmode rid eth plabel
huawei(config)#raio-format pitp-pmode rid xpon plabel
huawei(config)#pitp enable pmode
huawei(config)#pitp port 0/2/0 enable
huawei(config)#pitp service-port 1 enable
huawei(config)#raio-mode user-defined pitp-pmode
huawei(config)#raio-format pitp-pmode cid eth anid eth frame/slot/port:vlanid
huawei(config)#raio-format pitp-pmode cid xpon anid xpon frame/slot/
port:ontid.vlanid
huawei(config)#raio-format pitp-pmode rid eth plabel
huawei(config)#raio-format pitp-pmode rid xpon plabel
huawei(config)#pitp enable pmode
huawei(config)#pitp port 0/2/0 enable
huawei(config)#pitp service-port 1 enable
```

Assume the following configuration:

- RAIO profile ID: 10
- RAIO mode: user-defined mode
- CID/RID format for the ATM access mode: subrack ID/slot ID/port ID:VPI.VCI
- CID/RID format for the Ethernet access mode: subrack ID/slot ID/port ID:VLAN ID
- CID/RID format for the xPON access mode: subrack ID/slot ID/port ID:ONT ID.VLAN ID
- Service port 0: in VLAN 11

To set the Ethernet protocol type of VBRAS packets to be the same as that of the upper-layer BRAS, that is, 0x8500, and enable the PITP V mode of service port 0, do as follows:

```
huawei(config)#raio-profile index 10
huawei(config-raio-profile-10)#raio-mode user-defined pitp-vmode
huawei(config-raio-profile-10)#raio-format pitp-vmode atm anid atm frame/slot/
port:vpi.vci
huawei(config-raio-profile-10)#raio-format pitp-vmode eth anid eth frame/slot/
port:vlanid
huawei(config-raio-profile-10)#raio-format pitp-vmode xpon anid xpon frame/slot/
port:ontid.vlanid
huawei(config-raio-profile-10)#quit
huawei(config)#vlan bind raio-profile 11 index 10
huawei(config)#pitp vmode ether-type 0x8500
huawei(config)#pitp enable vmode
huawei(config)#pitp port 0/2/0 enable
huawei(config)#pitp service-port 0 enable
```

2.7.2 Configuring Anti-Theft and Roaming of User Accounts Through DHCP

Dynamic Host Configuration Protocol (DHCP) improves the user authentication security by adding the user physical location information to the option 82 field of the DHCP request packets initiated by the user, so as to prevent theft and roaming of the user account.

Context

The option 82 field contains the circuit ID (CID), remote ID (RID), and sub-option 90 field (optional), which provides the information such as the user subrack ID, slot ID, port ID, VPI, and VCI.

The MA5600T/MA5603T can work in the Layer 2 DHCP forwarding mode or Layer 3 DHCP forwarding mode. In either mode, anti-theft and roaming of user accounts through DHCP option 82 can be configured, and the configurations are the same.

Table 2-14 lists the default settings related to DHCP option 82.

Table 2-14 Default settings related to DHCP option 82

Parameter	Default Setting
Status of the DHCP option 82 function	Global status: disabled Port-level status: enabled VLAN-level status: enabled Service-port-level status: enabled
Status of the DHCP sub-option 7 function	Disabled
Status of the DHCP sub-option 90 function	Disabled

Procedure

Step 1 Configure the relay agent info option (RAIO). The RAIO is the short form for relay agent information option. Before using the DHCP function, you must configure the RAIO.

NOTE

You can configure RAIO in the global config mode or RAIO profile mode. If an RAIO profile is bound to a VLAN, the RAIO configuration in the RAIO profile mode takes effect. If the RAIO profile is not bound to any VLAN, the RAIO configuration in the global config mode takes effect.

Run the **raio-mode** command to set the RAIO mode.

- Select **dhcp-option 82** as the corresponding mode.
- In the user-defined mode, you need to run the **raio-format** command to configure the RAIO format, and select **dhcp-option 82** as the corresponding mode. To configure the user-defined format, mainly configure the RID in the CID. If the access mode is not selected, the configured format is valid to all access modes. If the access mode is selected, the configured format is valid to only this access mode. For details about the RAIO format, see the **raio-format** command.

- CID identifies the attribute information of the device.
- RID identifies the access information of the user.

Step 2 (Optional) Set the service port to allow or prohibit the user-side DHCP packets that carry the option 82 information.

- Run the **dhcp-option82 permit-forwarding service-port** command to set the service port to allow or prohibit the DHCP packets that carry the option 82 information.

  The system adds the device name, subrack ID, slot ID, and port ID to the option 82 field of DHCP packets to generate new packets. If the service port is set to allow the packets carrying the option 82 information, tagged packets are forwarded. If the service port is set to prohibit the packets carrying the option 82 information, tagged packets are dropped.

Step 3 Enable or disable the DHCP option 82 function.

Run the **dhcp option82** command to enable the DHCP option 82 function on the port. By default, the DHCP option 82 function is disabled globally.

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. System level: Run the **dhcp option82** command to enable the DHCP option 82 function globally. By default, the DHCP option 82 function is disabled globally.
2. Port level: Run the **dhcp option82 board** or **dhcp option82 port** command to enable the DHCP option 82 function for a board or port. By default, the DHCP option 82 function for a board or port is enabled.
3. VLAN level:
   a. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
   b. Run the **dhcp option82** command to enable the DHCP option 82 function. By default, the DHCP option 82 function is enabled.
   c. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after you run this command.
   d. Run the **quit** command to quit the VLAN service profile mode.
   e. Run the **vlan bind service-profile** command to bind the VLAN service profile created in **3.3.a** to the VLAN.
4. Service port level: Run the **dhcp option82 service-port** command to enable the DHCP option 82 function for a service port. By default, the DHCP option 82 function for a service port is enabled.

Step 4 (Optional) Enable or disable the sub-option function.

In the DHCP mode, reporting the sub-option 90 line parameters, including reporting the activation bandwidth, is supported. Enable or disable the sub-option function according to your requirements. In the DHCP option 82 mode, sub-option 81 to sub-option 91 in sub-option 9 need to be filled.

1. Run the **dhcp sub-option7** command to enable or disable the sub-option 7 function. By default, the sub-option 7 function is disabled.
2. Run the **dhcp sub-option90** command to enable or disable the sub-option 90 function. By default, the sub-option 90 function is disabled.

----End

Example

To enable the DHCP option 82 function to improve user security by assuming the following:

- RAIO mode: user-defined mode
- CID format for the ETH access mode: subrack ID/slot ID/sub slot ID/port ID: vlanid
- CID format for the xPON access mode: subrack ID/slot ID/sub slot ID/port ID: ontid.vlanid
- RID format for all access modes: label of the service port

do as follows:

```
huawei(config)#raio-mode user-defined dhcp-option 82
huawei(config)#raio-format dhcp-option 82 cid eth anid eth frame/slot/subslot/
port:vlanid
huawei(config)#raio-format dhcp-option 82 cid xpon anid xpon frame/slot/subslot/
port:ontid.vlanid
huawei(config)#raio-format dhcp-option 82 rid eth splabel
huawei(config)#raio-format dhcp-option 82 rid xpon splabel
huawei(config)#dhcp option 82 enable
```

To enable the DHCP option 82 function in VLAN 11 to improve user security by assuming the following:

- RAIO profile ID: 10
- RAIO mode: port-userlabel mode

```
huawei(config)#raio-profile index 10
huawei(config-raio-profile-10)#raio-mode port-userlabel dhcp-option82
huawei(config-raio-profile-10)#quit
huawei(config)#vlan bind raio-profile 11 index 10
huawei(config)#dhcp option82 enable
```

2.7.3 Configuring Anti-IP Spoofing

This topic describes how to configure IP address binding and anti-IP spoofing to prevent malicious users from attacking the device or authorized users by forging the IP addresses of authorized users.

Context

IP address binding refers to binding an IP address to a service port. After the binding, the service port permits only the packet whose source IP address is the bound address to go upstream, and discards the packets that carry other source IP addresses.

Anti-IP spoofing is to dynamically trigger the IP address binding, preventing illegal users from stealing the IP address of legal users. When anti-IP spoofing is enabled, a user port is bound to an IP address after the user goes online. Then, the user cannot go online through this port by using other IP addresses, and any user cannot go online through other ports by using this IP address.

Procedure

- Configure the IP address binding.

  Run the **bind ip** command to bind an IP address to a service port.

  To permit only the users of certain IP addresses to access the system so that illegal users cannot access the system by using the IP addresses of legal users, configure the IP address binding.

- Configure anti-IP spoofing.

  When the service flow binds to a VLAN service profile, anti-IP spoofing takes effect only when all its three levels are enabled.

  When the service flow does not bind to any VLAN service profile, anti-IP spoofing takes effect only when two levels of anti-IP spoofing functions (the VLAN level function is not included) are enabled.

  - Global function: Run the **security anti-ipspoofing** command to configure the global function. By default, the global function is disabled.
  - The VLAN-level function and the service-port-level function are enabled by default. When the global function is enabled, anti-IP spoofing is effective to all the service flows of the system. To disable anti-IP spoofing for a service flow in this case, do as follows:
    - If the VLAN of the service flow is bound to a VLAN service profile and the VLAN service profile specifies that all of its service flows must disable anti-IP spoofing, disable the VLAN-level function for VLANs bound to this profile.
    - If only anti-IP spoofing of the service flow needs to be disabled, disable the service-port-level function.
  - VLAN-level function:
    1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
    2. Run the **security anti-ipspoofing** command to configure the VLAN-level function. By default, the VLAN-level function is enabled.
    3. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after this command is executed.
    4. Run the **quit** command to quit the VLAN service profile mode.
    5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile configured in **1**.
  - Service-port-level function: Run the **security anti-ipspoofing service-port** command to configure the service-port-level function. By default, the service-port-level function is enabled.

  NOTE

  When anti-IP spoofing is enabled after a user is already online, the IP address of this user is not bound by the system. As a result, the service of this user is interrupted, this user goes offline, and the user needs to go online again. Only the user who goes online after anti-IP spoofing is enabled can have the IP address bound.

----End

Example

To bind IP address 10.1.1.245 to service port 2, that is, service port 2 permits only the packet whose source IP address is 10.1.1.245, do as follows:

```
huawei(config)#bind ip service-port 2 10.1.1.245
```

To enable anti-IP spoofing for service port 1 in service VLAN 10, do as follows:

```
huawei(config)#security anti-ipspoofing enable
huawei(config)#vlan service-profile profile-id 2
huawei(config-vlan-srvprof-2)#security anti-ipspoofing enable
```

```
  Info: Please use the commit command to make modifications take effect
huawei(config-vlan-srvprof-2)#commit
huawei(config-vlan-srvprof-2)#quit
huawei(config)#vlan bind service-profile 10 profile-id 2
huawei(config)#security anti-ipspoofing service-port 1 enable
```

2.7.4 Configuring Anti-MAC Spoofing

This topic describes how to configure MAC address binding, anti-MAC spoofing, anti-MAC duplicate, and virtual MAC (VMAC) address to prevent malicious users from attacking the device or authorized users by forging the MAC addresses of authorized users.

Context

Static MAC address binding refers to binding a static MAC address to a service port. After the binding, only the user whose MAC address is the bound MAC address can access the network through the service port. The MA5600T/MA5603T does not support the direct binding of a MAC address. Instead, the binding between a service port and a MAC address is implemented through setting a static MAC address entry of a port and setting the maximum number of learnable MAC addresses to 0.

Dynamic MAC address binding is implemented by the MAC spoofing function. Dynamic MAC address binding means that dynamic MAC addresses are bound to service ports, so only the packets whose source MAC address is the same as the bound MAC address can access the network. The purpose is to ensure that the services of legal users are not affected by preventing malicious users forging the MAC address of legal users. Anti-MAC spoofing is mainly applied to PPPoE and Dynamic Host Configuration Protocol (DHCP) access users.

VMAC adopts the trusty virtual MAC address allocated by the MA5600T/MA5603T to replace the source MAC addresses of terminal users and prevents untrusty MAC addresses from entering the network, preventing MAC address conflict and MAC address spoofing from malicious users.

The anti-MAC-duplicate function does not allow dynamic MAC addresses to be duplicated before they are aged. In this way, when MAC address conflicts occur between different users, the user that goes online first will not be affected.

Procedure

- Configure the static MAC address binding.
  1. Run the **mac-address static** command to add a static MAC address.
  2. Run the **mac-address max-mac-count** command to set the maximum number of learnable MAC addresses to 0.

     This parameter is to limit the maximum number of the MAC addresses that can be learned through one account, that is, to limit the maximum number of the PCs that can access the Internet through one account.
- Configure the dynamic MAC address binding.

  ⚠ **CAUTION**

  To ensure device security, it is recommended that you enable this function.

  – Dynamic MAC address binding is implemented by the MAC spoofing function.

- The anti-MAC spoofing function can be enabled or disabled at three levels. The anti-MAC spoofing function is enabled only when it is enabled at all the three levels.

- Global function: Run the **security anti-macspoofing** command to configure the global function. By default, the global function is disabled.
- You can configure the VLAN-level function in either of the following two modes:
  - In the global config mode: Run the **security anti-macspoofing vlan** command to configure the VLAN-level function. By default, the VLAN-level function is disabled.
  - In the VLAN service profile:
    1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
    2. Run the **security anti-macspoofing** command to configure the VLAN-level function. By default, the VLAN-level function is disabled.
    3. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after this command is executed.
    4. Run the **quit** command to quit the VLAN service profile mode.
    5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile configured in **1**.
- Service-port-level function: Run the **security anti-macspoofing max-mac-count** command to configure the maximum number of MAC addresses that can be bound to the service port. By default, up to eight MAC addresses can be bound.

NOTE

When anti-MAC spoofing is enabled after a user is already online, the MAC address of this user is not bound by the system. As a result, the service of this user is interrupted, this user goes offline, and the user needs to go online again. Only the user who goes online after anti-MAC spoofing is enabled can have the MAC address bound.

- Configure 1:1 VMAC. Use the xDSL access as an example.
  1. Configure VMAC-related attributes.
     a. Run the **vmac dslam-id** command to configure the DSLAM ID.

        The DSLAM ID is bits 21-39 of the VMAC address, 19 bits in total. VMAC can be enabled only when *dslam-id* is in the range of 0x0000-0x7FFFF.

        NOTE

        The uniqueness of the DSLAM ID must be ensured by the configuration engineer to prevent allocating the same VMAC address to two DSLAMs.

     b. (Optional) Run the **vmac port-vmac-count** command to configure the number of VMAC addresses on each port.

        To limit the number of VMAC addresses on each port, run this command. By default, the number of VMAC addresses on each port is 32.

     c. (Optional) Run the **vmac reserved-bits** command to configure the reserved bits of the VMAC address.

        This command is used to set the value of the reserved bits (bits 47-42) in the VMAC address generating format. The VMAC value is made up of the value of reserved bits and other bits. To enable VMAC, the value of the reserved bits must be in the range of [0x0,0x3F]. Otherwise, VMAC fails to be enabled. By default, the value is 0x0.

2. (Optional) Configure the mode for allocating MAC addresses to xPoE/xPoA users.

   The xPoE/xPoA MAC address can be allocated in two modes: single-MAC or multi-MAC (default). When VMAC is enabled:

   - Single-MAC: Also called N:1 VMAC. The device uses a unique VMAC address to replace the MAC addresses of a group of users. The relationship between user MAC address and device VMAC address is N:1.
   - Multi-MAC: Also called 1:1 VMAC. The device uses a unique VMAC address to replace the MAC address of a single user. The relationship between user MAC address and device VMAC address is 1:1.

   NOTE

   - If VMAC is disabled, the PPPoA and IPoA MAC addresses are obtained from the configured MAC address pool (by running the **mac-pool** command).
   - IPoA does not supports obtaining the MAC address through VMAC and supports obtaining the MAC address from the MAC address pool only.

   The MAC address allocation mode has two levels: global level and VLAN service profile level.

   a. Configure the global MAC address allocation mode.
      - Run the **pppoa mac-mode** command to configure the MAC address allocation mode for PPPoA users.
      - Run the **pppoe mac-mode** command to configure the MAC address allocation mode for PPPoE users.

   b. Configure the MAC address allocation mode at the VLAN service profile level.

      When VMAC is enabled, the xPoA/xPoE MAC allocation mode can be set to multi-MAC only.

      a. In the global config mode, run the **vlan service-profile** command to enter the VLAN service profile mode.
      b. Run the **pppoe mac-mode** command to configure the MAC address allocation mode for PPPoE users.
      c. Run the **pppoa mac-mode** command to configure the MAC address allocation mode for PPPoA users.

3. Enable VMAC.

   Run the **vmac enable** command to enable VMAC. After VMAC is enabled, the VMAC address is generated according to the DSLAM ID, slot ID, and port ID.

   VMAC can be enabled for the system or for the VLAN service profile. VMAC takes effect only when it is enabled at two levels.

   a. In the global config mode, run the **vmac enable** command to enable VMAC.
   b. Run the **vlan service-profile** command to enter the VLAN service profile mode.
   c. Run the **vmac enable** command to enable VMAC at the VLAN service profile level.
   d. Run the **commit** command to commit the configuration.

- Configure N:1 VMAC. Use the xPON access as an example.

  1. Configure VMAC-related attributes.

     a. Run the **vmac dslam-id** command to configure the OLT ID.

The OLT ID identifies an OLT. A reliable MAC address needs to be generated to replace the user MAC address.

NOTE

You must ensure the uniqueness of the OLT ID and do not allocate the same VMAC to two OLT IDs.

b. (Optional) Run the **vmac ont-vmac-count** command to configure the number of VMAC addresses on each port.

   To limit the number of VMAC addresses on an ONT, run this command. By default, the number of VMAC addresses on each ONT is 8.

c. (Optional) Run the **vmac reserved-bits** command to configure the reserved bits of the VMAC address.

   Configure values of the reserved bits (bits 47-42) in the VMAC generating format. The values of the reserved bits and other fields form the VMAC value. The values of the reserved bits must be within the range of [0x0, 0x3F] when the VMAC feature is enabled. Otherwise, the VMAC feature cannot be enabled. The default value is 0.

2. (Optional) Configure the MAC address allocation mode for xPoE users.

   The MAC address allocation mode for xPoE users can be single-MAC or multi-MAC (default). When VMAC is enabled:

   - Single-MAC (that is, N:1 VMAC): The device uses a unique VMAC address to replace the MAC addresses of a group of users. N user MAC addresses map one device VMAC.
   - Multi-MAC (that is, 1:1 VMAC): The device uses a unique VMAC address to replace the MAC address of a single user. One user MAC address maps one device VMAC.

   The MAC address allocation mode is controlled at the VLAN level and the global level. The allocation mode takes effect only when it is enabled at both levels.

   - In the global config mode, run the **pppoe mac-mode** command to configure the MAC address allocation mode at the global level.
   - In the global config mode, run the **pppoe vlan vlanid mac-mode** command to configure the MAC address allocation mode at the VLAN level. Or, in the VLAN service profile mode, run the **pppoe mac-mode** command to configure the MAC address allocation mode at the VLAN level.

3. Enable VMAC. After you enable the VMAC feature, the VMAC address is generated based on the OLT ID, slot ID, port ID, and ONT.

   The VMAC function is controlled at the VLAN level and the global level. The VMAC function takes effect only when it is enabled at both levels.

   - In the global config mode, run the **vmac enable** command to enable the global VMAC function.
   - In the VLAN service profile mode, run the **vlan service-profile** command to enter the VLAN service profile mode.
   - Run the **vmac enable** command to enable the VMAC function of the VLAN service profile.
   - Run the **commit** command to save the configuration.

- Configure the anti-MAC-duplicate function.

After the anti-MAC-duplicate function is enabled and before the dynamic MAC address learned by the system is aged, the packets transmitted from other ports will be discarded if the packets carry the same MAC address.

NOTE

- By default, the system disables anti-MAC-duplicate, that is, MAC address duplicate is allowed.
- If the system uses the SCUN/SCUH control board, the system enables anti-MAC-duplicate from the network side to the user side, disables anti-MAC-duplicate from the user side to the network side, and does not allow users to modify or delete these settings. That is, regardless of the status of anti-MAC-duplicate, the system prohibits MAC-duplicate from the network side to the user side but allows MAC-duplicate from the user side to the network side.
- If the system uses the SCUN/SCUH control board, this command is used to configure anti-MAC-duplicate between ports on the network side and anti-MAC-duplicate between ports on the user side. If the system uses the control boards such as SCUL, SCUF, and SCUB, this command is used to configure anti-MAC-duplicate on the network side, which includes anti-MAC-duplicate between ports on the network side and anti-MAC-duplicate from the network side to the user side.
- For the SCUL, SCUF, and SCUB control boards, run the **security anti-macduplicate** command to prevent MAC address transfer after enabling anti-MAC spoofing.

1. Run the **security anti-macduplicate** command to enable anti-MAC duplicate.
2. Run the **display security config** command to query the configuration.

----End

Example

To bind static MAC address 1010-1010-1010 to service port 1, and set the maximum number of learnable MAC addresses to 0, that is, service port 1 permits only the packet whose source MAC address is 1010-1010-1010, do as follows:

```
huawei(config)#mac-address static service-port 1 1010-1010-1010
huawei(config)#mac-address max-mac-count service-port 1 0
```

To enable anti-MAC spoofing for VLAN 10, and set the maximal number of MAC address bound to service port 2 (related to VLAN 10) to 7.

```
huawei(config)#security anti-macspoofing enable
huawei(config)#security anti-macspoofing vlan 10 enable
huawei(config)#security anti-macspoofing max-mac-count service-port 2 7
```

In the xDSL access, to enable the VMAC function of VLAN 10 to improve the PPPoE user security and set the MAC address allocation mode to 1:1 VMAC, do as follows:

```
huawei(config)#vmac dslam-id 0x0e02
huawei(config)#vmac port-vmac-count 16
huawei(config)#vmac reserved-bits 0x01
huawei(config)#pppoe mac-mode multi-mac
huawei(config)#vmac enable
huawei(config)#vlan service-profile profile-id 2
huawei(config-vlan-srvprof-2)#pppoe mac-mode multi-mac
huawei(config-vlan-srvprof-2)#vmac enable
huawei(config-vlan-srvprof-2)#commit
huawei(config-vlan-srvprof-2)#quit
huawei(config)#vlan bind service-profile 10 profile-id 2
```

In the xPON access, to enable the VMAC function of VLAN 20 to improve the PPPoE user security and set the MAC address allocation mode to N:1 VMAC, do as follows:

```
huawei(config)#vmac dslam-id 0x0e01
huawei(config)#vmac port-vmac-count 4
huawei(config)#vmac reserved-bits 0x01
huawei(config)#pppoe mac-mode single-mac
huawei(config)#vmac enable
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#pppoe mac-mode single-mac
huawei(config-vlan-srvprof-3)#vmac enable
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
huawei(config)#vlan bind service-profile 20 profile-id 3
```

To enable anti-MAC duplicate so that the user that goes online first will not be affected when MAC address conflicts occur between different users, do as follows:

```
huawei(config)#security anti-macduplicate enable
huawei(config)#display security config
   Anti-ipspoofing function                          : disable
   Anti-dos function                                 : disable
   Anti-macspoofing function                         : disable
   Anti-macspoofing control-protocol IPv6oE function : disable
   Anti-ipattack function                            : disable
   Anti-icmpattack function                          : disable
   Source-route filter function                      : disable
   Anti-macduplicate function                        : enable
   PPPoE overall aging time(sec)                     : 360
   PPPoE aging period(sec)                           : 90
   ARP detect mode                                   : dummy
   Anti-dos control-packet policy                    : deny
   Packet unaffected by anti-ipspoofing              : --
   Packet unaffected by anti-macspoofing             : IGMP
   NS-reply function                                 : disable
   NS-reply unknown-policy                           : forward
   ARP-reply function                                : disable
   ARP-reply unknown-policy                          : forward
   Anti-ipv6spoofing function                        : disable
   IPv6 ND detect mode                               : gateway
   IPv6 DAD proxy function                           : disable
   IPv6 bind route and ND                            : disable
   DHCP client identifier                            : chaddr
```

2.8 Configuring System Security

This topic describes how to configure the network security and protection measures of the system to protect the system from malicious attacks.

Context

With the system security feature, the MA5600T/MA5603T can be protected against the attacks from the network side or user side, and therefore the MA5600T/MA5603T can run stably in the network. System security includes the following items:

- ACL/Packet filtering firewall
- Blacklist
- Anti-DoS attack
- Anti-ICMP/IP attack
- Source route filtering
- Source MAC address filtering
- User-side ring network detection
- Allowed/Denied address segment

The following common inappropriate configurations affect the system security:

- The ring network detection and anti-address spoofing functions are not enabled. If the anti-address spoofing function is not enabled, an unauthorized user may forge the MAC address of an authorized user to send PPPoE or DHCP control packets, threatening the system security.

  Preventive methods or measures:

  - Run the **ring check** command to enable the function of checking user-side ring networks.
  - Run the **security anti-macspoofing enable** command to enable the anti-MAC spoofing.
- Use a public network address to manage the device. The access rights are not strictly limited when the ACL is configured. Therefore, the network may be attacked.

  Preventive methods or measures:

  - Use a private network address to manage the device.
  - When configuring the ACL, apply the minimum authorization principle.
  - Configure the permitted IP address segment, and add only the necessary management IP address segment. IP addresses other than have been specified are not permitted to access the device through the management port.
- Packets accessing the management interface of the device are not controlled. When a device is attacked by packets, the system is busy and the services cannot be provided in the normal state.

  Preventive methods or measures: Run the **firewall packet-filter** command to apply the firewall packet filtering rule on the interface to filter packets received on the interface and prevent packet attacks.

Table 2-15 lists the default settings of system security.

Table 2-15 Default settings of system security

Parameter	Default Setting
Firewall blacklist	Disabled
Anti-DoS attack	Disabled
Anti-ICMP attack	Disabled
Anti-IP attack	Disabled
Source route filtering	Disabled
User-side ring network detection	Disabled

2.8.1 Configuring a Firewall

A firewall monitors and decides whether data flows are allowed to enter an access device by analyzing data packets. Firewalls protect internal networks against unauthorized or unauthenticated access and attacks from external networks.

Context

The MA5600T/MA5603T filters data packets using the following firewall techniques: firewall blacklist, combination of firewall blacklist and advanced access control list (ACL) rules, ACL-based packet filtering firewall, and permitted or denied IP address segment.

Table 2-16 Firewall techniques supported by the MA5600T/MA5603T

Technique	Function	Feature
Firewall blacklist	A firewall blacklist filters data packets by source IP address.	Matching source IP addresses against a blacklist is simple, and packets can be quickly filtered. However, because data packets are filtered by only one rule, this process lacks flexibility.
Firewall blacklist and advanced access control list (ACL) rules	The combination of a firewall blacklist and advanced ACL rules enables the system to further filter packets by advanced ACL rules.	Data packets are filtered based on a firewall blacklist and advanced ACL rules. The filter rules can be flexibly configured.
ACL-based packet filtering firewall	An ACL-based packet filtering firewall verifies data packets at the network layer and forwards or denies them according to the security policy.	Advantage: This technique supports more flexible configurations and better filtering capabilities than firewall blacklist. Disadvantages: ● The packet filtering performance deteriorates sharply as the ACL complexity increases. ● The system does not check the session status or analyze any data, and is vulnerable to IP spoofing attacks.
Permitted or denied IP address segment	The system supports settings the IP address segment of the firewall to allow access, deny access for specified protocol type to prevent users of illegal IP address segment to log in to the system.	-

Procedure

- Configure a firewall blacklist.

1. Manually add IP addresses to the firewall blacklist.

   Run the **firewall blacklist item** command to add source IP addresses to the blacklist. Data packets carrying the specified source IP addresses will be considered as untrustworthy.
2. Enable the firewall blacklist feature.

   Run the **firewall blacklist enable** command to enable the firewall blacklist feature.

- Configure a combination of a firewall blacklist and advanced ACL rules.
  1. Manually add IP addresses to the firewall blacklist.

     Run the **firewall blacklist item** command to add source IP addresses to the blacklist. Data packets carrying the specified source IP addresses will be considered as untrustworthy.
  2. Configure advanced ACL rules for filtering data packets that carry the source IP addresses specified in the blacklist.
     a. Run the **acl** command to create an ACL rule. Only advanced ACL rules can be applied with the firewall blacklist feature, so the ACL rule IDs range from 3000 to 3999.
     b. Run the rule(adv acl) command to create an advanced ACL rule.
     c. Run the **quit** command to return to the global config mode.
  3. Enable the firewall blacklist feature.

     Run the **firewall blacklist enable acl-number *acl-number*** command to enable the firewall blacklist feature and apply the ACL rules to the packets that carry the source IP addresses specified in the blacklist.
- Configure an ACL-based packet filtering firewall.
  1. Run the **acl** command to create an ACL rule. Either basic or advanced ACL rules can be applied with the packet filtering firewall, so the ACL rule IDs range from 2000 to 3999.
  2. Run the **rule** command and specify different parameters to create different ACL rules.
     - Run the **rule(basic acl)** command to create a basic ACL rule.
     - Run the **rule(adv acl)** command to create an advanced ACL rule.
  3. Run the **quit** command to return to the global config mode.
  4. To configure a firewall filtering rule for the METH port, run the **interface meth** command to enter the METH mode; to configure a firewall filtering rule for the VLAN interface, run the **interface vlanif** command to enter the VLAN interface mode.
  5. Run the **firewall packet-filter** command to apply firewall filtering rules to an interface.

     NOTE

     When you run the **firewall packet-filter** command to activate an ACL rule, the NE software determines the precedence of the sub-rules included in the ACL rule. The ACL sub-rule configured earlier has a higher precedence.
  6. Run the **firewall default** command to configure the rule for filtering data packets when they are not matched with any ACL rule.
  7. Run the **firewall enable** command to enable the firewall function. The firewall is disabled by default.

To filter data packets on a port based on ACL rules, the firewall function must be enabled.

- Configure permitted or denied address segments (protecting against unauthorized logins).

⚠ **CAUTION**

- To ensure device security, use the minimum authorization principle. Specifically, configure a permitted IP address segment and add only the necessary management IP addresses to it. Any attempts using other IP addresses to access the management interface of the device will be denied.
- It is recommended that the permitted IP address segment and the denied IP address segment do not overlap each other. Only the data packets whose IP addresses are in the permitted segment but not in the denied segment are allowed to access the device.

1. Run the **sysman ip-access** command to configure the IP address segment that is permitted to access the device through telnet, Secure Shell (SSH), or Simple Network Management Protocol (SNMP).
2. Run the **sysman ip-refuse** command to configure the IP address segment that is denied access to the device through telnet, SSH, or SNMP.
3. Run the **sysman firewall*protocol-type* enable** command to enable the firewall feature based on the telnet, SSH, or SNMP protocol. By default, the protocol-based firewall feature is disabled.

----End

Example

This example assumes the scenario in which the IP address 192.168.10.18 is added to the firewall blacklist, its aging time is set to 100 minutes, and an advanced ACL rule is created to allow data packets in the 10.10.10.0 IP address segment to pass. To perform the configuration, do as follows:

```
huawei(config)#firewall blacklist item 192.168.10.18 timeout 100
huawei(config)#acl 3000
huawei(config-acl-adv-3000)#rule permit ip source 10.10.10.0 0.0.0.255 destination
 10.10.10.20 0
huawei(config-acl-adv-3000)#quit
huawei(config)#firewall blacklist enable acl-number 3000
```

This example assumes the scenario in which the users in the 172.16.25.0 IP address segment are not allowed to access the maintenance Ethernet port on the device whose IP address is 172.16.25.28. To perform the configuration, do as follows:

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)#rule 5 deny icmp source 172.16.25.0 0.0.0.255 destin
ation 172.16.25.28 0
huawei(config-acl-adv-3001)#quit
huawei(config)#firewall enable
huawei(config)#interface meth 0
huawei(config-if-meth0)#firewall packet-filter 3001 inbound
 ACL applied successfully
```

This example assumes the scenario in which the Telnet protocol firewall is enabled to allow only users in the IP address segment of 10.10.5.1 to 10.10.5.254 to access the device through telnet. To perform the configuration, do as follows:

```
huawei(config)#sysman ip-access telnet 10.10.5.1 10.10.5.254
huawei(config)#sysman firewall telnet enable
```

This example assumes the scenario in which the SSH protocol firewall is enabled to allow only users in the IP address segment of 10.20.22.1 to 10.20.22.254 to access the device through SSH. To perform the configuration, do as follows:

```
huawei(config)#sysman ip-access ssh 10.20.22.1 10.20.22.254
huawei(config)#sysman firewall ssh enable
```

This example assumes the scenario in which the SNMP protocol firewall is enabled so that users in the IP address segment of 10.10.20.1 to 10.10.20.254 are not allowed to log in to the device from the network management system (NMS). To perform the configuration, do as follows:

```
huawei(config)#sysman ip-refuse snmp 10.10.20.1 10.10.20.254
huawei(config)#sysman firewall snmp enable
```

2.8.2 Configuring Anti-attack

This topic describes how to configure system security features to protect the system against attacks initiated by malicious users and enhance system security.

Context

The table below lists the countermeasures against attacks and configuration procedures. Choose an appropriate countermeasure depending on network conditions.

Table 2-17 System security schemes

Vulnerability	Security Scheme	Suggestion
Malicious users send a large number of protocol packets to attack the system. Under an attack, the system fails to process normal service requests from users.	Anti-denial of service (DoS) attack	Use this security scheme during deployment.

Vulnerability	Security Scheme	Suggestion
Malicious users send ICMP or IP packets whose destination IP address is the system IP address of the access device. As a result, the system resources of the access device are exhausted and the access device may be malfunctioning. For example: ● Malicious users send a large number of ping packets to request responses from the access device. As a result, the access device is overloaded. ● Malicious users may find system vulnerabilities by pinging or telneting the access device and then initiate attacks. **NOTE** In a broad sense, ICMP or IP attacks are DoS attacks.	● Anti-ICMP attack on the user side ● Anti-IP attack on the user side	Use this security scheme during deployment if the access device is a Layer 2 device.
Attackers may forge some IP addresses to attack networks by setting source route options. Under such an attack, the system fails to process normal service requests from users.	Source route filtering	Use this security scheme during deployment for PCs and terminals that support source route filtering.

Countermeasures and configuration procedures

System Security Feature	Configuration Method	Remarks
Anti-denial of service (DoS) attack	● Run the **security anti-dos enable** command to configure anti-DoS attack. ● Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs. ● Run the **security anti-dos control-packet rate** command to configure the rate threshold for sending protocol packets to the CPU.	**CAUTION** The packet processing policies for anti-DoS attacks take effect only when anti-DoS attack is enabled globally by running the **security anti-dos enable** command globally.
Anti-Internet Control Message Protocol (ICMP) attack on the user side	Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.	-
Anti-IP attack on the user side	Run the **security anti-ipattack enable** command to enable anti-IP attack.	
Source route filtering	Run the **security source-route enable** command to enable source route filtering. This function is mainly used to filter the packets that are carrying route information and destined for the Layer 3 network.	-

Example

This example assumes that the system drops protocol packets when suffering from a DoS attack. To enable anti-DoS attack globally, and anti-IP attack, do as follows:

```
huawei(config)#security anti-dos enable
huawei(config)#security anti-dos control-packet policy deny
huawei(config)#security anti-ipattack enable
```

2.8.3 Preventing the Access of Illegal Users

Only the users of the permitted IP address segment can access the device, and the users of the denied IP address segment cannot access the device. This prevents the users of illegal IP address segments from logging in to the system, safeguarding the system.

Context

- Each firewall can be configured with up to 10 address segments.
- When adding an address segment, ensure that the start address does not repeat an existing start address.
- To delete an address segment, you only need to enter the start address of the address segment.

CAUTION

- To ensure the device security, apply the minimum authorization principles. That is, configure the permitted IP address segment, and add only the necessary management IP address segment. IP addresses other than have been specified are not permitted to access the device through the management port.
- It is recommended that the permitted IP address segment and the denied IP address segment should not overlap, and only the user whose IP address is in the permitted address segment and is not in the denied address segment can access the device.

Procedure

- Configure the permitted/denied IP address segment for the access through Telnet.
  1. Run the **sysman ip-access telnet** command to configure the IP address segment that is permitted to access the device through Telnet.
  2. Run the **sysman ip-refuse telnet** command to configure the IP address segment that is forbidden to access the device through Telnet.
  3. Run the **sysman firewall telnet enable** command to enable the firewall function for the access through Telnet. By default, the firewall function of the system is disabled.
- Configure the permitted/denied IP address segment for the access through SSH.
  1. Run the **sysman ip-access ssh** command to configure the IP address segment that is permitted to access the device through SSH.
  2. Run the **sysman ip-refuse ssh** command to configure the IP address segment that is forbidden to access the device through SSH.
  3. Run the **sysman firewall ssh enable** command to enable the firewall function for the access through SSH. By default, the firewall function of the system is disabled.
- Configure the permitted/denied IP address segment for the access through SNMP (NMS).
  1. Run the **sysman ip-access snmp** command to configure the IP address segment that is permitted to access the device through SNMP.
  2. Run the **sysman ip-refuse snmp** command to configure the IP address segment that is forbidden to access the device through SNMP.
  3. Run the **sysman firewall snmp enable** command to enable the firewall function for the access through SNMP. By default, the firewall function of the system is disabled.

----End

Example

To enable the firewall function for the access through Telnet, and permit only the users of the IP address segment 10.10.5.1-10.10.5.254 to log in to the device through Telnet, do as follows:

```
huawei(config)#sysman ip-access telnet 10.10.5.1 10.10.5.254
huawei(config)#sysman firewall telnet enable
```

To enable the firewall function for the access through SSH, and permit only the users of the IP address segment 10.10.20.1-10.10.20.254 to log in to the device through SSH, do as follows:

```
huawei(config)#sysman ip-access ssh 10.10.20.1 10.10.20.254
huawei(config)#sysman firewall ssh enable
```

To enable the firewall function for the access through SNMP, and permit only the users of the IP address segment 10.10.20.1-10.10.20.254 to log in to the device through SNMP, do as follows:

```
huawei(config)#sysman ip-refuse snmp 10.10.20.1 10.10.20.254
huawei(config)#sysman firewall snmp enable
```

2.9 Configuring the ACL

This topic describes the type, rule, and configuration of the access control list (ACL) on the MA5600T/MA5603T.

Context

An access control list (ACL) is used to filter certain packets by a series of preset rules. In this manner, the objects that need to be filtered can be identified. After the specific objects are identified, the corresponding data packets are permitted to pass or prohibited from passing according to the preset policy. The ACL-based traffic filtering process is a prerequisite for configuring the quality of service (QoS) or user security.

Table 2-18 lists the ACL types.

Table 2-18 ACL types

Type	Value Range	Feature
Basic ACL	2000-2999	The rules of a standard ACL are only defined according to the Layer 3 source IP address for analyzing and processing data packets.
Advanced ACL	3000-3999	The rules of an advanced ACL are defined according to the source IP address, destination IP address, type of the protocol over IP, and features of the protocol (including Transmission Control Protocol (TCP) source port, TCP destination port, and Internet Control Message Protocol (ICMP) message type). Compared with the basic ACL, the advanced ACL contains more accurate, abundant, and flexible rules.
Link layer ACL	4000-4999	A link-layer ACL allows definition of rules according to the link-layer information such as the source MAC address, VLAN ID, link-layer protocol type, and destination MAC address, and the data is processed accordingly.

Type	Value Range	Feature
User-defined ACL	5000-5999	The rules of a user-defined ACL are defined according to any 32 bytes of the first 80 bytes in the Layer 2 data frame for analyzing and processing data packets.

- When an arrival traffic stream matches two or more ACL rules, the matching sequence is as follows:
  - The priority of a user-defined rule is higher than the priority of all non-user-defined rules even if the highest priority is configured for the non-user-defined rule. If the user-defined rule is used, the other rule may be invalid. Therefore, exercise caution when using this rule.
  - An ACL rule is valid only when it is within the period of *time-range-name*.
  - If the rules are all user-defined rules or non-user-defined rules, and are issued to the physical port, the rules are matched based on priorities in a descending order; this process stops once a rule is matched. Then:
    - If you specify the priority when configuring a rule, the configured priority prevails and the priority increases with the value. When the priority is not configured or the configured priorities are the same, comply with the following rules:
    - If the rules of an ACL are activated at the same time, the rule with a larger *rule-id* has a higher priority.
    - If the rules of an ACL are activated one by one, the rule activated later has a higher priority than the one activated earlier.
    - If the rules are issued to the port from different ACLs, the rule activated later has a higher priority than the one activated earlier.
    - When both the Layer 3 ACL (basic ACL and advanced ACL) and the Layer 2 ACL (link-layer ACL) are issued, all rules use the priority that is configured for the Layer 2 ACL rule.
    - When both the IPv6-based rule and the link-layer rule exist, the link-layer rule has higher priority even if a higher priority is configured for the IPv6-based rule.
  - Among the rules issued to the routing interface or firewall, the rule with smaller *rule-id* has a higher priority. It is irrelative to the activation sequence or the configured priority. The rules are used to match the packets based on **rule-id** in an ascending order. Once the rule with a smaller **rule-id** matches the packets, its subsequent rules are not used. That is, the rules with a larger **rule-id** are invalid.
- When you run the **packet-filter** command to use an ACL and specify the **to-cpu** packet, the rules are matched based on priorities in a descending order; this process stops once a rule is matched. The matching sequence is irrelative to whether the rule is a user-defined rule, whether the rule is an IPv6 rule, or the priority configured for the rule. Rules are matched based on only the following principles:
  - If the rules of an ACL are activated at the same time, the rule with a larger *rule-id* has a higher priority.
  - If the rules of an ACL are activated one by one, the rule activated later has a higher priority than the one activated earlier.

  - If the rules are issued to the port from different ACLs, the rule activated later has a higher priority than the one activated earlier.

Precautions

Because the ACL is flexible in use, Huawei provides the following suggestions on its configuration:

- It is recommended that you define a general rule, such as permit any or deny any, in each ACL, so that each packet has a matching traffic rule that determines to forward or filter the unspecified packet.
- The activated ACL rules share the hardware resources with the protocol modules (such as Dynamic Host Configuration Protocol (DHCP) module and Internet Protocol over ATM (IPoA) module). In this case, the hardware resources are limited and may be insufficient. To prevent the failure to enable other service functions due to insufficient hardware resources, it is recommended you enable the protocol module first and then activate ACL rules in the data configuration. If you fail to enable a protocol module, perform the following steps:
  1. Check whether ACL rules occupy too many resources.
  2. If ACL rules occupy too many resources, deactivate or delete the unimportant or temporarily unused ACL configurations, and then configure and enable the protocol module.

2.9.1 Configuration Differences Between IPv4 ACLs and IPv6 ACLs

This topic describes differences regarding to configuration between IPv4 ACLs and IPv6 ACLs. It is recommended that you know well about how to configure IPv4 ACLs and then configure IPv6 ACLs based on their differences.

Context

- The configuration differences between IPv4 ACLs and IPv6 ACLs are as follows:
  - IPv6 and IPv4 have different IP address formats and packet formats, so the **ipv6** parameter must be specified for configuring IPv6 basic ACLs and advanced ACLs. Use the **ipv6** parameter to choose between IPv4 ACLs and IPv6 ACLs.
  - IPv4 and IPv6 have the same link-layer packet encapsulation format, so configurations do not differentiate IPv6 link-layer ACLs and IPv4 link-layer ACLs.
  - Users define packets matching ACLs based on the packet type. IPv4 and IPv6 have the same packet command for user-defined ACLs, so configurations do not differentiate IPv6 user-defined ACLs and IPv4 user-defined ACLs. When user-defined ACLs are used for filtering packets, the protocol type of the packets must be the same as the protocol type of the ACL rules. If they are different, filtering may encounter errors.

2.9.2 Filtering Packets by a Basic ACL

This topic is applicable to the scenario where the device needs to classify traffic for packets according to the source IP address.

Context

- The number of a basic access control list (ACL) is in the range of 2000-2999.

- A basic ACL is only defined according to the Layer 3 source IP address for analyzing and processing data packets.

Procedure

Step 1 (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

Step 2 Create a basic ACL.

Run the **acl** command to create a basic ACL, and then enter the ACL mode. The number of a basic ACL can only be in the range of 2000-2999.

Step 3 Configure a basic ACL rule.

In the acl-basic mode, run the **rule** command to create a basic ACL rule. The parameters are as follows:

- *rule-id*: Indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: Indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: Indicates the keyword for discarding the data packets that meet related conditions.
- **time-range**: Indicates the keyword of the time range during which the ACL rule will be effective.

Step 4 Activate the ACL.

After an ACL is configured, only an ACL gets generated but it will not be functional. You need to run other commands to activate the ACL. Some common commands are as follows:

- Run the **packet-filter** command to activate an ACL.
- Run the **firewall packet-filter** command to activate an ACL. For details, see **Configuring the Firewall**.
- Perform the quality of service (QoS) operation. For details, see **Configuring Traffic Management Based on ACL Rules**.

----End

Example

To configure port 0/2/0 on the MA5600T/MA5603T to receive only the packets from 2.2.2.2 from 00:00 to 12:00 on Fridays, and to discard the packets from other addresses, do as follows:

```
huawei(config)#time-range time1 00:00 to 12:00 fri
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule permit source 2.2.2.2 0.0.0.0 time-range time1
huawei(config-acl-basic-2000)#rule deny time-range time1
huawei(config-acl-basic-2000)#quit
huawei(config)#packet-filter inbound ip-group 2000 port 0/2/0
huawei(config)#save
```

2.9.3 Filtering Packets by an Advanced ACL

This topic describes how to classify traffic for the data packets according to the source IP address, destination IP address, protocol type over IP, and features for protocol, such as Transmission Control Protocol (TCP) source port, TCP destination port, and Internet Control Message Protocol (ICMP) type of the data packets.

Context

The number of an advanced ACL is in the range of 3000-3999.

An advanced access control list (ACL) can classify traffic according to the following information:

- Protocol type
- Source IP address
- Destination IP address
- Source port ID (source port of the UDP or TCP packets)
- Destination port ID (destination port of the UDP or TCP packets)
- ICMP packet type
- Precedence value: priority field of the data packet
- Type of service (ToS) value: ToS field of the data packet
- Differentiated services code point (DSCP) value: DSCP of the data packet

Procedure

Step 1 (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

Step 2 Create an advanced ACL.

Run the **acl** command to create an advanced ACL, and then enter the acl-adv mode. The number of an advanced ACL can only be in the range of 3000-3999.

Step 3 Configure a rule of the advanced ACL.

In the acl-adv mode, run the **rule** command to create an ACL rule. The parameters are as follows:

- *rule-id*: Indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: Indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: Indicates the keyword for discarding the data packets that meet related conditions.
- **time-range**: Indicates the keyword of the time range during which the ACL rules are effective.

Step 4 Activate the ACL.

After an ACL is configured, only an ACL is generated and the ACL does not take effect. You need to run other commands to activate the ACL. Some common commands are as follows:

- Run the **packet-filter** command to activate an ACL.
- Run the **firewall packet-filter** command to activate an ACL. For details, see **2.8.1 Configuring a Firewall**.
- Perform the quality of service (QoS) operation. For details, see **2.10.2 Configuring Traffic Management Based on ACL Rules**.

----End

Example

Assume that the service board of the MA5600T/MA5603T resides in slot 1 and belongs to a VLAN, and the IP address of the VLAN Layer 3 interface is 10.10.10.101. To prohibit the ICMP (such as ping) and telnet operations from the user side to the VLAN interface on the device, do as follows:

```
huawei(config)#acl 3001
huawei(config-acl-basic-3001)rule 1 deny icmp destination 10.10.10.101 0
huawei(config-acl-basic-3001)rule 2 deny tcp destination 10.10.10.101 0
destination-port eq telnet
huawei(config-acl-basic-3001)quit
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/2/0
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/2/0
huawei(config)#save
```

2.9.4 Filtering Packets by a Link-layer ACL

This topic describes how to classify traffic according to the link layer information such as source MAC address, source VLAN ID, Layer 2 protocol type, and destination MAC address.

Context

A link layer ACL can classify traffic according to the following link layer information:

- Protocol type over Ethernet
- 802.1p priority
- VLAN ID
- Source MAC address
- Destination MAC address

Procedure

Step 1 (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

Step 2 Create a link layer ACL.

Run the **acl** command to create a link layer ACL, and then enter the acl-link mode. The number of a link layer ACL can only be in the range of 4000-4999.

Step 3 Configure a link layer ACL rule.

In the acl-link mode, run the **rule** command to create a link layer ACL rule. The parameters are as follows:

- *rule-id*: Indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: Indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: Indicates the keyword for discarding the data packets that meet related conditions.
- **time-range**: Indicates the keyword of the time range during which the ACL rule is effective.

Step 4 Activate the ACL.

After an ACL is configured, only an ACL is generated and the ACL does not take effect. You need to run other commands to activate the ACL. Some common commands are as follows:

- Run the **packet-filter** command to activate an ACL.
- Perform the quality of service (QoS) operation. For details, see **2.10.2 Configuring Traffic Management Based on ACL Rules**.

----End

Example

To create a link layer ACL rule that allows data packets with protocol type 0x8863 (pppoe-control message), VLAN ID 12, CoS 1, source MAC address 2222-2222-2222, and destination MAC address 00e0-fc11-4141 to pass, do as follows:

```
huawei(config)#acl 4001
huawei(config-acl-link-4001)rule 1 permit type 0x8863 cos 1 source 12
2222-2222-2222 0000-0000-0000 destination 00e0-fc11-4141 0000-0000-0000
huawei(config-acl-basic-4001)quit
huawei(config)#save
```

2.9.5 Filtering Packets by a User-defined ACL

This topic describes how to classify traffic according to any 32 bytes of the first 80 bytes of a Layer 2 data frame.

Prerequisites

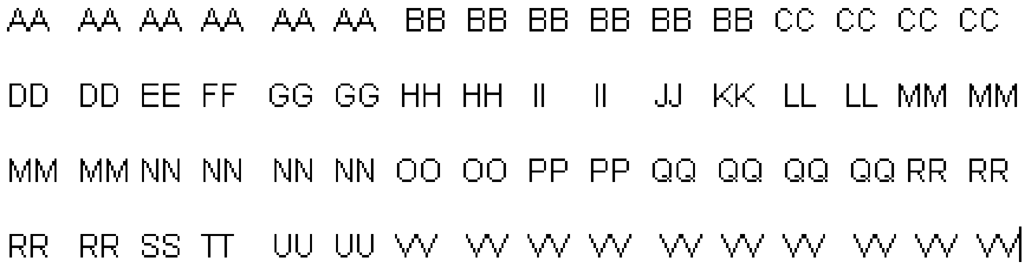
Configuring a user-defined access control list (ACL) requires a deep understanding of the Layer 2 data frame structure. Be sure to make a data plan according to the format of the Layer 2 data frame.

Context

The number of a user-defined ACL must be in the range of 5000-5999.

A user-defined ACL rule can be created according to any 32 bytes of the first 80 bytes of a Layer 2 data frame.

Figure 2-8 First 64 bytes of a data frame



```
AA AA AA AA AA AA BB BB BB BB BB BB CC CC CC CC
DD DD EE FF GG GG HH HH II II JJ KK LL LL MM MM
MM MM NN NN NN NN OO OO PP PP QQ QQ QQ QQ RR RR
RR RR SS TT UU UU VV VV VV VV VV VV VV VV VV VV
```

Table 2-19 lists the meaning of the letters and their offset values.

Table 2-19 Description of letters and their offset values

Letter	Description	Offset	Letter	Description	Offset
A	Destination MAC address	0	L	IP check sum	28
B	Source MAC address	6	M	Source IP address	30
C	VLAN tag	12	N	Destination IP address	34
D:	Protocol type	16	O	Transmission Control Protocol (TCP) source port	38
E	IP version number	18	P	TCP destination port	40
F	Type of service	19	Q	Serial number	42
G	Length of the IP packet	20	R	Acknowledgment field	46
H	ID	22	S	IP header length and reserved bit	50
I	Flags	24	T	Reserved bit and flags bit	51
J7	Time to live	26	U	Window size	52
K	Protocol ID ("6" represents TCP and "17" represents User Datagram Protocol (UDP))	27	V	Other	54

NOTE

The offset value of each field is the offset value in data frame ETH II+VLAN tag. In a user-defined ACL, you can use the two parameters of rule mask and offset to extract any bytes from the first 80 bytes of the data frame. After the comparison with the user-defined rule, the data frame matching the rule is filtered for related processing.

Procedure

Step 1 (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

Step 2 Create a user-defined ACL.

Run the **acl** command to create a user-defined ACL, and then enter the acl-user mode. The number of a user-defined ACL can only be in the range of 5000-5999.

Step 3 Configure the user-defined ACL rule.

In the acl-user mode, run the **rule** command to create an ACL rule. The parameters are as follows:

- *rule-id*: Indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: Indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: Indicates the keyword for discarding the data packets that meet related conditions.
- *rule-string*: Indicates the character string of the user-defined rule. The character string is in hexadecimal notation. The number of characters in the string must be an even number.
- *rule-mask*: Indicates the mask of the user-defined rule. It is a positive mask, used to perform the AND operation with the data packets for extracting the information of the data packets.
- *offset*: Indicates the offset. With the header of the packet as the reference point, it specifies the byte from which the AND operation begins. Together with the rule mask, it extracts a character string from the packets.
- **ipoe**: Indicates that the Ethernet packet header encapsulates an IP packet, including the IP packet without VLAN tag, IP packet with one VLAN tag, and IP packet with two VLAN tags.
- **non-ipoe**: Indicates that the Ethernet packet header encapsulates a non-IP packet, including the non-IP packet without VLAN tag, non-IP packet with one VLAN tag, non-IP packet with two VLAN tags, and non-IP packet with multiple VLAN tags.
- **time-range**: Indicates the keyword of the time range during which the ACL rule will be effective.

Step 4 Activate the ACL.

After an ACL is configured, only an ACL gets generated but it will not be functional. You need to run other commands to activate the ACL. Some common commands are as follows:

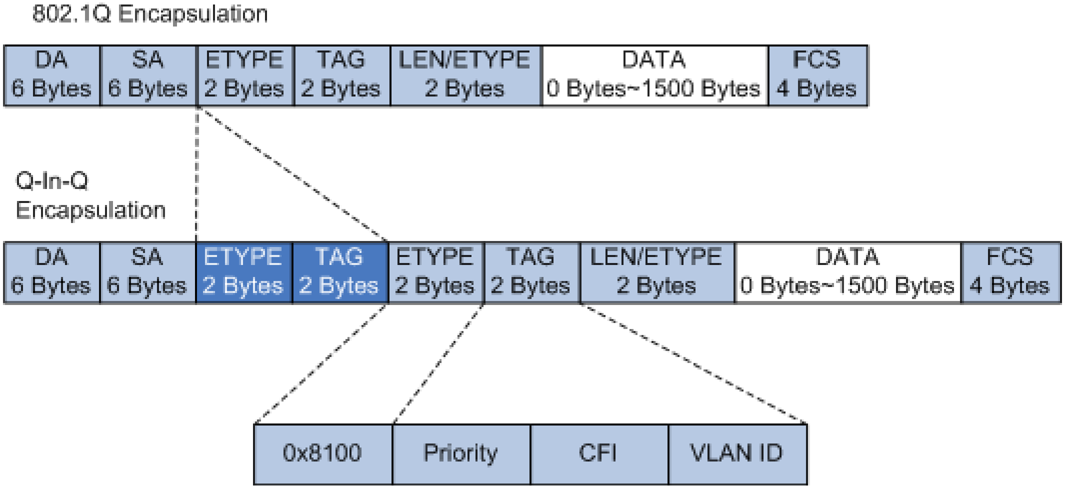
- Run the **packet-filter** command to activate an ACL.
- Perform the quality of service (QoS) operation. For details, see **2.10.2 Configuring Traffic Management Based on ACL Rules**.

----End

Example

Assume that the packet sent from port 0/2/0 to the MA5600T/MA5603T is the QinQ packet containing two VLAN tags. To change the CoS priority in the outer VLAN tag (VLAN ID: 10) to 5, do as follows:

Figure 2-9 QinQ packet format



```
huawei(config)#acl 5001
huawei(config-acl-user-5001)#rule 1 permit 8100 ffff 16
```

NOTE

The type value of a QinQ packet varies with different vendors. Huawei adopts the default 0x8100. As shown in **Figure 2-9**, the offset of this type value should be 16 bytes.

```
huawei(config-acl-user-5001)#rule 10 permit 0a ff 19
huawei(config-acl-user-5001)#quit
```

NOTE

"19" indicates the ADN operation after an offset of 19 bytes with the header of the packet as the base. "0a" refers to the value of the inner tag field of the QinQ packet. In this example, the second byte of the inner tag field is a part of the VLAN ID, which is exactly the value of the inner VLAN ID (VLAN 10).

```
huawei(config)#traffic-priority inbound user-group 5001 cos 5 port 0/2/0
```

2.10 Configuring QoS

This topic describes how to configure quality of service (QoS) on the MA5600T/MA5603T.

Context

Configuring QoS in the system can provide different quality guarantees for different services. QoS does not have a unified service model. Therefore, make the QoS plan for networkwide services before making the configuration solution.

On the MA5600T/MA5603T, the key points for implementing QoS are as follows:

- Traffic management

  Configuring traffic management can limit the traffic for a user service or user port.

- Queue scheduling

  For the service packets that are already configured with traffic management, through the configuration of queue scheduling, the service packets can be placed into queues with different priorities, implementing QoS inside the system.

In addition to the preceding key points, the MA5600T/MA5603T supports hierarchical quality of service (HQoS) and ACL-based traffic management.

- HQoS

  Two levels of traffic management is supported: for HQoS users and for the HQoS user group.

- ACL-based traffic management

  In the scenario where users have flexible requirements on implementing QoS for traffic streams, the ACL can be used to implement flexible traffic classification (see **2.9 Configuring the ACL**), and then QoS can be implemented for traffic streams.

2.10.1 Configuring Traffic Management

This topic describes how to configure traffic management on the MA5600T/MA5603T.

Overview

The MA5600T/MA5603T supports traffic management for the inbound and outbound traffic streams of the system. Traffic management can be implemented based on the following three granularities:

- Based on service port

  NOTE

  For details on configuring traffic classification, see **4.6 Creating an xDSL Service Port** or **6.6 Creating a GPON Service Port**.

- Based on port+CoS
- Based on port+VLAN

In addition, the MA5600T/MA5603T supports rate limit on the Ethernet port and traffic suppression on inbound broadcast packets and unknown (multicast or unicast) packets.

Configuring Traffic Management Based on Service Port

This topic describes how to configure traffic management based on service port. When configuring a service port, you need to bind an IP traffic profile to the service port and manage the traffic of the service port through the traffic parameters defined in the profile.

Context

Traffic management based on service port is implemented by creating an IP traffic profile and then binding the IP traffic profile when creating the service port.

- The system has seven default IP traffic profiles with the IDs of 0-6. You can run the **display traffic table** command to query the traffic parameters of the default traffic profiles.
- It is recommended that you use the default traffic profiles. A new IP traffic profile is created only when the default traffic profiles cannot meet the requirements.

Table 2-20 lists the traffic parameters defined in the IP traffic profiles.

Table 2-20 Traffic parameters defined in the IP traffic profiles

Item	Parameter Description
Parameters of two rate three color management	CIR: committed information rate. CBS: committed burst size, CBS=min(2000+CIR*32, 10240000). PIR: peak information rate, PIR=min(2*CIR, 10240000). PBS: peak burst size, PBS=min(2000+32*PIR, 10240000). **NOTE** ● CIR is mandatory, and the other three parameters are optional. If you configure only CIR, the system calculates the other three parameters based on the formula. Therefore, you are recommended to configure only CIR. ● The system marks the service packets with colors according to the CIR and PIR parameters. To be specific, for the packets whose rate is equal to or lower than CIR, the system marks them as green (allowed to pass). For the packets whose rate is higher than CIR and lower than PIR, the system marks them as yellow (allowed to pass). For the packets whose rate is higher than PIR, the system drops such packets. After the configuration is completed, green packets are allowed to pass, yellow packets that do not exceed the bandwidth can also pass, and yellow packets that exceed the bandwidth are dropped.
Priority policies	The priority policies are classified into the following three types: ● user-cos: Copy the 802.1p priority in the outer VLAN tag of the packet to the 802.1p priority in the VLAN tag of the outbound packet. ● user-inner-cos: Copy the 802.1p priority in the inner VLAN tag (CTag) of the packet to the 802.1p priority in the VLAN tag of the outbound packet. ● user-tos: Copy the ToS priority in the VLAN tag of the packet to the 802.1p priority in the VLAN tag of the outbound packet.
Scheduling policies	There are three types of scheduling policies: ● Tag-In-Package: The system performs scheduling according to the 802.1p priority of the packet. ● Local-Setting: It is the local priority. That is, the system performs scheduling according to the 802.1p priority specified in the traffic profile bound to the traffic stream. ● Tag-In-Ingress-Package: For the downstream packets, The system schedules the packet by the priority that the ingress packet.

NOTE

"Outbound" (upstream) in this document refers to the direction from the user side to the network side, and "inbound" (downstream) refers to the direction from the network side to the user side.

Procedure

Step 1 Run the **display traffic table** command to query whether there is a proper traffic profile in the system.

Check whether an existing traffic profile meets the planned traffic management parameters, priority policy, and scheduling policy to confirm the index of the traffic profile to be used. If a proper traffic profile does not exist in the system, create an IP traffic profile.

Step 2 Run the **traffic table ip** command to create a traffic profile.

The usage of this command is complicated. The following is a detailed description:

- The traffic management parameters must contain at least **CIR**, which must be assigned with a value.
- Keyword **priority** must be entered to set the outer 802.1p priority of the packet. Two options are available for setting the priority policy:
  - Enter a value in the range of 0-7 to specify a priority for the packet.
  - If the priority of the user-side packet is copied according to user-cos, user-inner-cos, or user-tos, you need to enter the default 802.1p priority of the packet (a value in the range of 0–7). If the user-side packet does not carry a priority, the specified default 802.1p priority of the packet is adopted as the priority of the outbound packet.
- (Optional) Enter keyword **inner-priority** to set the inner 802.1p priority (the 802.1p priority in the CTag) of the packet. Two options are available for setting the priority policy:
  - Enter a value in the range of 0-7 to specify a priority for the packet.
  - If the priority of the user-side packet is copied according to user-cos, user-inner-cos, or user-tos, you need to enter the default 802.1p priority of the packet (a value in the range of 0-7). If the user-side packet does not carry a priority, the specified default 802.1p priority of the packet is adopted as the priority of the outbound packet.
- Keyword **priority-policy** must be entered to specify a scheduling policy for the inbound packet. For details about the scheduling policies, see **Table 2-20**.

Step 3 Run the **service port** command to bind a proper traffic profile.

----End

Example

Assume that the CIR is 2048 kbit/s, 802.1p priority of the outbound packet is 6, and the scheduling policy of the inbound packet is Tag-In-Package. To add traffic profile 9 with these settings, do as follows:

```
huawei(config)#traffic table ip index 9 cir 2048 priority 6 priority-policy tag-In-
Package
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 9
  TD Name              : ip-traffic-table_9
  Priority             : 6
  Copy Priority        : -
  Mapping Index        : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : tag-pri
  CIR                  : 2048 kbps
  CBS                  : 67536 bytes
  PIR                  : 4096 kbps
  PBS                  : 133072 bytes
  Color policy         : dei
  Referenced Status    : not used
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#display traffic table ip index 9
```

```
  ------------------------------------------------
  TD Index            : 9
  TD Name             : ip-traffic-table_9
  Priority            : 6
  Copy Priority       : -
  Mapping Index       : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy     : tag-pri
  CIR                 : 2048 kbps
  CBS                 : 67536 bytes
  PIR                 : 4096 kbps
  PBS                 : 133072 bytes
  Color policy        : dei
  Referenced Status   : not used
  ------------------------------------------------
```

Configuring Traffic Management Based on Port+CoS

This topic describes how to configure traffic management based on port+CoS so that different IP traffic profiles can be specified for the traffic streams that have different 802.1p priorities on a port.

Prerequisites

A proper IP traffic profile must be created and the index of the IP traffic profile to be used must be confirmed. For the configuration method, see **Configuring Traffic Management Based on Service Port**.

Context

- Traffic management based on service ports conflicts with traffic management based on port +CoS. By default, the system supports traffic management based on service ports.
- If service ports are configured on the board, the traffic management mode of the board cannot be changed.

Procedure

Step 1 According to the type of the board to be configured, enter the ADSL, SHDSL, VDSL, or GPON mode.

Step 2 Run the **car-mode port-cos** command to configure the traffic management mode of the service board to traffic management based on port+CoS.

The configured traffic management mode is valid to all the ports on the board. The configured traffic management mode has the following two options:

- service-port: Indicates traffic management based on service port (default).
- port-cos: Indicates traffic management based on port+CoS.

Step 3 Run the **car-port** command to specify the 802.1p priority for the port, and bind an IP traffic profile to the traffic streams that meet the specified 802.1p priority.

When traffic management based on port+CoS is selected for a board, pay attention to the following points:

- For a non-xPON board, you can bind the corresponding traffic profile in the inbound/ outbound direction according to a CoS value of a port on the board.

- For a GPON board, you can bind the corresponding traffic profile in the inbound/outbound direction according to a CoS value of a GEM port on the board.

----End

Example

To configure GEM port 130 on port 0 of the GPON board in slot 0/2, and bind traffic profile 2 to the packets with priority 7, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#car-mode port-cos
huawei(config-if-gpon-0/2)#car-port 0 gemport 130 cos 0 inbound 2 outbound 2
huawei(config-if-gpon-0/2)#display car-mode
  The CAR mode of the board: port-cos
huawei(config-if-gpon-0/2)#display car-port 0 gemport
130
  ----------------------------------------------
  Port GEM port CoS Inbound-index Outbound-index
  ----------------------------------------------
     0      130   7             2              2
  ----------------------------------------------
```

To configure port 0 of theVDSL2 board in slot 0/2, and bind traffic profile 3 to the packets with priority 3, do as follows:

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#car-mode port-cos
huawei(config-if-vdsl-0/2)#car-port 0 cos 3 inbound 3 outbound 3
huawei(config-if-vdsl-0/2)#display car-mode
  The CAR mode of the board: port-cos
huawei(config-if-vdsl-0/2)#display car-port 0
  ----------------------------------------------
  Port  CoS Inbound-index Outbound-index
  ----------------------------------------------
   0     3             3               3
  ----------------------------------------------
```

Configuring Traffic Management Based on Port+VLAN

After configuring traffic management based on port+VLAN, you can specify different IP traffic profiles for different VLAN packets carried on the same port.

Prerequisites

- A proper IP traffic profile must be created and the index of the IP traffic profile to be used must be confirmed. For details about the configuration method, see **Configuring Traffic Management Based on Service Port**.
- The MA5600T/MA5603T must be configured with the SPUA board. Currently, only the SPUA board supports traffic management based on port+VLAN.

Procedure

Step 1 In the global config mode, run the **interface eth** command to enter the ETH mode.

Step 2 Run the **car-port portid vlan** command to configure traffic management based on port+VLAN.

This command can be used to configure IP traffic profiles for the packets in the specified VLAN range on the specified port, implementing inbound and outbound traffic management.

----End

Example

To configure port 0 on the SPUA board in slot 0/2, and use traffic profile 6 for controlling the packets with VLAN 10, do as follows:

```
huawei(config)#display traffic table ip index 6
  --------------------------------------------
  TD Index            : 6
  TD Name             : ip-traffic-table_6
  Priority            : 6
  Copy Priority       : user-cos
  Mapping Index       : 0
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : tag-pri
  CIR                 : off
  CBS                 : off
  PIR                 : off
  PBS                 : off
  Color policy        : dei
  Referenced Status    : used
  --------------------------------------------
huawei(config)#interface eth 0/2
huawei(config-if-eth-0/2)#car-port 0 vlan 10  inbound 6 outbound 6
```

Configuring User-based Rate Limitation

In the user-based rate limitation, the VoIP, IPTV service, and Internet access service of each user share a total user bandwidth. When there is no voice or IPTV service, the Internet access service can hold a burst of the total user bandwidth so that the total user bandwidth can be managed in a unified manner.

Context

When the user uses the Triple play service, the VoIP, IPTV service, and Internet access service of each user share a total user bandwidth. All services of the user hold the total user bandwidth, and the service with the highest CoS priority is ensured first. When other services carry no traffic, each service can hold a burst of the total user bandwidth. The multicast bandwidth is determined by the bandwidth of demanded programs. The total bandwidth of demanded programs cannot exceed the total user bandwidth.

Procedure

- For PON access users.
  - In the user-based rate limitation, multiple service ports of a user are added to a rate-limited group. Through the QoS strategy applied on the rate-limited group, the total user bandwidth is ensured on the basis that the committed information rate (CIR) and peak information rate (PIR) of each service are ensured, and each service is allowed to hold a burst of the total user bandwidth.
  - Only the GPBD service boards support user-based rate limitation.

  1. Run the **traffic table ip** command to create an IP traffic profile to configure the CoS priority of each service and ensure the CIR and PIR.
     - The CoS priorities of services are VoIP, IPTV service, and Internet access service in a descending order.
     - In the IP traffic profile used by the rate-limited group, the PIR must be equal to or larger than the sum of CIRs of all services in other IP traffic profiles.

2. Run the **service-port** command to create service ports of the VoIP, IPTV service, and Internet access service, using the IP traffic profile created in **Step 1**.
3. Run the **car-group** command to create the rate-limited group of service ports to manage the total user bandwidth of multiple services.
   - To ensure the user bandwidth, the PIR of the rate-limited group must be equal to or larger than the sum of CIRs of all services in the rate-limited group.
   - The PIR is equal to the total user bandwidth. In the case that any two services carry no traffic, the third service can hold a burst of the total user bandwidth.
4. Run the **car-group add-member service-port** command to add service ports to the rate-limited group.

   Pay attention to the following points when adding service ports to the rate-limited group:

   - Only service ports of the same PON port can be added to the same rate-limited group.
   - For Type C and Type D, only service ports of the same ONT can be added to the same rate-limited group.
   - One service port cannot be added to multiple rate-limited groups.
   - A maximum of eight service ports can be added to a rate-limited group.

- For ADSL2+ and VDSL access users.

  Each port corresponds to a user. By limiting the upstream/downstream rate of the port, set the maximum upstream/downstream rate to the total user bandwidth. All services of the user hold the total user bandwidth, and the service with the highest CoS priority is ensured first. When other services carry no traffic, each service can hold a burst of the total user bandwidth.

  1. Set the maximum upstream/downstream rate to the total user bandwidth.
     - For the ADSL2+ access mode:
       a. Run the **adsl line-profile quickadd** command to quickly add an ADSL2+ line profile, or run the interactive **adsl line-profile add** command to add an ADSL2+ line profile.
       b. Run the **adsl channel-profile quickadd** command to quickly add an ADSL2 + channel profile, or run the interactive **adsl channel-profile add** command to add an ADSL2+ channel profile. In the channel profile, configure the maximum upstream and downstream rates to limit the user bandwidth.
       c. Run the **adsl line-template quickadd** command to quickly add an ADSL+ line template, or run the interactive **adsl line-template add** command to add an ADSL2+ line template.
     - For the VDSL (common mode) access mode:
       a. Run the **vdsl line-profile quickadd** command to quickly add a VDSL line profile, or run the interactive **vdsl line-profile add** command to add a VDSL line profile.
       b. Run the **vdsl channel-profile quickadd** command to quickly add a VDSL channel profile, or run the interactive **vdsl channel-profile add** command to add a VDSL channel profile. In the channel profile, configure the maximum upstream and downstream rates to limit the user bandwidth.

    c. Run the **vdsl line-template quickadd** command to quickly add a VDSL2 line template, or run the interactive **vdsl line-template add** command to add a VDSL2 line template.

  - For the VDSL (TI mode) access mode:

    a. Run the **vdsl service-profile quickadd** command to quickly add a VDSL2 service profile, or run the interactive **vdsl service-profile add** command to add a VDSL2 service profile.

    b. Run the **vdsl spectrum-profile quickadd** command to quickly add a VDSL2 spectrum profile, or run the interactive **vdsl spectrum-profile add** command to add a VDSL2 spectrum profile.

2. Run the **traffic table ip** command to create an IP traffic profile to configure the CoS priority of each service and ensure the CIR and PIR. The PIR is equal to the total user bandwidth. When other services carry no traffic, each service can hold a burst of the total user bandwidth.

   The CoS priorities of services are VoIP, IPTV service, and Internet access service in a descending order.

3. Run the **service-port** command to create service ports of the services, using the IP traffic profile created in **Step 2**.

4. Run the **queue-scheduler strict-priority** command to configure queue scheduling mode of the port to strict priority queue scheduling.

----End

Example

Assume that under GPON port 0/2/1, the user with the ONT 1 is provided with the VoIP, IPTV, and Internet access services. Set the total user bandwidth to 10 Mbit/s, add rate-limited group 0, add service ports 100, 101, and 102 of the user to rate-limited group 0, and use traffic profile 30 to control traffic of rate-limited group 0. In the case that any two services carry no traffic, the third service can hold a burst of the total user bandwidth. To perform such a configuration with the following parameters, do as follows:

- Service port 100 of the Internet access service uses traffic profile 10, with the CIR 2 Mbit/s and the 802.1p priority 4.
- Service port 101 of the VoIP service uses traffic profile 11, with the CIR 1 Mbit/s and the 802.1p priority 6.
- Service port 102 of the IPTV service uses traffic profile 12, with the packet rate not limited and the 802.1p priority 5.

```
huawei(config)#traffic table ip index 10 cir 2048 pir 10240 priority 4 priority-
policy local-Setting
huawei(config)#service-port 100 vlan 2 gpon 0/2/1 ont 1 gemport 4 multi-service
user-vlan 20 rx-cttr 10 tx-cttr 10
huawei(config)#traffic table ip index 11 cir 1024 pir 10240 priority 6 priority-
policy local-Setting
huawei(config)#service-port 101 vlan 2 gpon 0/2/1 ont 1 gemport 5 multi-service
user-vlan 30 rx-cttr 11 tx-cttr 11
huawei(config)#traffic table ip index 12 cir off priority 5 priority-policy local-
Setting
huawei(config)#service-port 102 vlan 2 gpon 0/2/1 ont 1 gemport 6 multi-service
user-vlan 40 rx-cttr 12 tx-cttr 12
huawei(config)#traffic table ip index 30 cir 10240 pir 10240 priority 3 priority-
policy local-Setting
huawei(config)#car-group 0 inbound traffic-table index 30 outbound traffic-table
index
```

```
huawei(config)#car-group 0 add-member service-port 100-102
huawei(config)#display car-group 0

Command:
          display car-group 0
 ----------------------------------------------------------------------------
                                                           Inbound   Outbound
 GroupID                                      Member List    Index     Index
 ----------------------------------------------------------------------------
       0                                     100,101,102        10         10
 ----------------------------------------------------------------------------
Total: 1
```

Assume that under ADSL port 0/3/1, a user is provided with the VoIP, IPTV, and Internet access services. Set the total user bandwidth to 10 Mbit/s. In the case that any two services carry no traffic, the third service can hold a burst of the total user bandwidth. To perform such a configuration with the following parameters, do as follows:

- Service port 100 of the Internet access service uses traffic profile 10, with the CIR 2 Mbit/s and the 802.1p priority 4.
- Service port 101 of the VoIP service uses traffic profile 11, with the CIR 1 Mbit/s and the 802.1p priority 6.
- Service port 100 of the IPTV service uses traffic profile 12, with the packet rate not limited and the 802.1p priority 5.

```
huawei(config)#adsl line-profile quickadd 10
huawei(config)#adsl channel-profile quickadd 10 rate 32 32 10240 32 32 6000
huawei(config)#adsl line-template quickadd 10 channel1 10 10 60 channel2 10
huawei(config)#interface adsl 0/3
huawei(config-if-adsl-0/3)#deactivate 1
huawei(config-if-adsl-0/3)#activate 1 template-index 10
huawei(config-if-adsl-0/3)#quit
huawei(config)#traffic table ip index 10 cir 2048 pir 10240 priority 4 priority-
policy local-Setting
huawei(config)#service-port 100 vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service user-
vlan 20 rx-cttr 10 tx-cttr 10
huawei(config)#traffic table ip index 11 cir 1024 pir 10240 priority 6 priority-
policy local-Setting
huawei(config)#service-port 101 vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service user-
vlan 30 rx-cttr 11 tx-cttr 11
huawei(config)#traffic table ip index 12 cir off priority 5 priority-policy local-
Setting
huawei(config)#service-port 102 vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service user-
vlan 40 rx-cttr 12 tx-cttr 12
huawei(config)#queue-scheduler strict-priority
```

Configuring Rate Limitation on an Ethernet Port

This topic describes how to configure rate limitation on a specified Ethernet port.

Prerequisites

The Ethernet board must be configured in the system.

Context

- Rate limitation on an Ethernet port is valid only to the Ethernet board.
- Traffic streams exceeding the specified rate are discarded.

Procedure

Step 1 In the global config mode, run the **line-rate** command to configure rate limitation on a specified Ethernet port.

The main parameters are as follows:

- target-rate: Indicates the limited rate of the port, in the unit of kbit/s.
- port: Indicates the subrack ID/slot ID/port ID.

Step 2 You can run the **display qos-info line-rate port** command to query the configured rate limitation on the specified Ethernet port

----End

Example

To limit the rate of Ethernet port 0/19/0 to 6400 kbit/s, do as follows:

```
huawei(config)#line-rate 6400 port 0/19/0
huawei(config)#display qos-info line-rate port 0/19/0
line-rate:
port 0/19/0:
   Line rate: 6400 Kbps
```

Configuring Queue-based Rate Limit

With queue-based rate limit, traffic rates of a specified queue or queue group can be limited using the shaping function, packets can be buffered when the traffic exceeds the limit, and the buffered packets can be sent at an appropriate time (for example, periodic check). In this manner, lost packets are reduced, meeting requirements of packet transmission. Usually, the shaping function is used to reshape and stabilize traffic at ports.

Prerequisites

- Only ADK, ADP, ADQ, H80BCAME, VDT, VDJ, VDPM, and VDNF boards support shaping of queue groups.
- H805GPBD, H801GPFD, H801XGBCboards support shaping of a single queue.

Procedure

Step 1 In global configuration mode, run the **queue-shaping** command to configure queue-based rate limit.

Parameters to be set are as follows:

- queue: indicates shaping of a queue group. The queue group has fixed queues, queue 3 and queue 4. The PQ scheduling is used between queue 3 and queue 4 and the traffic shaping parameters are CIR and CBS that are configured in the traffic profile. Shaping of the queue group is secondary queue scheduling. That is, queue 3 and queue 4 are regarded as a whole which is scheduled based on the scheduling mode set by using the **queue-scheduler** command. The PQ scheduling is used between queue 3 and queue 4.
- queue-list: indicates shaping of a specified queue. The traffic shaping parameters are PIR and PBS configured in the traffic profile.

Step 2 Run the **display queue-shaping** command to query shaping of queues.

----End

Example

Example: Run the following commands to configure shaping of queues 3 and 4 at port 0/2/0 and use traffic profile 5 to rate limit packets in the upstream direction. (Queue 3 and 4 carry packets for high-speed Internet access services.)

```
huawei(config)#queue-shaping 0/2/0 queue 3 4 outbound 5
huawei#display queue-shaping  0/2/0
{ <cr>|ont<K> }:

  Command:
            display queue-shaping  0/2/0
  ----------------------------------------------------------------------------
  F/ S/ P    QUEUE-ID1     QUEUE-ID2     OUTBOUND-INDEX        CIR
CBS
  ----------------------------------------------------------------------------
  0/ 2/ 0          3             4                 5       6400       12800
  ----------------------------------------------------------------------------
```

Configuring GPON Rate Limitation

This topic describes how to configure rate limitation for GPON services, thereby providing differentiated quality of service (QoS) for various GPON services.

Context

- There are multiple methods of rate-limiting GPON services, for example, rate-limiting downstream traffic by using an IP traffic profile and ACL rules, rate-limiting the ONT upstream bandwidth by using a DBA profile, and rate-limiting the GEM port and GEM port traffic on an ONT.
- Rate limitation on GPON services can be performed on the OLT and the ONT concurrently. If more than one rate limitation modes are configured in the system, the minimum rate prevails.
- Which method of rate-limiting the ONT upstream bandwidth is used depends on the ONT capability. Specifically, if an ONT supports various rate limitation methods and the ONT upstream traffic is small (for example, FTTH service), a DBA profile is a best choice to rate-limit the ONT upstream traffic. If a T-CONT carries upstream traffic for multiple users (for example, FTTB/FTTC service), rate limitation on GEM port is generally used to prevent a user from occupying bandwidth for a long time. If the priority of user packets is trustable (for example, an enterprise user), priority queue (PQ) scheduling is generally used.

Procedure

- Perform rate limitation on the OLT.
  - Rate limitation using an IP traffic profile includes two modes. For details, see **Configuring Traffic Management Based on Service Port**, and **Configuring Traffic Management Based on Port+CoS**.
  - Performing rate limitation by configuring an ACL rule can control the traffic matching the ACL rule. For details, see **Controlling the Traffic Matching an ACL Rule**.
- Perform rate limitation on the ONT.

NOTE

- In the case of an MxU device, rate limitation can be performed on downstream traffic of a service port or a port by configuring an IP traffic profile. For details, see MxU manuals.
- In the case of H805GPBD board, you can run the **traffic-limit ont** command to limit the traffic of downstream packets on a specified ONT. The system limits the traffic of downstream packets on an ONT by using the shaping function and buffers the packets that exceed the limit (that is the PIR parameter in traffic profile) and transmits them at a proper time (such as during periodic checks). This reduces packet drop and at the same time complies with traffic features.

1. Run the **dba-profile add** command to add a DBA profile. The DBA profile is used to schedule the ONT upstream bandwidth properly, achieving the best bandwidth utilization.

   A DBA profile supports five types (Type1 to Type5). Generally, Services with a higher priority adopts Type1 or Type2 DBA profiles and services with a lower priority adopts Type3 or Type4 DBA profiles. Table 2-21 shows the features of the DBA profile of each type.

   Table 2-21 The features of the DBA profile

Profile Type	Features
Type1	Indicates the fixed bandwidth. After the DBA profile of Type1 is bound, the system assigns a specified bandwidth, regardless of whether there is upstream traffic.
Type2	Indicates the assured bandwidth. After the DBA profile of Type2 is bound, the system meets the bandwidth requirements if the upstream traffic does not exceed a specified value. When there is no upstream traffic, the system does not assign any bandwidth.
Type3	Indicates the hybrid of assured bandwidth and non-assured bandwidth. The DBA profile of Type3 specifies an assured value and non-assured value. After assigning the fixed bandwidth and assured bandwidth, the system assigns the remaining bandwidth (if any) to the user bound with the DBA profile of Type3 (the assigned bandwidth does not exceed the non-assured bandwidth).
Type4	Indicates the best-effort bandwidth. The DBA profile of Type4 just specifies a maximum value. After the DBA profile of Type4 is bound, its priority for obtaining the bandwidth is the lowest. That is, after assigning the fixed bandwidth, assured bandwidth, and non-assured bandwidth, the system assigns the remaining bandwidth (if any) to the user bound with the DBA profile of Type4 (the assigned bandwidth does not exceed the maximum value).
Type5	Indicates the hybrid bandwidth. The preceding four types of values need to be specified.

2. Run the **ont-lineprofile gpon** command to add a GPON ONT line profile, and then enter the GPON ONT line profile mode.
3. Run the **tcont** command to bind a T-CONT to the DBA profile.

It is recommended that one service type use one T-CONT and different T-CONTs be planned with different bandwidth assurance types.

4. Run the **qos-mode** command to configure a QoS mode of the GPON ONT line profile to ensure that the QoS mode is the same as that of the GEM port.

   By default, the QoS mode of the GPON ONT line profile (that is, the ONT scheduling mode) is priority queue (PQ). The QoS mode includes:

   - gem-car: Indicates the rate limitation mode based on the GEM port of the T-CONT. Rate limitation is performed on a specified GEM port in the ONT upstream direction. To select the gem-car mode, set **gem add** to **gem-car**. The maximum traffic is determined by the DBA profile bound to the GEM port. If a T-CONT contains multiple GEM ports, the scheduling mechanism of packets between multiple GEM ports depends on the default scheduling mechanism of the ONT.
   - flow-car: Indicates the rate limitation mode based on traffic streams of a GEM port. Rate limitation is performed on a specified traffic stream in the ONT upstream direction. To select the flow-car mode, set **gem mapping** to **flow-car**. The maximum traffic is determined by the DBA profile bound to the traffic stream. Flow-car is more specific than gem-car. After rate limitation based on traffic streams is performed, traffic is scheduled in the T-CONT queue. The scheduling mechanism depends on the default scheduling mechanism of the ONT. Before configuring flow-car, make sure that the required traffic profile is created by running the **traffic table ip** command.

     NOTE

     The traffic stream in this topic refers to the service channel between an ONT and OLT. It is different the service port created by running the **service-port** command.
   - priority-queue: Indicates the PQ mode based on the GEM port of the T-CONT. Traffic is scheduled based on PQ between multiple GEM ports in the ONT upstream direction. To select priority-queue mode, set **gem add** to **priority-queue**. By default, the system supports eight (0–7) queues. Queue 7 has the highest priority and services of queue 7 are preferentially guaranteed. The maximum traffic is determined by the DBA profile to which the T-CONT is bound.

5. Run the **commit** command to make the profile configuration take effect. The configuration of the line profile takes effect only after you run this command.

----End

Example

Assume that:

- A user under ONT 1 connected to GPON port0/2/1 requires 2 Mbit/s high-speed Internet access service.
- The priority of user packets is trustable. The PQ scheduling mechanism is used, with priority 1.
- The default IP traffic profile, namely IP traffic profile 5 is used for rate limitation on a GPON port, with CIR of 2048 kbit/s.
- DBA profile 10 of Type4 is used and the maximum bandwidth in the ONT upstream direction is 100 Mbit/s.

To perform the preceding configurations, do as follows:

```
huawei(config)#dba-profile add profile-id 10 type4 max 102400
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 10
huawei(config-gpon-lineprofile-5)#qos-mode Priority-queue
huawei(config-gpon-lineprofile-5)#gem add 1 eth tcont 1 priority-queue 1
huawei(config-gpon-lineprofile-5)#mapping-mode vlan
huawei(config-gpon-lineprofile-5)#gem mapping 1 2 vlan 10
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 5
huawei(config-if-gpon-0/2)#quit
huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 1 rx-cttr 5 tx-
cttr 5
```

Configuring Traffic Suppression

This topic describes how to configure traffic suppression. The purpose of traffic suppression is to ensure normal provisioning of services for system users by suppressing the broadcast, unknown multicast, and unknown unicast packets received by the system.

Context

Traffic suppression includes setting various rate limits or forwarding policies for broadcast, unknown multicast, and unknown unicast packets. The **traffic-suppress** command takes effect on the control board. The **vlan packet-policy** or **packet-policy** command takes effect on service boards.

Table 2-22 describes the methods for configuring traffic suppression on broadcast, unknown multicast, and unknown unicast packets.

Table 2-22 Methods for configuring traffic suppression

Packet Type	Taking Effect on Control Boards		Taking Effect on Service Boards	
Broadcast packet	Granularity	System-level and port-level	Granularity	Virtual local area network (VLAN)-level and port-level

Packet Type	**Taking Effect on Control Boards**		**Taking Effect on Service Boards**	
	Configuration method	● In general interface unit (GIU) or super control unit (SCU) mode, run the **traffic-suppress** { *portid* | **all** } **broadcast** command. ● In global config mode, run the **traffic-suppress** { *frameid/ slotid* | **all** } **broadcast** command. **NOTE** Only ETH boards support configuration of the traffic suppression level in global config mode.	Configuration method	● In global config mode, run the **vlan packet-policy broadcast** command. ● In VLAN service profile mode, run the **packet-policy broadcast** command. ● In ETH mode, run the **traffic-suppress** { *portid* | **all** } **broadcast** command.
Unknown multicast packets	Granularity	System-level and port-level	Granularity	VLAN-level, port-level, and BTV-level

Packet Type	Taking Effect on Control Boards		Taking Effect on Service Boards	
	Configuration method	● In GIU or SCU mode, run the **traffic-suppress** { *portid* | **all** } **multicast** command. ● In global config mode, run the **traffic-suppress** { *frameid/ slotid* | **all** } **multicast** command. **NOTE** Only ETH boards support configuration of the traffic suppression level in global config mode.	Configuration method	● In global config mode, run the **vlan packet-policy multicast** command. ● In VLAN service profile mode, run the **packet-policy multicast** command. ● In ETH mode, run the **traffic-suppress** { *portid* | **all** } **multicast** command. ● Run the **multicast-unknown policy** command to configure the traffic stream-based forwarding policy for unknown multicast packets. **NOTE** Only when both the VLAN-based and traffic stream-based forwarding policies for unknown multicast packets are forwarding, unknown multicast packets are forwarded. Otherwise, they are discarded.
Unknown unicast packets	Granularity	System-level and port-level	Granularity	VLAN-level and port-level

Packet Type	Taking Effect on Control Boards		Taking Effect on Service Boards	
	Configuration method	● In GIU or SCU mode, run the **traffic-suppress** { *portid* | **all** } **unicast** command. ● In global config mode, run the **traffic-suppress** { *frameid/ slotid* | **all** } **unicast** command. NOTE Only ETH boards support configuration of the traffic suppression level in global config mode.	Configuration method	● In global config mode, run the **vlan packet-policy unicast** command. ● In VLAN service profile mode, run the **packet-policy unicast** command. ● In ETH mode, run the **traffic-suppress** { *portid* | **all** } **unicast** command.

NOTE

Procedure

- Configure traffic suppression on broadcast, unknown multicast, and unknown unicast packets. After successful configuration, traffic suppression takes effect on control boards.
  1. Run the **display traffic-suppress** command to query the threshold of traffic suppression.
  2. Run the **traffic-suppress** command to configure board-based or port-based traffic suppression.

     The parameters are as follows:

     - *broadcast*: Suppresses the broadcast traffic.
     - *multicast*: Suppresses the unknown multicast traffic.
     - *unicast*: Suppresses the unknown unicast traffic.
     - *value*: Indicates the index of the traffic suppression level. The index value is the value queried in **Step 1**.

NOTE

- Only ETH boards support configuration of the traffic suppression level in global config mode.
- The traffic-suppress command takes effect on the control boards only in ETH mode and takes effect on service boards in other modes.

- Configure the forwarding policy for broadcast, unknown multicast, and unknown unicast packets. After successful configuration, the forwarding policy takes effect on service boards.
  1. Run the **vlan service-profile** command to create a VLAN service profile.
  2. In VLAN service profile mode, run the **packet-policy** command to configure the forwarding policy for broadcast, unknown multicast, and unknown unicast packets.

     The parameters are as follows:
     - *broadcast*: Sets the forwarding policy for broadcast packets.
     - *multicast*: Sets the forwarding policy for unknown multicast packets
     - *unicast*: Sets the forwarding policy for unknown unicast packets.
     - *forward*: The MA5600T/MA5603T forwards the received packets.
     - *discard*: Discards the received packets by the MA5600T/MA5603T.
  3. In VLAN service profile mode, run the **commit** command to submit parameters in the VLAN service profile.

     NOTE

     After configuration is complete, run the **commit** command to make the configuration take effect.
  4. Run the **vlan bind service-profile** command to bind the VLAN service profile to a VLAN.

     NOTE

     - In global config mode, run the **vlan packet-policy** command to configure the VLAN-based forwarding policy for broadcast, unknown multicast, and unknown unicast packets. If a VLAN is bound to a VLAN service profile, the forwarding policy in VLAN service profile mode takes effect. Otherwise, the forwarding policy in global config mode takes effect.
     - Run the **multicast-unknown policy** command to configure the traffic stream-based forwarding policy for unknown multicast packets. Only when both the VLAN-based and traffic stream-based forwarding policies for unknown multicast packets are forwarding, unknown multicast packets are forwarded. Otherwise, they are dropped.

----End

Example

To configure traffic suppression on broadcast packets according to traffic suppression level 8 for port 0 on the SCU board in slot 0/9, run the following commands:

```
huawei(config)#interface scu 0/9
huawei(config-if-scu-0/9)#display traffic-suppress all

 Command:
          display traffic-suppress all
  Traffic suppression ID definition:
  --------------------------------------------------------------------
   NO.  Min bandwidth(kbps)  Max bandwidth(kbps)  Package number(pps)
  --------------------------------------------------------------------
     1                   6                  145                   12
     2                  12                  291                   24
     3                  24                  582                   48
     4                  48                 1153                   95
     5                     97                  2319                   191
     6                    195                  4639                   382
     7                    390                  9265                   763
     8                    781                 18531                  1526
     9                   1562                 37063                  3052
    10                   3125                 74126                  6104
    11                   6249                148241                 12207
    12                  12499                296483                 24414
    13                      0                     0                     0
  ---------------------------------------------------------------------
  ---------------------------------------------------------------------
   PortID     Broadcast_index     Multicast_index     Unicast_index
  ---------------------------------------------------------------------
        0                   7                   7               OFF
        1                   7                   7               OFF
        2                   7                   7               OFF
        3                   7                   7               OFF
  ---------------------------------------------------------------------
huawei(config-if-scu-0/9)#traffic-suppress all broadcast value 8
huawei(config-if-scu-0/9)#display traffic-suppress 0
 Traffic suppression ID definition:
  ---------------------------------------------------------------------
   NO.  Min bandwidth(kbps)  Max bandwidth(kbps)  Package number(pps)
  ---------------------------------------------------------------------
     1                      6                   145                    12
     2                     12                   291                    24
     3                     24                   582                    48
     4                     48                  1153                    95
     5                     97                  2319                   191
     6                    195                  4639                   382
     7                    390                  9265                   763
     8                    781                 18531                  1526
     9                   1562                 37063                  3052
    10                   3125                 74126                  6104
    11                   6249                148241                 12207
    12                  12499                296483                 24414
    13                      0                     0                     0
  ---------------------------------------------------------------------
  ----------------------------------------------------------------
  Current traffic suppression index of broadcast       :  7
  Current traffic suppression index of multicast       :  7
  Current traffic suppression index of unknown unicast :  7
  ----------------------------------------------------------------
```

To prevent downstream broadcast packets from occupying network resources and configure the forwarding policy for broadcast packets to **discard** in VLAN service profile 2 to which VLAN 10 is bound, run the following commands:

```
huawei(config)#vlan service-profile
{ profile-id<K>|profile-name<K> }:profile-id
{ profile-id<U><1,256> }:2
{ <cr>|profile-name<K> }:

  Command:
          vlan service-profile profile-id 2

huawei(config-vlan-srvprof-2)#packet-policy
{ broadcast<K>|multicast<K>|unicast<K> }:broadcast
{ discard<K>|forward<K> }:discard

  Command:
          packet-policy broadcast discard
  Info: Please use the commit command to make modifications take effect

huawei(config-vlan-srvprof-2)#commit
huawei(config)#vlan bind service-profile
{ vlan-list<S><Length 1-256> }:10
{ profile-id<K>|profile-name<K> }:profile-id
{ profile-id<U><1,256> }:2
```

```
Command:
        vlan bind service-profile 10 profile-id 2
```

2.10.2 Configuring Traffic Management Based on ACL Rules

The ACL can be used to implement flexible traffic classification according to user requirements. After traffic classification based on ACL rules is completed, you can perform QoS for the traffic streams.

Controlling the Traffic Matching an ACL Rule

This topic describes how to control the traffic matching an ACL rule on a specified port, and process the traffic that exceeds the limit, such as adding the DSCP tag or dropping the packet directly.

Prerequisite

The ACL and the rule of the ACL are configured, and the port for traffic limit is working in the normal state.

Context

- The traffic statistics are only effective for the permit rules of an ACL.
- The limited traffic must be an integer multiple of 64 kbit/s.

Procedure

Step 1 Run the **traffic-limit** command to control the traffic matching an ACL rule on a specified port.

Use the **target-rate** parameter to set the fixed maximum rate of the port, or use CAR parameters to set a rate for trTCM-based ports. The two rates cannot be set at a time. Run this command to set the action to be taken when the traffic received on the port exceeds the limited value. Two options are available:

- **drop**: Drop the traffic that exceeds the limited value.
- **remark-dscp** *value*: To set the DSCP priority for the traffic that exceeds the limited value, use this parameter.

Step 2 Run the **display qos-info traffic-limit port** command to query the traffic limit information on the specified port.

----End

Example

To limit the traffic that matches ACL 2001 received on port 0/2/0 to 512 kbit/s, and add the DSCP priority tag (af1) to packets that exceed the limit, do as follows:

```
huawei(config)#traffic-limit inbound ip-group 2001 512 exceed remark-dscp af1 port
0/2/0
//"af1" represents a dscp type: Assured Forwarding 1 service (10).
huawei(config)#display qos-info traffic-limit port 0/2/0
traffic-limit:
port 0/2/0:
 Inbound:
   Matches: Acl 2001 rule 5     running
```

```
          Target rate: 512 Kbps
          Exceed action: remark-dscp af1
```

Adding a Priority Tag to the Traffic Matching an ACL Rule

This topic describes how to add a priority tag to the traffic matching an ACL rule on a specified port so that the traffic can obtain the service that matches the specified priority. The priority tag type can be ToS, DSCP, or 802.1p.

Prerequisite

The ACL and the rule of the ACL are configured, and the port for traffic limit is working in the normal state.

Context

- The traffic statistics are only valid to permit rules of an ACL.
- The ToS and the DSCP priorities are mutually exclusive. Therefore, they cannot be configured at the same time.

Procedure

Step 1 Run the **traffic-priority** command to add a priority tag to the traffic matching an ACL rule on a specified port.

Step 2 Run the **display qos-info traffic-priority port** command to query the configured priority.

----End

Example

To add a priority tag to the traffic that matches ACL 2001 received on port 0/2/1, and the DSCP priority and local priority of the traffic are 10 (af1) and 0 respectively, do as follows:

```
huawei(config)#traffic-priority inbound ip-group 2001 dscp af1 local-precedence 0
port 0/2/1
huawei(config)#display qos-info traffic-priority port 0/2/1

traffic-priority:
port 0/2/1:
 Inbound:
   Matches: Acl 2001 rule 5 running
     Priority action: dscp af1 local-precedence 0
```

Enabling the Statistics Collection of the Traffic Matching an ACL Rule

This topic describes how to enable the statistics collection of the traffic matching an ACL rule, analyzing and monitoring the traffic.

Prerequisite

The ACL and the rule of the ACL are configured, and the port for traffic statistics is working in the normal state.

Context

The traffic statistics are only valid to permit rules of an ACL.

Procedure

Step 1 Run the **traffic-statistic** command to enable the statistics collection of the traffic matching an ACL rule on a specified port.

Step 2 Run the **display qos-info traffic-mirror port** command to query the statistics information about the traffic matching an ACL rule on a specified port.

----End

Example

To enable the statistics collection of the traffic that matches ACL 2001 received on port 0/19/0, do as follows:

```
huawei(config)#traffic-statistic inbound ip-group 2001 port 0/19/0
huawei(config)#display qos-info traffic-statistic port 0/19/0

traffic-statistic:
port 0/19/0:
 Inbound:
   Matches: Acl 2001 rule 5     running
     0 packet
```

Enabling the Mirroring of the Traffic Matching an ACL Rule

This topic describes how to mirror the traffic matching an ACL rule on a port to a specified port. Mirroring does not affect packet receipt and transmission on the mirroring source port. You can monitor the traffic of the mirroring source port by analyzing the traffic that passes the mirroring destination port.

Prerequisite

The ACL and the rule of the ACL are configured, and the port for traffic mirroring is working in the normal state.

Context

- The traffic statistics are only valid to permit rules of an ACL.
- The destination mirroring port cannot be an aggregation port.
- The system supports only one mirroring destination port and the mirroring destination port must be the upstream port.

Procedure

Step 1 Run the **traffic-mirror** command to enable the mirroring of the traffic matching an ACL rule on a specified port.

Step 2 Run the **display qos-info traffic-mirror port** command to query the mirroring information about the traffic matching an ACL rule on a specified port.

----End

Example

To mirror the traffic that matches ACL 2001 received on port 0/2/1 to port 0/19/0, do as follows:

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/2/1 to port 0/19/0
huawei(config)#display qos-info traffic-mirror port 0/2/1

traffic-mirror:
port 0/2/1:
 Inbound:
   Matches: Acl 2001 rule 5     running
   Mirror to: port 0/19/0
```

Enabling the Redirection of the Traffic Matching an ACL Rule

This topic describes how to redirect the traffic matching an ACL rule on a specified port. After this operation is executed successfully, the original port does not forward the traffic matching the ACL rule, but the specified port forwards the traffic.

Prerequisites

The ACL and the rule of the ACL are configured, and the port for redirection is working in the normal state.

Context

- The traffic statistics are only valid to permit rules of an ACL.
- Currently, the service ports support only redirection of the traffic matching the ACL rule to upstream ports. The upstream ports support only redirection of the traffic matching the ACL rule to ports on the board of the same type.

Procedure

Step 1 Run the **traffic-redirect** command to redirect the traffic matching an ACL rule on a specified port.

Step 2 Run the **display qos-info traffic-redirect port** command to query the redirection information about the traffic matching an ACL rule on a specified port.

----End

Example

To redirect the traffic that matches ACL 2001 received on port 0/19/0 to port 0/19/1, do as follows:

```
huawei(config)#traffic-redirect inbound ip-group 2001 port 0/19/0 to port 0/19/1
huawei(config)#display qos-info traffic-redirect port 0/19/0
traffic-redirect:
port 0/19/0:
 Inbound:
   Matches: Acl 2001 rule 5     running
     Redirected to: port 0/19/1
```

2.10.3 Configuring Early Drop

This topic describes how to configure early drop, which is applicable to the dropping policy settings for the packets in the queue.

Context

Early drop means that the system drops the packets that wait to enter the queue when congestion occurs. This process occurs after traffic management. The MA5600T/MA5603T supports early drop based on the following criteria:

- Color

  The system drops the yellow packets when congestion occurs.

- Priority

  The system supports the global configuration of the early drop threshold for each CoS priority, differentiating the services with different priorities in the same queue.

Configuring Priority-based Early Drop

The MA5600T/MA5603T can differentiate the services with different priorities in the same queue. The packet priority serves as a criterion for dropping packets.

Procedure

- Configure the early drop mode.

  In the global config mode, run the **early-drop mode pri-base** command to configure the priority-based early drop. After the configuration is completed, the system performs early drop according to the outer 802.1p priorities of the packets. When congestion occurs in a queue, the packets are dropped according to the early drop thresholds of the priorities.

- (Optional) Configure the early drop threshold.

  1. Configure the early drop threshold.

     Run the **early-drop** command to configure the mapping between service priorities and drop thresholds. After configuration is successful, if the packets of the specified service priority reach the threshold of the queue (the percentage of the queue depth), subsequent packets of the same service priority will be dropped instead of entering the queue.

  2. Query the configured early drop threshold.

     You can run the **display early-drop** command to query the configured early drop threshold.

----End

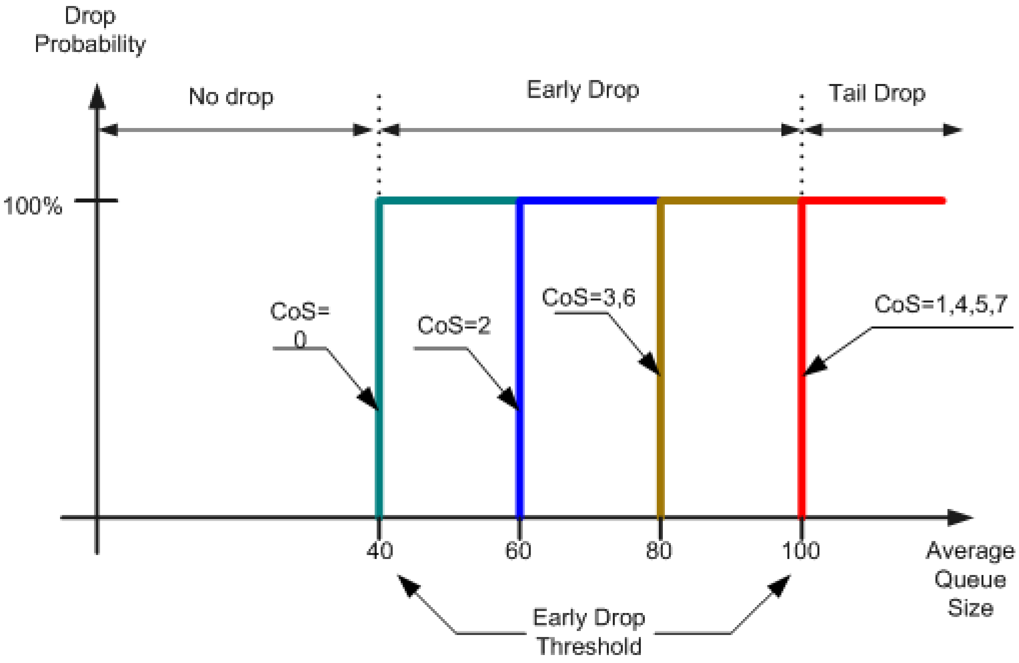
Example

To set the early drop threshold of the packet with CoS value 0 to 40, CoS value 2 to 60, and CoS values 3 and 4 to 80, do as follows:

```
huawei(config)#early-drop mode pri-base
huawei(config)#early-drop cos0 40 cos2 60 cos3 80 cos6 80
{<cr>|cos1<k>|cos4<k>|cos5<k>|cos7<k>}:
Command:
          early-drop cos0 40 cos2 60 cos3 80 cos6 80
huawei(config)#display early-drop
  ------------------------
  Priority       Threshold
  ------------------------
         0              40
         1             100
         2              60
         3              80
         4             100
```

```
          5              100
          6               80
          7              100
  ------------------------
```

The following figure shows the implementation of the early drop as configured.



Configuring Color-based Early Drop

According to the parameters in the IP traffic profile, the MA5600T/MA5603T can implement early drop based on the color of packets. When congestion occurs, the yellow packets are dropped.

Prerequisites

Only the SCUN board, SPUA board, OPGD board and the xPON board support Color-based early drop.

Procedure

- Configure the early drop mode.

  In the global config mode, run the **early-drop mode color-base** command to configure the color-based early drop.

  According to the *CIR* and *PIR* parameters in the IP traffic profile, the system marks packets with colors. The packets within the *CIR* bandwidth are marked as green, and the packets between the *CIR* and *PIR* bandwidth are marked as yellow.

  After the configuration is completed, green packets are allowed to pass, yellow packets with high priority are allowed to pass.

----End

2.10.4 Configuring the Queue Scheduling

A queue is a unit based on which packets are scheduled in a physical port. After the queue scheduling is configured, the packet of the priority service can be processed in time when network congestion occurs.

Configuring the Queue Scheduling Mode

This topic describes how to configure the queue scheduling mode for ensuring that packets in the queue with a higher priority can be processed in time in case of congestion.

Context

The MA5600T/MA5603T supports three queue scheduling modes: priority queuing (PQ), weighted round robin (WRR), and PQ+WRR.

- PQ

  The PQ gives preference to packets in a queue with a higher priority. When a queue with a higher priority is empty, the packets in a queue with a lower priority can be transmitted.

  By default, the PQ mode is used.

- WRR

  The system supports WRR for eight queues. Each queue has a weight value (w7, w6, w5, w4, w3, w2, w1, and w0 in descending order) for resource acquisition. In the WRR mode, queues are scheduled in turn to ensure that each queue can be scheduled.

  Table 2-23 lists the mapping between the configured weight and the actual weight of queues.

Table 2-23 Mapping between the configured weight and the actual weight of queues

Queue No.	Configured Weight	Actual Weight (for Port Supporting Eight Queues)	Actual Weight (for Port Supporting Four Queues)
7	W7	W7	-
6	W6	W6	-
5	W5	W5	-
4	W4	W4	-
3	W3	W3	W7+W6
2	W2	W2	W5+W4
1	W1	W1	W3+W2
0	W0	W0	W1+W0

Wn: Indicates the weight of queue n. The weight sum of all queues must be 0 or 100 (excluding the queue with weight 255). Here, 0 indicates that the PQ mode is used and 255 indicates that the queue is not used.

- PQ+WRR
  - The system supports PQ for some queues and WRR for the other queues. When the specified WRR value is 0, the queue is scheduled by PQ.
  - The queue scheduled by PQ should be a queue that has a higher priority.
  - The weight sum of queues scheduled by WRR must be equal to 100.

Procedure

Step 1 Run the **queue-scheduler** command to configure the queue scheduling mode.

Step 2 Run the **display queue-scheduler** command to query the configuration of the queue scheduling mode.

----End

Example

To configure WRR scheduling, with the weight values of the eight queues as 10, 10, 20, 20, 10, 10, 10, and 10 respectively, do as follows:

```
huawei(config)#queue-scheduler wrr 10 10 20 20 10 10 10 10
huawei(config)#display queue-scheduler
  Queue scheduler mode: WRR
  ---------------------------------
  Queue  Scheduler Mode  WRR Weight
  ---------------------------------
      0  WRR                     10
      1  WRR                     10
      2  WRR                     20
      3  WRR                     20
      4  WRR                     10
      5  WRR                     10
      6  WRR                     10
      7  WRR                     10
  ---------------------------------
```

To configure PQ+WRR scheduling, with the weight values of the six queues as 20, 20, 10, 30, 10, and 10 respectively, do as follows:

```
huawei(config)#queue-scheduler wrr 20 20 10 30 10 10 0 0
huawei(config)#display queue-scheduler
  Queue scheduler mode: WRR
  ---------------------------------
  Queue  Scheduler Mode  WRR Weight
  ---------------------------------
      0  WRR                     20
      1  WRR                     20
      2  WRR                     10
      3  WRR                     30
      4  WRR                     10
      5  WRR                     10
      6  PQ                      --
      7  PQ                      --
  ---------------------------------
```

Configuring the Mapping Between the Queue and the 802.1p Priority

This topic describes how to configure the mapping between the queue and the 802.1p priority so that packets with different 802.1p priorities are mapped to the specified queues based on the configured mapping. This enhances the flexibility of mapping packets to queues.

Context

- The configuration is valid to all the service boards in the system.
- By default, the mapping between the queue and the 802.1p priority is as listed in **Table 2-24**.

Table 2-24 Mapping between the queue and the 802.1p priority

Queue Number	Actual Queue Number (Port Supporting Eight Queues)
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

Procedure

Step 1 Run the **cos-queue-map** command to configure the mapping between the 802.1p priority and the queue.

Step 2 Run the **display cos-queue-map** command to query the mapping between the 802.1p priority and the queue.

----End

Example

To map 802.1p priority 0 to queue 0, 802.1p priority 1 to queue 2, and the other 802.1p priorities to queue 6, do as follows:

```
huawei(config)#cos-queue-map cos0 0 cos1 2 cos2 6 cos3 6 cos4 6 cos5 6 cos6 6
cos7
6
huawei(config)#display cos-queue-map
  CoS and queue map:
  ------------------------
  CoS             Queue ID
  ------------------------
    0                    0
    1                    2
    2                    6
    3                    6
    4                    6
    5                    6
    6                    6
    7                    6
  ------------------------
```

Configuring the Queue Depth

This topic describes how to configure the queue depth (the queue buffer space) to re-allocate buffer space to the queues, therefore to improve the flexibility of QoS.

Context

The queue depth determines the capability of a queue for processing burst packets. The greater the queue depth, the larger the buffer space, and the more capable is the queue in processing burst packets.

The queue depth of the port is allocated on a percentage basis. **Table 2-25** lists the default queue depths of the system.

Table 2-25 Queue depth allocation

Queue Number	Queue Depth (Port Supporting Eight Queues)
7	L7 (default: 6)
6	L6 (default: 25)
5	L5 (default: 12)
4	L4 (default: 12)
3	L3 (default: 13)
2	L2 (default: 13)
1	L1 (default: 6)
0	L0 (default: 13)

Ln: Indicates the depth of queue n. The sum of all the queue depths must be equal to 100.

Procedure

Step 1 Run the **queue-buffer** command to configure the queue depth of the service board.

Step 2 Run the **display queue-buffer** command to query the queue depth of the current service board.

----End

Example

To set the queue depths to 20, 20, 10, 10, 10, 10, 10, and 10, do as follows:

```
huawei(config)#queue-buffer 20 20 10 10 10 10 10 10
huawei(config)#display queue-buffer
```

```
------------------------
Queue   Depth size ratio
------------------------
    0              20
    1              20
    2              10
    3              10
    4              10
    5              10
    6              10
    7              10
------------------------
```

2.10.5 Configuring HQoS

The hierarchical QoS (HQoS) is a QoS technology that controls user traffic on a port with finer granularity and also schedules services of a user based on the service priority. This topic describes the configuration of HQoS.

Configuring HQoS Based on CAR Group

This topic describes how to configure HQoS based on CAR group for ensuring the bandwidth of each service of a user and the total bandwidth of the user.

Procedure

Step 1 Configure CAR for user traffic streams.

In the global config mode, run the **service-port** command to specify a traffic profile for rate limitation of HQoS users.

Step 2 Configure CAR for an HQoS user.

1. Create a CAR group for a service port.

   In the global config mode, run the **car-group** command to create a CAR group for a service port and bind a traffic profile to the CAR group.

2. Add a service port to the CAR group.

   In the global config mode, run the **car-group add-member service-port** command to add a service port to the CAR group. Bandwidth of service ports in this CAR group is limited by the traffic profile bound to the CAR group.

Step 3 (Optional) Configure CAR for an HQoS user group.

In the ETH mode, run the **car-port*portid* vlan** command to specify a traffic profile for rate limitation of an HQoS user group.

NOTE

An HQoS user group can be considered as a collection of users whose port IDs and VLAN IDs are within the port+VLAN range specified by this command.

- **inbound** *ip-traffic-table-index*: Sets the index of the traffic profile for packets transmitted from the outside of a device to the inside of the device.
- **outbound** *ip-traffic-table-index*: Sets the index of the traffic profile for packets transmitted from the inside of a device to the outside of the device.

----End

Example

Assume that the maximum bandwidth of a user is 5 Mbit/s. To configure 2 Mbit/s Internet access service, non-rate-limited voice service, and 4 Mbit/s multicast service for the user, do as follows:

```
huawei(config)#traffic table ip index 8 cir 2048 priority 1 priority-policy tag-In-
Package
huawei(config)#traffic table ip index 9 cir off priority 6 priority-policy tag-In-
Package
huawei(config)#traffic table ip index 10 cir 4096 priority 4 priority-policy tag-In-
Package
huawei(config)#traffic table ip index 20 cir 5120 priority 6 priority-policy tag-In-
Package
huawei(config)#service-port 1 vlan 100 gpon 0/1/1 ont 1 gemport 1 multi-service
user-vlan 10 rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 200 gpon 0/1/1 ont 1 gemport 2 multi-service
user-vlan 20 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 3 vlan 300 gpon 0/1/1 ont 1 gemport 3 multi-service
user-vlan 30 rx-cttr 10 tx-cttr 10
huawei(config)#car-group 1 inbound traffic-table index 20 outbound traffic-table
index 20
huawei(config)#car-group 1 add-member service-port 1-3
```

Configuring Priority-based HQoS

This topic describes how to configure the priority-based HQoS for ensuring different CIRs and PIRs for data with different priorities in the private line services (that is, data with a higher priority preferentially occupies the bandwidth).

Procedure

Step 1 Configure the CAR threshold for the CoS priority.

In the global config mode, run the **car-threshold** command to enable the priority-based CAR function and configure the CAR threshold for the CoS priority.

Step 2 Configure CAR for an HQoS user.

In the global config mode, run the **service-port** command to specify a traffic profile for rate limitation of HQoS users.

Step 3 (Optional) Configure CAR for an HQoS user group.

In the ETH mode, run the **car-port portid vlan vlanid** command to specify a traffic profile for rate limitation of an HQoS group.

NOTE

An HQoS user group can be considered as a collection of users on a specified port within a specified VLAN range.

- **inbound** *ip-traffic-table-index*: Sets the index of the traffic profile for packets transmitted from the outside of a device to the inside of the device.
- **outbound** *ip-traffic-table-index*: Sets the index of the traffic profile for packets transmitted from the inside of a device to the outside of the device.

----End

Example

Assume the following settings: A user has assured 2 Mbit/s bandwidth, the upstream port of the device has 10 Mbit/s bandwidth (without burst bandwidth) in the upstream direction and assured

20 Mbit/s bandwidth (with burst bandwidth of 30 Mbit/s) in the downstream direction, the CAR threshold for the user data with priority 3 is 25%, and the CAR threshold for the user data with priority 4 is 50%. After the setting, data with a higher priority preferentially occupies the CIR bandwidth. To implement these settings, do as follows:

```
huawei(config)#car-threshold cos3 25 cos4 50
huawei(config)#traffic table ip index 8 cir 2048 priority user-cos priority-policy
tag-In-Package
huawei(config)#traffic table ip index 9 cir 10240 priority user-cos priority-policy
tag-In-Package
huawei(config)#traffic table ip index 10 cir 20480 pir 30720 priority user-cos
priority-policy tag-In-Package
huawei(config)#service-port 1 vlan 100 eth 0/2/0 multi-service user-vlan 20 rx-cttr
8 tx-cttr 8
huawei(config)#interface eth 0/2
huawei(config-if-eth-0/2)#car-port 0 vlan 100 inbound 10 outbound 9
```

2.11 Configuring AAA

This topic describes how to configure the AAA on the MA5600T/MA5603T, including configuring the MA5600T/MA5603T as the local and remote AAA servers.

Context

AAA refers to authentication, authorization, and accounting. In the process that a user accesses network resources, through AAA, certain rights are authorized to the user if the user passes authentication, and the original data about the user accessing network resources is recorded.

- Authentication: Checks whether a user is allowed to access network resources.
- Authorization: Determines what network resources a user can access.
- Accounting: Records the original data about the user accessing network resources.

Application Context

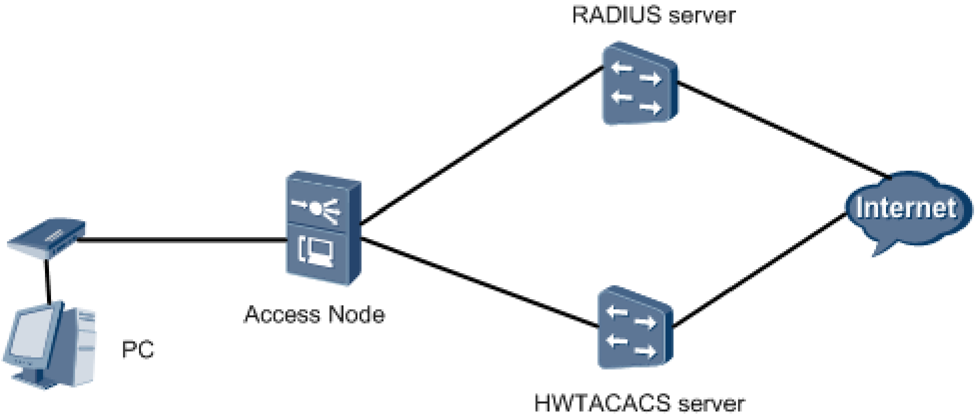
AAA is generally applied to the users that access the Internet in the PPPoA, PPPoE, 802.1x, VLAN, WLAN, ISDN, or Admin Telnet (associating the user name and the password with the domain name) mode.

NOTE

In the existing network, 802.1x and Admin Telnet correspond to the local AAA, that is, the MA5600T/MA5603T functions as a local AAA server; PPPoE corresponds to the remote AAA, that is, the MA5600T/MA5603T functions as the client of a remote AAA server.

Figure 2-10 shows an example network of the AAA application.

Figure 2-10 Example network of the AAA application



The preceding figure shows that the AAA function can be implemented on the MA5600T/MA5603T in the following three ways:

- The MA5600T/MA5603T functions as a local AAA server. In this case, the local AAA needs to be configured. The local AAA does not support accounting.
- The MA5600T/MA5603T functions as the client of a remote AAA server, and is connected to the HWTACACS server through the HWTACACS protocol, implementing the AAA.
- The MA5600T/MA5603T functions as the client of a remote AAA server, and is connected to the RADIUS server through the RADIUS protocol, implementing the AAA. The RADIUS protocol, however, does not support authorization.

Table 2-26 lists the differences between HWTACACS and RADIUS.

Table 2-26 Differences between HWTACACS and RADIUS

HWTACACS	RADIUS
Uses TCP to ensure more reliable network transmission.	Uses UDP for transmission.
Encrypts the body of HWTACACS packets, except their header.	Encrypts only the password field of the authenticated packets.
Separated authorization and authentication.	Concurrent processing of authentication and authorization.
Applicable to security control.	Applicable to accounting.
Supports authorization of the configuration commands on the router.	Does not support the authorization of the configuration commands on the router.

2.11.1 Configuring the Local AAA

This topic describes how to configure the local AAA so that the user authentication can be performed locally.

Context

- The local AAA configuration is simple, which does not depend on the external server.
- The local AAA supports only authentication.

Procedure

Step 1 Configure the AAA authentication scheme.

NOTE

- The authentication scheme specifies how all the users in an Internet service provider (ISP) domain are authenticated. The system supports up to 16 authentication schemes.
- The system has a default authentication scheme named **default**. It can be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode local** command to configure the authentication mode of the authentication scheme.
4. Run the **quit** command to return to the AAA mode.

Step 2 Create a domain.

NOTE

- A domain is a group of users of the same type.
- In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. In the AAA mode, run the **domain** command to create a domain.

Step 3 Refer the authentication scheme.

NOTE

You can refer an authentication scheme in a domain only after the authentication scheme is created.

1. In the domain mode, run the **authentication-scheme** command to reference the authentication scheme.
2. Run the **quit** command to return to the AAA mode.

Step 4 Configure a local user.

In the AAA mode, run the **local-user password** command to create a local AAA user.

----End

Example

User1 in the isp domain adopts the local server for authentication. The authentication scheme is newscheme, the password is a123456, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
  Info: Create a new authentication scheme
huawei(config-aaa-authen-newscheme)#authentication-mode local
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#domain isp
```

```
  Info: Create a new domain
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#quit
huawei(config-aaa)#local-user user1 password a123456
```

2.11.2 Configuring the Remote AAA (RADIUS Protocol)

The MA5600T/MA5603T is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

Context

- What is RADIUS:
  - Radius is short for the remote authentication dial-in user service. It is a distributed information interaction protocol with the client-server structure. Generally, it is used to manage a large number of distributed dial-in users.
  - Radius implements the user accounting by managing a simple user database.
  - The authentication and accounting requests of users can be passed on to the Radius server through a network access server (NAS).
- Principle of RADIUS:
  - When a user tries to access another network (or some network resources) by setting up a connection to the NAS through a network, the NAS forwards the user authentication and accounting information to the RADIUS server. The RADIUS protocol specifies the means of transmitting the user information and accounting information between the NAS and the RADIUS server.
  - The RADIUS server receives the connection requests of users sent from the NAS, authenticates the user account and password contained in the user data, and returns the required data to the NAS.
- Specification:
  - For the MA5600T/MA5603T, the RADIUS is configured based on each RADIUS server group.
  - In actual networking, a RADIUS server group can be any of the following:
    - An independent RADIUS server
    - A pair of primary/secondary RADIUS servers with the same configuration but different IP addresses
  - The following lists the attributes of a RADIUS server template:
    - IP addresses of primary and secondary servers
    - Shared key
    - RADIUS server type
- The configuration of the RADIUS protocol defines only the essential parameters for the information exchange between the MA5600T/MA5603T and the RADIUS server. To make the essential parameters take effect, the RADIUS server group should be referenced in a certain domain.
- The RADIUS attribute list defines the attribute parameters for interaction between the MA5600T/MA5603T and the RADIUS server. **Table 2-27** describes the parameters.

Table 2-27 RADIUS attribute list

Parameter Code	Parameter Name	Description
1	User-Name	Indicates the user name for authentication.
2	Password	Indicates the user password for authentication. This parameter is valid only for PAP authentication.
3	Challenge-Password	Indicates the user password for authentication. This parameter is valid only for CHAP authentication.
4	NAS-IP-Address	Indicates the IP address of the access device. If the RADIUS server group is bound to an interface address, use the bound interface address; otherwise, use the address of the interface where packets are sent.
5	NAS-Port	Indicates the user access port. The format of this parameter is four-digit slot ID + two-digit card number + five-digit port number + 21-digit VLAN ID.
6	Service-Type	Indicates the user service type. The value of this parameter is 2 (frame) for access users and is 6 for remote management users. Currently, the MA5600T/ MA5603T supports only 802.1x access users but not PPP, L2TP, or DHCP access users for RADIUS authentication.
7	Framed-Protocol	The value of this parameter is fixed to 1 (PPP) because ITU-T RFC 2856 does not define 802.1x for this parameter.
14	Login-IP-Host	Indicates the host IP address of a login user.
15	Login-Service	Indicates the login service type. The valid types are SSH, Rlogin, TCP Clear, PortMaster (proprietary), and LAT.

Parameter Code	Parameter Name	Description
24	State	If the access challenge packet that the RADIUS server sends to a device contains this parameter, the subsequent access request packet sent by the device to the RADIUS server must also contain this parameter of the same value as that is contained in the access challenge packet.
25	Class	If the access accept packet sent by the RADIUS server to a device contains this parameter, the subsequent charging request packet sent by the device to the RADIUS server must also contain this parameter of the same value. For a standard RADIUS server, a device can use the Class attribute to represent the CAR parameter.
27	Session-Timeout	Indicates the available remaining time in the unit of second. It is the user re-authentication time in the EAP challenge packet.
29	Termination-Action	Indicates the service termination mode. The valid modes are re-authentication and forcing users to go offline.
31	Calling-Station-Id	Allows the NAS to send the calling number.
32	NAS-Identifier	Indicates the host name of the device.
40	Acct-Status-Type	Indicates the charging packet type. ● 1: charging start packet ● 2: charging stop packet ● 3: real-time charging packet
41	Acct-Delay-Time	Indicates the time for generating a charging packet in the unit of second.

Parameter Code	Parameter Name	Description
42	Acct-Input-Octets	Indicates the number of upstream bytes in the unit of byte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
43	Acct-Output-Octets	Indicates the number of downstream bytes in the unit of byte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
44	Acct-Session-Id	Indicates the charging connection number. The connection numbers for the charging start packet, real-time charging packet, and charging stop packet of the same connection must be the same.
45	Acct-Authentic	Indicates the user authentication mode. ● 1: RADIUS authentication ● 2: local authentication
46	Acct-Session-Time	Indicates the time for a user to go online in the unit of second.
47	Acct-Input-Packets	Indicates the number of upstream packets.
48	Acct-Output-Packets	Indicates the number of downstream packets.
49	Terminate-Cause	Indicates the user connection interruption cause. The valid values are as follows: ● User-Request(1): The user actively goes offline. ● Lost Carrier(2): The handshake fails, such as the EAPOL detection fails. ● User Error(17): The user authentication fails or times out.
52	Acct-Input-Gigawords	Indicates the number of upstream bytes in the unit of 4Gbyte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.

Parameter Code	Parameter Name	Description
53	Acct-Output-Gigawords	Indicates the number of downstream bytes in the unit of 4Gbyte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
55	Event-Timestamp	Indicates the user online time in the unit of second. The value is the absolute number of seconds counting from 1970-01-01 00:00:00.
60	CHAP-Challenge	Indicates the challenge field for CHAP authentication. This parameter is valid only for CHAP authentication.
61	NAS-Port-Type	Indicates the NAS port type.
79	EAP-Message	Carries EAP packets.
80	Message-Authenticator	Verifies validity of packets between the RADIUS server and RADIUS client to prevent malicious attacks.
85	Acct-Interim-Interval	Indicates the interval for real-time charging in the unit of second.
87	NAS-Port-Id	Indicates the user access port number. The format of this parameter uses the format when DHCP option 82 is in common raio mode.
88	Framed-Pool	Indicates the name and address segment number of the address pool. After being delivered by the RADIUS server, this parameter is filled to suboption 7 in user DHCP packets by the MA5600T/MA5603T.
26-29 **NOTE** The preceding parameters are RADIUS standard attributes. Starting from this row, the following parameters are Huawei-defined attributes.	Exec-Privilege	Indicates the priority of operation users such as SSH users. The value ranges from 0 to 15. ● 0: common user ● 1: operator ● 2: administrator ● 3-15: common user

Parameter Code	Parameter Name	Description
26-60	Ip-Host-Address	Indicates the user IP address and MAC address that are contained in authentication and charging packets. The format is A.B.C.D HH:HH:HH:HH:HH:HH. The IP address and MAC address are separated by a space.
26-254	Version	Indicates the software version of the access device.
26-255	Product-ID	Indicates the product name.

NOTE

The super level user cannot be authenticated. You can query the user level by the command **display terminal user**.

Procedure

Step 1 Configure the authentication scheme.

NOTE

- The authentication scheme specifies how all the users in an ISP domain are authenticated.
- The system supports up to 16 authentication schemes. The system has a default accounting scheme named **default**. It can only be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode radius** command to configure the authentication mode of the authentication scheme.
4. Run the **quit** command to return to the AAA mode.

Step 2 Configure the accounting scheme.

NOTE

- The accounting scheme specifies how all the users in an ISP domain are charged.
- The system supports up to 128 accounting schemes. The system has a default accounting scheme named **default**. It can be modified, but cannot be deleted.

1. In the AAA mode, run the **accounting-scheme** command to add an AAA accounting scheme.
2. Run the **accounting-mode radius** command to configure the accounting mode.
3. Run the **accounting interim interval** command to set the interval of real-time accounting. By default, the interval is 0 minutes, that is, the real-time accounting is not performed.
4. Run the **quit** command to return to the AAA mode.

Step 3 Configure the RADIUS server template.

1. Run the **radius-server template** command to create an RADIUS server template and enter the RADIUS server template mode.
2. Run the **radius-server authentication** command to configure the IP address and the UDP port ID of the RADIUS server for authentication.

NOTE

- To guarantee normal communication between the MA5600T/MA5603T and the RADIUS server, before configuring the IP address and UDP port of the RADIUS server, make sure that the route between the RADIUS server and the MA5600T/MA5603T is in the normal state.
- Make sure that the configuration of the RADIUS service port of the MA5600T/MA5603T is consistent with the port configuration of the RADIUS server.

3. Run the **radius-server accounting** command to configure the IP address and the UDP port ID of the RADIUS server for accounting.
4. Run the **radius-server shared-key** command to configure the shared key of the RADIUS server.

   NOTE

   - The RADIUS client (MA5600T/MA5603T) and the RADIUS server use the MD5 algorithm to encrypt the RADIUS packets. They check the validity of the packets by setting the encryption key. They can receive the packets from each other and can respond to each other only when their keys are the same.
   - By default, the shared key of the RADIUS server is **huawei**.
5. (Optional) Run the **radius-server timeout** command to set the response timeout time of the RADIUS server. By default, the timeout time is 5s.

   The MA5600T/MA5603T sends the request packets to the RADIUS server. If the RADIUS server does not respond within the response timeout time, the MA5600T/MA5603T re-transmits the request packets to the RADIUS to ensure that users can get corresponding services from the RADIUS server.
6. (Optional) Run the **radius-server retransmit** command to set the maximum re-transmit time of the RADIUS request packets. By default, the maximum re-transmit time is 3.

   When the re-transmit time of the RADIUS request packets to a RADIUS server exceeds the maximum re-transmit time, the MA5600T/MA5603T considers that its communication with the RADIUS server is interrupted, and therefore transmits the RADIUS request packets to another RADIUS server.
7. Run the **(undo)radius-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the RADIUS server. By default, the user name of the RADIUS server carries the domain name.
   - An access user is named in the format of **userid@domain-name**, and the part after @ is the domain name. The MA5600T/MA5603T classifies a user into a domain according to the domain name.
   - If an RADIUS server group rejects the user name carrying the domain name, the RADIUS server group cannot be set or used in two or more domains. Otherwise, when some access users in different domains have the same user name, the RADIUS server considers that these users are the same because the names transmitted to the server are the same.
8. Run the **quit** command to return to the global config mode.

Step 4 Create a domain.

A domain is a group of users of the same type.

In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.

The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In the AAA mode, run the **domain** command to create a domain.

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

In the domain mode, run the **authentication-scheme** command to use the authentication scheme.

Step 6 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

In the domain mode, run the **accounting-scheme** command to use the accounting scheme.

Step 7 Use the RADIUS server template.

NOTE

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

1. In the domain mode, run the **radius-server template** command to use the RADIUS server template.
2. Run the **quit** command to return to the AAA mode.

----End

Example

User1 in the isp domain adopts the HWTACACS protocol for authentication and accounting. The accounting interval is 10 minutes, the authentication password is a123456, HWTACACS server 10.10.66.66 functions as the primary authentication and accounting server, and HWTACACS server 10.10.66.67 functions as the standby authentication and accounting server. On the HWTACACS server, the authentication port ID is 1812, accounting port ID 1813, and other parameters adopt the default values. To perform the preceding configuration, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config)#radius-server template hwtest
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.67 1812
secondary
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.66 1813
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-radius-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#radius-server hwtest
huawei(config-aaa-domain-isp)#quit
```

2.11.3 Configuration Example of the RADIUS Authentication and Accounting

The MA5600T/MA5603T is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

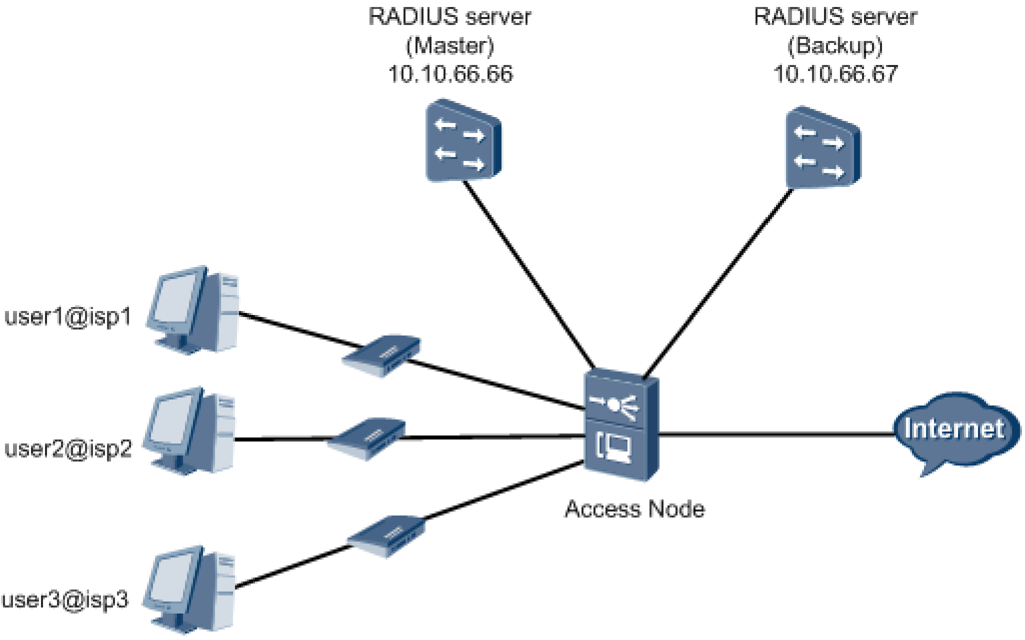
Service Requirements

- The RADIUS server performs authentication and accounting for users in the ISP1 and ISP2 domains.
- The RADIUS server with the IP address 10.10.66.66 functions as the primary server for authentication and accounting.
- The RADIUS server with the IP address 10.10.66.67 functions as the secondary server for authentication and accounting.
- The authentication port number is 1812, and the accounting port number is 1813.
- Other parameters adopt the default settings.

Networking

Figure 2-11 shows an example network of the RADIUS Authentication and Accounting application.

Figure 2-11 Example network of the RADIUS Authentication and Accounting application.



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **newscheme** (users are authenticated through RADIUS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
  Info: Create a new authentication scheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
```

Step 2 Configure the accounting scheme.

Configure accounting scheme named **newscheme** (users are authenticated through RADIUS). the interval is 10 minutes.

```
huawei(config-aaa)#accounting-scheme newscheme
  Info: Create a new accounting scheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
```

Step 3 Configure the RADIUS protocol.

Create RADIUS server template named **hwtest** with the RADIUS server 10.10.66.66 as the primary authentication and accounting server, and the RADIUS server 10.10.66.67 as the secondary authentication and accounting server.

```
huawei(config)#radius-server template hwtacacs
 Note: Create a new server template
huawei(config-radius-hwtacacs)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-hwtacacs)#radius-server authentication 10.10.66.67 1812
secondary
huawei(config-radius-hwtacacs)#radius-server accounting 10.10.66.66 1813
huawei(config-radius-hwtacacs)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-radius-hwtacacs)#quit
```

Step 4 Create a domain.

Create a domain named isp1.

```
huawei(config)
#aaa
huawei(config-aaa)#domain isp1
  Info: Create a new domain
```

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 6 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

```
huawei(config-aaa-domain-isp1)#accounting-scheme newscheme
```

Step 7 Use the RADIUS server template.

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

```
huawei(config-aaa-domain-isp1)#radius-server hwtacacs
huawei(config-aaa-domain-isp1)#quit
```

----End

Result

User 1 in ISP 1 can pass authentication only if both the user name and password are correct, and then can log in to the MA5600T/MA5603T. Then, the user starts to be accounted.

Configuration File

```
aaa
authentication-scheme newscheme
authentication-mode radius
quit
accounting-scheme
newscheme
accounting-mode
radius
accounting interim interval 10
quit
quit
radius-server template radtest
radius-server authentication 10.10.66.66
1812
radius-server authentication 10.10.66.67 1812 secondary
radius-server accounting 10.10.66.66
1813
radius-server accounting 10.10.66.67 1813 secondary
quit
aaa

domain
isp1
authentication-scheme newscheme
accounting-scheme newscheme
radius-server
hwtacacs
quit
```

2.11.4 Configuring the Remote AAA (HWTACACS Protocol)

The MA5600T/MA5603T is interconnected with the HWTACACS server through the HWTACACS protocol to implement authentication, authorization, and accounting.

Context

- What is HWTACACS:
  - HWTACACS is a security protocol with enhanced functions on the base of TACACS (RFC1492). Similar to the RADIUS protocol, HWTACACS implements multiple subscriber AAA functions through communications with the HWTACACS server in the client/server (C/S) mode.
  - HWTACACS is used for the authentication, authorization, and accounting for the 802.1 access users and management users.
- Principle of HWTACACS:

  Adopting the client/server architecture, HWTACACS is a protocol through which the NAS (MA5600T/MA5603T) transmits the encrypted HWTACACS data packets to communicate with the HWTACACS database of the security server. The working mode is as follows:
  - HWTACACS authentication. When the remote user connects to the corresponding port of the NAS, the NAS communicates with the daemon of the HWTACACS server, and obtains the prompt of entering the user name from the daemon. Then, the NAS displays

the message to the user. When the remote user enters the user name, the NAS transmits the user name to the daemon. Then, the NAS obtains the prompt of entering the password, and displays the message to the user. After the remote user enters the password, the NAS transmits the password to the daemon.

- HWTACACS authorization. After being authenticated, the user can be authorized. The NAS communicates with the daemon of the HWTACACS server, and then returns the accept or reject response of the authorization.

NOTE

- The HWTACACS configuration only defines the parameters used for data exchange between the MA5600T/MA5603T and the HWTACACS server. To make these parameters take effect, you need to use the HWTACACS server group in a domain.
- The settings of an HWTACACS server template can be modified regardless of whether the template is bound to a server or not.

Procedure

Step 1 Configure the AAA authentication scheme.

The authentication scheme specifies how all the users in an ISP domain are authenticated.

The system supports up to 16 authentication schemes. The system has a default authentication scheme named **default**. It can be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode local** command to configure the authentication mode of the authentication scheme. Use the HWTACACS protocol to authenticate users.
4. Run the **quit** command to return to the AAA mode.

Step 2 Configure the AAA authorization scheme.

The authorization scheme specifies how all the users in an ISP domain are authorized.

1. In the AAA mode, run the **authorization-scheme** command to add an AAA authorization scheme.
2. Run the **authorization-mode hwtacacs** command to configure the authorization mode.
3. Run the **quit** command to return to the AAA mode.
4. Run the **quit** command to return to the global config mode.

Step 3 Configure the AAA accounting scheme.

The accounting scheme specifies how all the users in an ISP domain are charged.

The system supports up to 128 accounting schemes. The system has a default accounting scheme named **default**. It can be modified, but cannot be deleted.

1. In the AAA mode, run the **accounting-scheme** command to add an AAA accounting scheme.
2. Run the **accounting-mode hwtacacs** command to configure the accounting mode. By default, the accounting is not performed.
3. Run the **accounting interim interval** command to set the interval of real-time accounting. By default, the interval is 0 minutes, that is, the real-time accounting is not performed.
4. Run the **quit** command to return to the AAA mode.

Step 4 Configure the HWTACACS protocol.

The configuration of the HWTACACS protocol of the MA5600T/MA5603T is on the basis of the HWTACACS server group. In actual networking scenarios, an HWTACACS server group can be an independent HWTACACS server or a combination of two HWTACACS servers, that is, a primary server and a secondary server with the same configuration but different IP addresses.

Each HWTACACS server template contains the primary/secondary server IP address, shared key, and HWTACACS server type.

Primary and secondary authentication, accounting, and authorization servers can be configured. The IP address of the primary server, however, must be different from that of the secondary server. Otherwise, the configuration of primary and secondary servers will fail. By default, the IP addresses of the primary and secondary servers are both 0.0.0.0.

1. Run the **hwtacacs-server template** command to create an HWTACACS server template and enter the HWTACACS server template mode.
2. Run the **hwtacacs-server authentication** command to configure a primary authentication server. You can select **secondary** to configure a secondary authentication server.

   NOTE

   - To ensure normal communication between the MA5600T/MA5603T and the HWTACACS server, before configuring the IP address and the UDP port of the HWTACACS server, make sure that the route between the HWTACACS server and the MA5600T/MA5603T is in the normal state.
   - Make sure that the HWTACACS server port of the MA5600T/MA5603T is the same as the port of the HWTACACS server.
3. Run the **hwtacacs-server accounting** command to configure a primary accounting server. You can select **secondary** to configure a secondary accounting server.
4. Run the **hwtacacs-server authorization** command to configure a primary authorization server. You can select **secondary** to configure a secondary authorization server.
5. (Optional) Run the **hwtacacs-server shared-key** command to configure the shared key of the HWTACACS server.

   NOTE

   - The HWTACACS client (MA5600T/MA5603T) and the HWTACACS server use the MD5 algorithm to encrypt the HWTACACS packets. They check the validity of the packets by configuring the encryption key. They can receive the packets from each other and can respond to each other only when their keys are the same.
   - By default, the HWTACACS server does not have a key.
6. (Optional) Run the **hwtacacs-server timer response-timeout** to set the response timeout time of the HWTACACS server.

   NOTE

   - If the HWTACACS server does not respond to the HWTACACS request packets within the timeout time, the communication between the MA5600T/MA5603T and the current HWTACACS server is considered as interrupted.
   - By default, the response timeout time of the HWTACACS server is 5s.
7. (Optional) In the global config mode, run the **hwtacacs-server accounting-stop-packet** command to configure the re-transmission mechanism of the accounting-stop packets of the HWTACACS server.

NOTE

- To prevent the loss of the accounting packets, the MA5600T/MA5603T supports the re-transmission of the accounting-stop packets of the HWTACACS server.
- By default, the re-transmit time of the accounting-stop packets of the HWTACACS server is 100.

8. (Optional) Run the **(undo)hwtacacs-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the HWTACACS server.
   - By default, the user name of the HWTACACS server carries the domain name.
   - After the **undo hwtacacs-server user-name domain-included** command is executed, the domain name is deleted from the user name when the client sends authentication and authorization requests to the HWTACACS server. The domain name in the user name of the accounting request is, however, reserved. This is to ensure that the users can be distinguished from each other in the accounting.
9. Run the **quit** command to return to the global config mode.

Step 5 Create a domain.

A domain is a group of users of the same type.

In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.

The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In the AAA mode, run the **domain** command to create a domain.

Step 6 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

In the domain mode, run the **authentication-scheme** command to use the authentication scheme.

Step 7 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

In the domain mode, run the **accounting-scheme** command to use the accounting scheme.

Step 8 Use the authorization scheme.

You can use an authorization scheme in a domain only after the authorization scheme is created.

In the domain mode, run the **authorization-mode** command to use the authorization scheme.

Step 9 Use the HWTACACS server template.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

1. In the domain mode, run the **hwtacacs-server** command to use the HWTACACS server template.
2. Run the **quit** command to return to the AAA mode.

----End

Example

User1 in the isp domain adopts the HWTACACS protocol for authentication, authorization, and accounting. The accounting interval is 10 minutes, the authentication password is a123456, HWTACACS server 10.10.66.66 functions as the primary authentication, authorization, and accounting server, and HWTACACS server 10.10.66.67 functions as the standby authentication, authorization, and accounting server. On the HWTACACS server, the parameters adopt the default values. To perform the preceding configuration, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode hwtacacs
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#authorization-scheme newscheme
huawei(config-aaa-author-newscheme)#authorization-mode hwtacacs
huawei(config-aaa-author-newscheme)#quit
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode hwtacacs
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config)#hwtacacs-server template hwtest
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 10.10.66.67
secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#authorization-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#hwtacacs-server hwtest
huawei(config-aaa-domain-isp)#quit
```

2.11.5 Configuration Example of the HWTACACS Authentication (802.1X access user)

The MA5600T/MA5603T is interconnected with the HWTACACS server through the HWTACACS protocol to implement authentication, authorization, and accounting.

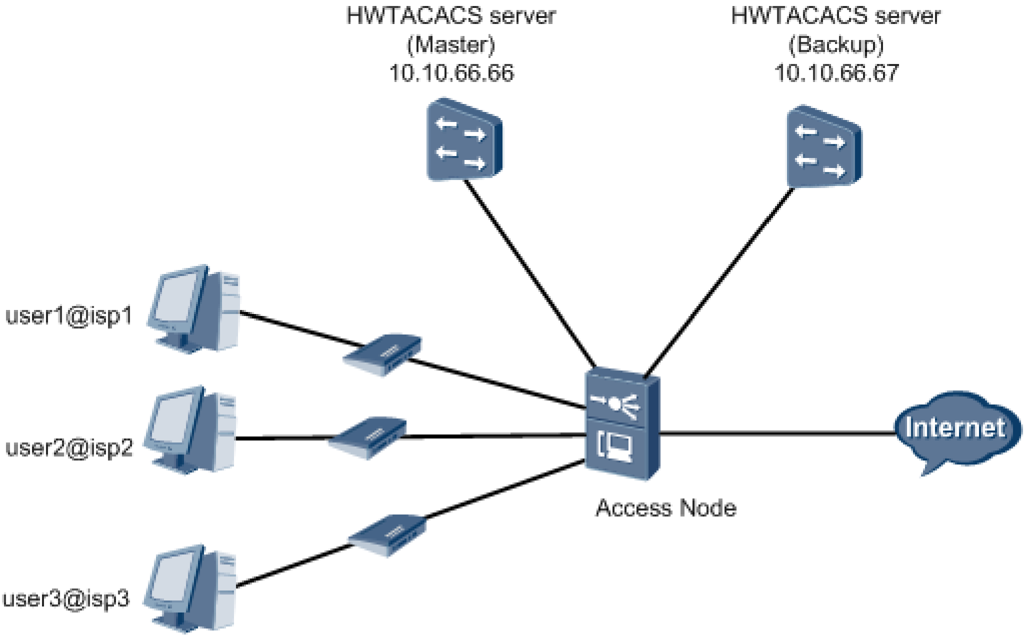
Service Requirements

- The HWTACACS server performs authentication, authorization, and accounting for 802.1X access users.
- The user logs in to the server carrying the domain name.
- The HWTACACS server with the IP address 10.10.66.66 functions as the primary server for authentication, authorization, and accounting.
- The HWTACACS server with the IP address 10.10.66.67 functions as the secondary server for authentication, authorization, and accounting.
- Other parameters adopt the default settings.

Networking

Figure 2-12 shows an example network of the HWTACACS authentication.

Figure 2-12 Example network of the HWTACACS authentication



Procedure

Step 1 Configure an authentication scheme.

Configure authentication scheme named **newscheme** (users are authenticated through HWTACACS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode hwtacacs
huawei(config-aaa-authen-newscheme)#quit
```

Step 2 Configure an authorization scheme.

Configure authorization scheme named **newscheme** (users are authorized through HWTACACS).

```
huawei(config-aaa)#authorization-scheme newscheme
huawei(config-aaa-author-newscheme)#authorization-mode hwtacacs
huawei(config-aaa-author-newscheme)#quit
```

Step 3 Configure the accounting scheme.

Configure accounting scheme named **newscheme** (users are authenticated through HWTACACS). the interval is 10 minutes.

```
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode hwtacacs
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
```

Step 4 Configure the HWTACACS protocol.

Create HWTACACS server template named **hwtest** with the HWTACACS server 10.10.66.66 as the primary authentication, authorization and accounting server, and the HWTACACS server 10.10.66.67 as the secondary authentication, authorization and accounting server.

```
huawei(config)#hwtacacs-server template hwtest
  Create a new HWTACACS-server template
huawei(config-hwtacacs-radtest)#hwtacacs-server authentication 10.10.66.66
huawei(config-hwtacacs-radtest)#hwtacacs-server authentication 10.10.66.67
secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.67 secondary
huawei(config-hwtacacs-radtest)#hwtacacs-server accounting 10.10.66.66
huawei(config-hwtacacs-radtest)#hwtacacs-server accounting 10.10.66.67 secondary
huawei(config-hwtacacs-radtest)#quit
```

Step 5 Configure the 802.1X authentication.

1. Enable the 802.1X global switch. Enable the 802.1X authentication for ports 1, 2, and 3. The 802.1X needs to be triggered by DHCP. Therefore, the DHCP-trigger authentication must be enabled.

```
huawei(config)#dot1x enable
huawei(config)#dot1x service-port 1
huawei(config)#dot1x service-port 2
huawei(config)#dot1x service-port 3
huawei(config)#dot1x dhcp-trigger enable
```

2. Configure an 802.1X parameters. In the local termination authentication, the 802.1X parameters should be configured to be in the EAP termination mode. The count of allowed handshake failure is 1 and the handshake interval is 20s.

```
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 1
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 2
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 3
huawei(config)#dot1x eap-end service-port 1
huawei(config)#dot1x eap-end service-port 2
huawei(config)#dot1x eap-end service-port 3
```

Step 6 Create a domain.

Create a domain named isp1.

```
huawei(config)
#aaa
huawei(config-aaa)#domain isp1
  Info: Create a new domain
```

Step 7 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 8 Use the authorization scheme.

You can use an authorization scheme in a domain only after the authorization scheme is created.

```
huawei(config-aaa-domain-isp1)#authorization-scheme newscheme
```

Step 9 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

```
huawei(config-aaa-domain-isp1)#accounting-scheme newscheme
```

Step 10 Bind the HWTACACS server template.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

```
huawei(config-aaa-domain-isp1)#hwtacacs-server hwtest
```

----End

Result

User 1 in ISP 1 can pass authentication only if both the user name and password are correct, and then can log in to the MA5600T/MA5603T. Then, the user starts to be accounted.

Configuration File

```
aaa
authentication-scheme newscheme
authentication-mode hwtacacs
quit
authorization-scheme newscheme
authorization-mode hwtacacs
quit
accounting-scheme newscheme
accounting-mode hwtacacs
accounting interim interval 10
quit
quit
hwtacacs-server template hwtest
hwtacacs-server authentication 10.10.66.66
hwtacacs-server authentication 10.10.66.67 secondary
hwtacacs-server authorization 10.10.66.66
hwtacacs-server authorization 10.10.66.67 secondary
hwtacacs-server accounting 10.10.66.66
hwtacacs-server accounting 10.10.66.67 secondary
quit
dot1x enable
dot1x service-port 1
dot1x service-port 2
dot1x service-port 3
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 1
dot1x keepalive retransmit 1 interval 20 service-port 2
dot1x keepalive retransmit 1 interval 20 service-port 3
dot1x eap-end service-port 1
dot1x eap-end service-port 2
dot1x eap-end service-port 3


domain
isp1
authentication-scheme newscheme
authorization-scheme newscheme
accounting-scheme newscheme
hwtacacs-server hwtest
```

2.11.6 Configuration Example of HWTACACS Authentication (Management User)

The MA5600T/MA5603T allows the management user of the device to log in to the system by the HWTACACS authentication mode.

Prerequisites

- The route from the MA5600T/MA5603T to the HWTACACS server must be configured.
- The management user information (user name@domain and password) must be configured on the HWTACACS server.

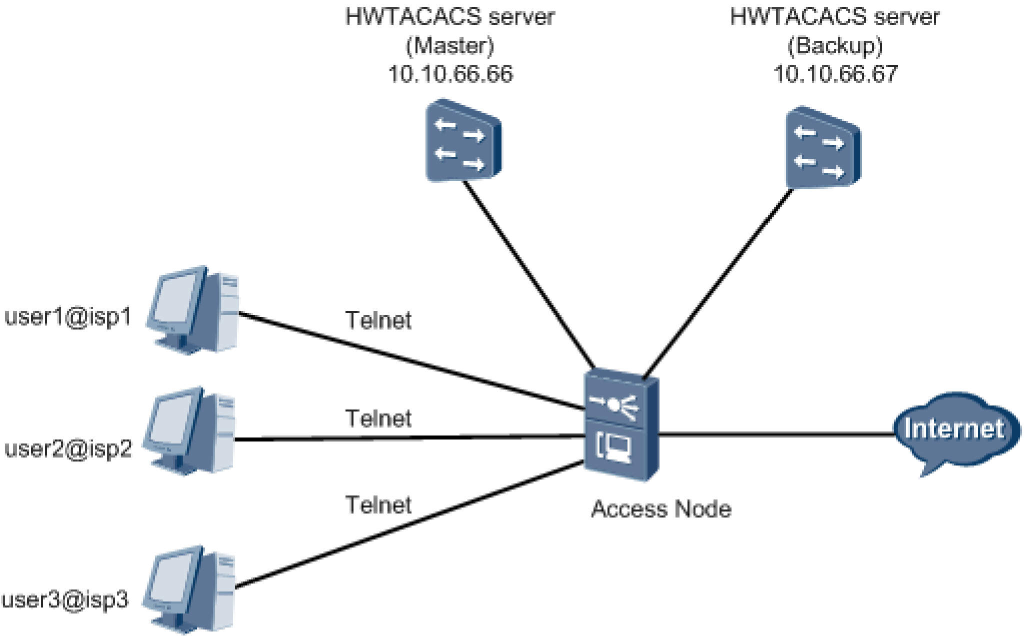
Service Requirements

- The HWTACACS server performs authentication for management user of domain **isp1**.
- The user logs in to the server carrying the domain name.
- The HWTACACS server with the IP address 10.10.66.66 functions as the primary server for authentication.
- The HWTACACS server with the IP address 10.10.66.67 functions as the secondary server for authentication.
- Other parameters adopt the default settings.

Networking

Figure 2-13 shows an example network of HWTACACS authentication.

Figure 2-13 Example network of HWTACACS authentication



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **login-auth** (users are authenticated through HWTACACS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme login-auth
huawei(config-aaa-authen-login-auth)#authentication-mode hwtacacs
huawei(config-aaa-authen-login-auth)#quit
```

Step 2 Configure the HWTACACS protocol.

Create HWTACACS server template named **ma56t-login** with HWTACACS server 10.10.66.66 as the primary authentication server, and HWTACACS server 10.10.66.67 as the secondary authentication server.

```
huawei(config)#hwtacacs-server template ma56t-login
  Create a new HWTACACS-server template
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.66
1812
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.67
1812 secondary
huawei(config-hwtacacs-ma56t-login)#quit
```

Step 3 Create a domain named **isp1**.

NOTE

- A domain is a group of users of the same type.
- In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

```
huawei(config)#aaa
huawei(config-aaa)#domain isp1
  Info: Create a new domain
```

Step 4 Use the authentication scheme **login-auth**.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme login-auth
```

Step 5 Bind the HWTACACS server template **ma56t-login** to the user.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

```
huawei(config-aaa-domain-isp1)#hwtacacs-server ma56t-login
```

----End

Result

- When the HWTACACS server is reachable, the management user can log in to the MA5600T/MA5603T through Telnet. After entering the user name and password specified on the HWTACACS server, the management user can successfully log in to the MA5600T/MA5603T.
- When the HWTACACS server is unreachable, the management user cannot log in to the MA5600T/MA5603T through Telnet by entering the user name and password specified on the HWTACACS server.

Configuration File

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme login-auth
huawei(config-aaa-authen-login-auth)#authentication-mode hwtacacs
huawei(config-aaa-authen-login-auth)#quit
huawei(config-aaa)#quit
huawei(config)#hwtacacs-server template ma56t-login
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.66
1812
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.67
1812 secondary
huawei(config-hwtacacs-ma56t-login)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp1
huawei(config-aaa-domain-isp1)#authentication-scheme login-auth
huawei(config-aaa-domain-isp1)#hwtacacs-server ma56t-login
huawei(config-aaa-domain-isp1)#quit
huawei(config-aaa)#quit
```

2.12 Configuring ANCP

Access Node Control Protocol (ANCP) is used to implement the functions such as topology discovery, line configuration, and L2C OAM on the user ports. The MA5600T/MA5603T establishes an ANCP session according to the GSMP communication IP address configured in the network access server (NAS).

Prerequisites

- The system must work in the normal state.
- The system must be connected to the network access server in the normal state.

Context

- The MA5600T/MA5603T and the NAS use the TCP connection to carry an ANCP session. Therefore, before creating the ANCP session, you must create a TCP connection between the MA5600T/MA5603T and the NAS. The NAS functions as the server of the TCP connection, and the MA5600T/MA5603T functions as the client of the TCP connection.
- After the TCP connection is created successfully between the MA5600T/MA5603T and the NAS, an ANCP session is created between the MA5600T/MA5603T and the NAS. After the ANCP session is created successfully, the MA5600T/MA5603T and the NAS need to use the ANCP ACK packets for heartbeat detection to maintain the ANCP session.
- The default values of the ANCP parameters are as follows:
  - GSMP address for an ANCP session: 0.0.0.0
  - ANCP session capability set: topology-discovery, line-config, and oam
  - ANCP packet sending priority: highest level 6
  - GSMP TCP communication port number on the NAS side in an ANCP session: 6068
  - Interval for sending packets during the initial stage of an ANCP session: 10 (unit: 0.1s)
  - Interval for sending packets during the ANCP session stage: 100 (unit: 0.1s)

Procedure

Step 1 Run the **ancp partition enable** command to enable the ANCP partition function.

By default, the ANCP partition function is disabled.

Step 2 Run the **ancp port** command to enable the ANCP function of a port.

The ANCP function takes effect only when the ANCP function in the ANCP session mode and ANCP session function of a port are enabled.

Step 3 (Optional) Run the **ancp version** command to configure the ANCP version.

- The configured ANCP version must be the same as that on the NAS.
- By default, the ANCP version is draft-01.

Step 4 Run the **ancp session** command to enter the ANCP session mode.

Step 5 (Optional) Run the **ancp partition** command to configure the ID of the partition associated with an ANCP session.

Step 6 Run the **ancp ip** command to configure the GSMP communication IP address for the ANCP session.

- The IP address configured here must be the same as the GSMP communication IP address configured on the NAS, but it should to not be the same as the default IP address, multicast IP address, or broadcast IP address.
- When an ANCP session is enabled, the GSMP communication IP address cannot be configured.

Step 7 (Optional) Run the **ancp capability** command to configure the capability set of the ANCP session.

- Supports topology discovery. When you select **topology-discovery** parameter, the MA5600T/MA5603T automatically reports the line parameters to the NAS.
- Supports line configuration. When you select **line-config** parameter, the MA5600T/MA5603T responds to the line configuration that is sent by the NAS.
- Supports the OAM. When you select **oam** parameter, the MA5600T/MA5603T responds to the line testing information that is sent by the NAS.
- Supports the preceding three types of capability.
- The default value is all, that is, the three capabilities (topology discovery, line configuration, and L2C OAM) are supported.

Step 8 (Optional) Run the **ancp ancp-8021p** command to set the priority for sending ANCP packets.

- You can set the priority according to the actual requirements and network conditions, the higher the priority, the higher the reliability.
- After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 9 (Optional) Run the **ancp nas-tcp-port** command to set the GSMP TCP communication port number for the ANCP session on the NAS.

- By default, the GSMP TCP communication port number is 6068.
- The GSMP TCP communication port number on the MA5600T/MA5603T must be the same as that on the NAS.
- Run the **ancp port begin** command to set the start port ID of the ANCP session. Make sure that the start port ID of the ANCP session is the same as the start ID of the ports on the service board.

Step 10 (Optional) Run the **ancp init-interval** command to set the interval for sending packets during the establishment of the ANCP session.

- By default, the general query interval is 125s.
- After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 11 (Optional) Run the **ancp keep-alive** command to set the interval for sending packets during the ACNP session so that the handshake messages can be sent to the peer end at the preset interval.

- By default, the interval is 10s.
- After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 12 (Optional) Run the **ancp bandwidthCAC** command to enable the ANCP multicast CAC. After the ANCP multicast CAC is enabled, if the bandwidth of the demanded multicast program is larger than the available multicast bandwidth of the user, the user can apply for the bandwidth resource of the unicast VOD program.

- After an ANCP session is enabled, its ANCP multicast CAC function cannot be enabled or disabled.
- The ANCP multicast CAC function of only one session can be enabled at a time.
- After the ANCP multicast CAC function is enabled, if the **ancp disable** command is executed, the ANCP will be disabled. The system still performs CAC using the bandwidth issued by the ANCP CAC and the original BTV CAC does not take effect. In this case, the normal BTV CAC takes effect only when the ANCP CAC function of the ANCP session is disabled by running the **ancp bandwidthCAC disable** command.

Step 13 Run the **ancp enable** command to enable the ANCP session.

- By default, the ANCP session is disabled.
- Before an ANCP session is enabled, related parameters can be modified. After an ANCP session is enabled, related parameters cannot be modified.

Step 14 Run the **quit** command to quit the ANCP mode.

Step 15 Run the **display ancp session** command to query the information about the ANCP session.

----End

Example

Consider configuring the ANCP topology discovery function of port 0/3/1 as an example. Configure the partition ID of the ANCP session to 1, ANCP version to draft-02, start port ID to 1, GSMP communication address of the ANCP session to 10.10.10.10, packet sending interval at the ANCP session creation phase to 2s, ANCP session capability set to topology-discovery, ANCP packet sending priority to 7, GSMP TCP communication port ID at the NSA side in the ANCP session to 6000, and packet sending interval at the ANCP session phase to 7s.

```
huawei(config)#ancp partition enable
huawei(config)#ancp port 0/3/1 partition 1
huawei(config)#ancp version draft-02
huawei(config)#ancp port begin 1
huawei(config)#ancp session 1
huawei(config-session-1)#ancp partition 1
huawei(config-session-1)#ancp ip 10.10.10.10
huawei(config-session-1)#ancp capability topology-discovery
huawei(config-session-1)#ancp ancp-8021p 7
huawei(config-session-1)#ancp nas-tcp-port 6000
huawei(config-session-1)#ancp init-interval 20
huawei(config-session-1)#ancp keep-alive 70
huawei(config-session-1)#ancp bandwidthCAC enable
huawei(config-session-1)#ancp enable
huawei(config-session-1)#quit
huawei(config)#display ancp session 1

  Session config status               : Enable
  Session running status              : Before syn phase
  Session diagnostic status           : -
  GSMP version                        : 3
  GSMP sub version                      : 1
  AN name                               : -
  NAS name                              : -
  NAS IP                                : 10.10.10.10
  Local IP                              : -
  AN instance                           : -
  NAS instance                          : -
  Config capabilities                   : TopologyDiscovery
  Negotiate capabilities                : -
  NAS TCP port                          : 6000
  Startup time(0.01s)                   : -
  Discontinuity time(0.01s)             : -
  Init interval(0.1s)                   : 20
  Keepalive interval(0.1s)              : 70
  PartitionID                           : 1
  Bandwidth CAC status                  : Enable
  Line config roll default              : Disable
  OAM threshold(0.01)                   : 100
  Topology report shaper interval(0.1s) : 10
  S-VLAN                                : -
  S-VLAN priority                       : 7
  C-VLAN                                : -
  C-VLAN priority                       : -
  Session down send trap status         : Disable
  Session up send trap status           : Disable
```

3 Configuring Layer 3 Features

About This Chapter

L3 feature configurations include configurations of common Layer 3 protocols and features. There is no obvious logical relation between Layer 3 feature configurations. You can perform Layer 3 feature configurations according to actual requirements.

3.1 Configuring Basic IPv6 Information
This topic describes the IPv6 features supported by the MA5600T/MA5603T. The basic IPv6 configuration includes configuration of the IPv6 address, IPv6 neighbor, path maximum transmission unit (PTMU), and transmission control protocol 6 (TCP6).

3.2 Configuring the IP-aware Bridge
After the IP-aware bridge function is enabled on the MA5600T/MA5603T, in the upstream direction of the MA5600T/MA5603T, user data can be forwarded to different upper-layer devices according to the destination IP address and the configured static route. With the IP-aware bridge function enabled, the MA5600T/MA5603T features the ARP proxy function: shielding the MAC address of the network-side device for the user side and shielding the user-side MAC address for the network side.

3.3 Configuring DHCP
The MA5600T/MA5603T can implement DHCP relay and DHCP proxy on a network. Configuring DHCP relay is applicable to the scenario where users dynamically obtain IP addresses from the DHCP server through DHCP. In DHCP proxy, the MA5600T/MA5603T proxy can implement certain functions of the DHCP server.

3.4 Configuring the Route
This topic describes the routing policy supported by the MA5600T/MA5603T and how to configure the routing protocol.

3.1 Configuring Basic IPv6 Information

This topic describes the IPv6 features supported by the MA5600T/MA5603T. The basic IPv6 configuration includes configuration of the IPv6 address, IPv6 neighbor, path maximum transmission unit (PTMU), and transmission control protocol 6 (TCP6).

Context

Internet Protocol Version 6 (IPv6), also called IP next generation (IPNG), is the second-generation standard protocol of network layer protocols. As a set of specifications defined by the Internet Engineering Task Force (IETF), IPv6 is the upgraded version of Internet Protocol Version 4 (IPv4). The most obvious difference between IPv6 and IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. IPv6 radically solves the problem of IP address shortage. Moreover, IPv6 has the following advantages: It is easy to deploy, compatible with various applications, easy for IPv4 networks to transit to IPv6 networks, and coexists and interworks with IPv4 networks.

The following table lists the IPv6 features supported by the MA5600T/MA5603T.

Table 3-1 IPv6 features supported by the MA5600T/MA5603T

Feature	Sub-feature	Configuration Process or Command
IPv6 address management and assignment	Static configuration of IPv6 global unicast addresses and IPv6 link-local addresses	**Configuring an IPv6 Address for an Interface**
	Automatic configuration of IPv6 link-local addresses	ipv6 address auto link-local
	DHCPv6, DHCPv6 L2/L3 Relay	**Configuring DHCP**
	Management information base (MIB) for IPv6 address management	-
IPv6 stack and IPv6 host function	IPv6/IPv4 dual-stack to ensure compatibility of IPv6 and IPv4	-
	Basic IPv6 protocols, including ICMPv6, TCP6, UDP6, and RawIP6	-
	IPv6 packet processing on the Layer 3 interface	-
	IPv6 Neighbor Discovery (ND) protocol and static configuration of IPv6 neighbors	**Configuring IPv6 Neighbor Discovery**
	IPv6 PMTU	**Configuring PMTU**

Feature	Sub-feature	Configuration Process or Command
	IPv6 ping and tracert	● ping ipv6 ● tracert ipv6
	IPv6 statistics query and clearance	● display ipv6 statistics ● reset ipv6 statistics
IPv6 route	IPv6 static routes	**Configuration Example of the IPv6 Static Route**
	BGP4+	**Configuration Example of BGP4+**
IPv6 QoS and security	IPv6 ACL	**Configuring ACL**
	Anti-MAC spoofing and 1:1 VMAC	**Configuring Anti-MAC Spoofing**
	Anti-IPv6 spoofing	**Configuring Anti-IP Spoofing**
	Anti-denial of service (DoS) attack	**Configuring Anti-Attack**
	DAD Proxy	ipv6 dad proxy
	Proxy advertisement for neighbor solicitation (NS) on the network side	-
IPv6 Layer 2 Transparent Transmission	Differentiation of service virtual ports based on the IPv6 over Ethernet (IPv6oE) type (0x86DD) and defining of VLANs for service virtual ports	service-port
	Transparent transmission of IPv6 over PPPoE packets	-
	VLAN-based transparent transmission of IPv6 packets	-

NOTE

In this manual:

- For the IPv6 features that are different from IPv4 features, configuration procedures and examples are provided for both IPv6 and IPv4 features.
- For the IPv6 features that are similar with IPv4 features, configuration procedures and examples are not provided for IPv6 features because they are the same as IPv4 features. To configure these IPv6 features, use IPv6 commands and follow the procedures of IPv4 features.

3.1.1 Configuring an IPv6 Address for an Interface

The MA5600T/MA5603T can communicate with other IPv6 equipment after its interface is configured with an IPv6 address. Before an IPv6 global unicast address or IPv6 link-local address is configured on an interface, the IPv6 packet forwarding function must be enabled on the device.

Context

Each interface can be configured with a maximum of ten global unicast addresses and only one link-local address.

- The global unicast address is equivalent to the IPv4 public address. It is used for data forwarding across the public network, which is necessary for the communication between users. An EUI-64 address has the same function as a global unicast address. The difference is that only the network bits need to be specified for the EUI-64 address and the host bits are transformed from the media access control (MAC) addresses of the interface while a complete 128-bit address needs to be specified for the global unicast address.
- The link-local address is used in neighbor discovery (ND), and in the communication between nodes on the local link in the stateless address auto-configuration. The packets using the link-local address as the source or destination address are not forwarded to other links.

  The link-local address can be automatically generated or manually configured. It is recommended to automatically generate a link-local address because the link-local address is used to implement communication requirements of protocol and is not directly related to the communication between users.

  NOTE

  In stateless address auto configuration, a host uses the prefix information and local interface ID obtained from the router advertisement (RA) received to automatically generate an IPv6 address. Instead, the host does not use stateful (DHCPv6) address configuration.

The MA5600T/MA5603T supports IPv6 address configuration on the virtual local area network (VLAN) interface, METH interface, and loopback interface. This topic uses the VLAN interface as an example.

Procedure

Step 1 Enable IPv6 packet forwarding capability.

Enabling the IPv6 function of the device and the interface is a prerequisite for configuring IPv6 features. To enable a device to forward IPv6 packets, you must enable the IPv6 capability in both the global config mode and the interface mode.

By default, the IPv6 function on the device and interface is disabled.

1. In global config mode, run the **ipv6** command to enable the IPv6 packet forwarding capability.
2. Run the **interface vlanif** command to enter the VLANIF mode.
3. In VLANIF mode, run the **ipv6 enable** command to enable the IPv6 function on the interface.

   NOTE

   Before configuring other IPv6 features on an interface, enable the IPv6 function in interface mode.

Step 2 Configure an IPv6 global unicast address for an interface.

In VLANIF mode, run the **ipv6 address** or **ipv6 address eui-64** command to configure an IPv6 global unicast address on the interface.

The EUI-64 address and the global unicast address can be configured simultaneously or alternatively. However, the IPv6 addresses configured for one interface cannot be in the same network segment.

Step 3 Configure an IPv6 link-Local address for an interface.

In VLAN interface mode, run the following commands based on the requirements:

- Run the **ipv6 address auto link-local** command to automatically generate a local-link address of an interface.

  After this command is executed, the deletion of the global unicast address does not affect local link communication. If the device only needs to communicate with another device that is directly connected to the device, using the link-local address saves global unicast address resources.

- Run the **ipv6 address link-local** command to manually configure a link-local address of an interface. The prefix of the IPv6 address configured by running this command must be FE80::/10.

  After this command is executed, the original link-local address is replaced by the new link-local address. If possible, do not change the link-local address.

In addition to configuring a link-local address through the preceding two commands, you can also configure a global unicast IPv6 address for automatically generating a link-local address.

Step 4 Query the address configuration information about an IPv6 interface.

- Run the **display ipv6 interface** command to query the IPv6 interface information.
- Run the **display ipv6 statistics** command to query the IPv6 packet statistics.

----End

Example

To create VLAN 10, set the IPv6 address of VLAN interface 10 to 2000::1/64, and configure automatic configuration of a link-local address, run the following commands:

```
huawei(config)#vlan 10
huawei(config)#ipv6
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ipv6 enable
huawei(config-if-vlanif10)#ipv6 address 2000::1 64
huawei(config-if-vlanif10)#ipv6 address auto link-local
```

3.1.2 Configuring an IPv6 Address Selection Policy Table

If multiple IPv6 addresses are configured on an interface of the device, the IPv6 address selection policy table can be used to select source and destination addresses for packets.

Context

IPv6 addresses can be classified into different types based on different applications.

- Link local addresses and global unicast addresses based on the effective range of the IPv6 addresses
- Temporary addresses and public addresses based on security levels
- Home addresses and care-of addresses based on the application in the mobile IPv6 field

- Physical interface addresses and logical interface addresses based on the interface attributes

The preceding IPv6 addresses can be configured on the same interface of the router. In this case, the device must select a source address or a destination addresses from multiple addresses on the interface. If the device supports the IPv4/IPv6 dual-stack, it also must select IPv4 addresses or IPv6 addresses for communication. For example, if a domain name maps both an IPv4 address and an IPv6 address, the system must select an address to respond to the domain name server (DNS) request of the client.

An IPv6 address selection policy table solves the preceding problems. It defines a group of address selection rules. The source and destination addresses of packets can be specified or planned based on these rules. This table, similar to a routing table, can be queried by using the longest matching rule. The address is selected based on the source and destination addresses.

- The *label* parameter can be used to determine the result of source address selection. The address whose *label* value is the same as the *label* value of the destination address is selected preferably as the source address.
- The destination address is selected based on both the *label* and the *precedence* parameters. If *label* values of the candidate addresses are the same, the address whose *precedence* value is largest is selected preferably as the destination address.

Procedure

Step 1 In global config mode, run the **ipv6 address-policy** command to configure the source and destination address selection policy.

By default, only default address selection policy entries are contained. These entries are prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

A maximum of 50 address selection policy entries are supported by the system.

Step 2 Query the IPv6 address selection policy.

Run the **display ipv6 address-policy** command to query the IPv6 address selection policy.

----End

3.1.3 Configuring IPv6 Neighbor Discovery

IPv6 neighbor discovery (ND) is a packet transmission process to identify the relationship between neighboring nodes. The Neighbor Discovery Protocol (NDP) is similar to the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) router Discovery messages, and ICMP redirect messages, and introduces neighbor reachability detection.

Prerequisite

The IPv6 address must be configured. For details, see **Configuring an IPv6 Address for an Interface**.

Context

Most of the ND configurations are implemented based on the interfaces. The MA5600T/MA5603T supports ND configurations on VLAN Layer 3 interfaces.

NOTE

For details about ND, see Neighbor Discovery in the *Feature Description*.

Procedure

- Configure the static neighbors.

  By configuring a static neighbor, you can obtain the mapping of the IPv6 address and media access control (MAC) address of the neighbor. The statically configured neighbor entries will overwrite the dynamically learned neighbor entries and they will not age.

  1. In global config mode, run the **interface vlanif** command to enter the VLAN interface mode.
  2. In VLAN interface mode, run the **ipv6 neighbor** command to configure a static IPv6 neighbor.

- Configure the parameters of router advertisement (RA) messages.

  The device periodically sends router advertisement messages containing information such as address prefixes, maximum number of hops, neighbor hold time, and keep-alive time. The IPv6 node on the local link receives RA messages and updates information such as the IPv6 prefix list and other information from the RA messages.

  1. In global config mode, run the **interface vlanif** command to enter the VLAN interface mode.
  2. Run the **undo ipv6 nd ra halt** command to enable RA message advertising.
     - When a device is connected to an IPv6 node, the RA message advertising function needs to be enabled so that the device periodically sends RA messages to the IPv6 node.
     - When a device is not connected to an IPv6 node, the RA message advertising function does not need to be enabled. By default, this function is disabled.

     By default, RA message advertising is disabled on the devices.
  3. (Optional) Configure parameters carried in an RA message.

     Select the following desired operations:

     - Run the **ipv6 nd ra** command to configure the interval for advertising RA messages.

       By default, the maximum interval is 600 seconds and the minimum interval is 200 seconds. The maximum interval cannot be shorter than the minimum interval. When the maximum interval is less than 9 seconds, the minimum interval is set to the same value as the maximum interval.
     - Run the **ipv6 nd ra router-lifetime** command to configure the lifetime of RA messages.

       By default, the lifetime is 1800 seconds. The lifetime of the messages advertised by the device must be longer than or equal to the interval for the device to advertise messages.
     - Run the **ipv6 nd ra prefix** command to configure the address prefixes to be advertised in RA messages.

       By default, RA messages contain only the address prefixes specified through the **ipv6 address** command. Run this command when the device advertises only the specified prefixes.
     - Configure the default router priority and route information in RA messages.

       RA messages that carry the default router priority and route information can be transmitted over the local link. In this manner, a proper device can be selected to forward messages of a host.

    - Run the **ipv6 nd ra preference** command to configure the default router priority in RA messages.
    - Run the **ipv6 nd ra route-information** command to configure the route information in RA messages.
  - Set the flag bit for stateful auto configuration in RA messages.
    - Run the **ipv6 nd autoconfig managed-address-flag** command to set the flag bit for stateful auto configuration addresses in RA messages.

      If this flag is set, hosts use the stateful protocol for address auto-configuration in addition to any automatically configured addresses using stateless address auto-configuration.
    - Run the **ipv6 nd autoconfig other-flag** command to set the flag bit for other stateful configurations.

      When this flag is set, hosts use the stateful protocol for auto-configuration of other (non-address) information.
  - Run the **ipv6 nd ns retrans-timer** command to configure the interval for detecting neighbor reachability in RA messages, that is, re-transmission timer of neighbor solicitation (NS) messages.

    Frequently sending NS packets helps to determine whether the neighbor is reachable but affects the device performance. Therefore, you are recommended to set the interval for sending NS messages to a greater value. The default interval, 1000 milliseconds, is recommended.
  - Run the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time in RA messages.

    NUD is short for neighbor unreachability detection. A smaller neighbor reachable time set on a device indicates that the device can probe the neighbor reachability more quickly but more network bandwidth and CPU resources are occupied. Therefore, you are recommended to set the interval for sending NS messages to a greater value. The default interval, 30000 milliseconds, is recommended.
  - Configure the maximum number of hops for the route device.

    Run the **quit** command to quit the VLANIF mode. In global config mode, run the **ipv6 nd hop-limit** command to configure the maximum number of hops for the route device, that is, the maximum number of hops for the IPv6 unicast packets initiated by the host. The value for the maximum number of hops for the route device is the same as that for the maximum number of hops in the RA messages. The default value is 64.

- Configure duplicate address detection (DAD).

  DAD is used to check whether an IPv6 address is available. When a node is configured with an IPv6 address, it immediately sends an NS message to check whether this address is used by other neighboring nodes.

  1. In the global config mode, run the **interface vlanif** command to enter the VLANIF mode.
  2. Run the **ipv6 nd dad attempts** to configure the number of DAD attempts, that is, number of attempts to send neighbor request messages. The default value is 1.
  3. Run the **ipv6 nd ns retrans-timer** command to configure the interval of DAD, that is, re-transmission timer of neighbor solicitation (NS) messages. The default interval, 1000 milliseconds, is recommended.

- Query the IPv6 neighbor information.
  - Run the **display ipv6 neighbors** command to query the IPv6 neighbor information.
  - Run the **display ipv6 interface** command to query the IPv6 interface information.
  - Run the **display ipv6 prefix** command to query the IPv6 prefixes in the RA message sent from the IPv6 interface.
  - Run the **display ipv6 route-information** command to query the route information in the RA message sent from the IPv6 interface.

----End

Example

To configure the function of automatically generating a link-local unicast address on VLAN interface 10, set the local unicast address of site EUI-64 and the prefix to be advertised by the RA message to 3000::/64, set the valid lifetime and preferred lifetime of the prefix to 1000s, and enable RA message advertising, run the following commands:

```
huawei(config)#vlan 10
huawei(config)#ipv6
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ipv6 enable
huawei(config-if-vlanif10)#ipv6 address auto link-local
huawei(config-if-vlanif10)#ipv6 address 3000::/64 eui-64
huawei(config-if-vlanif10)#ipv6 nd ra prefix 3000::/64 1000 1000
huawei(config-if-vlanif10)#undo ipv6 nd ra halt
```

3.1.4 Configuring PMTU

By setting the path maximum transmission unit (PMTU), you can select a proper maximum transmission unit (MTU) for packet transmission. In this manner, packets do not have to be fragmented during transmission and loads on intermediate devices are reduced. In addition, network resources are used more efficiently and the network throughput reaches the optimal value.

Context

Dynamic PMTU values can be set on a device by default, ensuring the smallest value of MTU values is used on all interfaces along the source to the destination nodes. Configuring a static PMTU sets the maximum length of a packet that can be sent from the source end to the destination end. This prevents attacks initiated by sending jumbo packets. When both static PMTUs and dynamic PMTUs are configured, only static PMTUs take effect. In other words, the priority of static PMTUs is higher than the priority of the dynamic PMTUs.

Procedure

Step 1 Configure a static PMTU.

In the global mode, run the **ipv6 pathmtu** command to configure a static PMTU for the path destined for the specified IPv6 address. By default, the PMTU of the path destined for an IPv6 address is 1500 bytes.

Generally, the static PMTU value is smaller than or equal to the MTU value of all interfaces on the same path. If the static PMTU value is larger than the MTU value of the interfaces, the system segments packets according to the MTU value. If the static PMTU value is manually configured based on the smallest MTU value of the patch that packets are transmitted, the packets will be transmitted at a higher rate.

Step 2 Configure the aging time of dynamic PMTU entries.

Run the **ipv6 pathmtu age** command to configure the aging time of dynamic PMTU entries. By default, the aging time of dynamic PMTU entries is 10 minutes.

The **ipv6 pathmtu age** command is used to change the life cycle of the dynamic PMTU entries in the buffer. It is invalid for static PMTU entries, because static PMTU entries do not age.

Step 3 Query the PMTU information.

- Run the **display ipv6 pathmtu** command to query the PMTU information.
- Run the **display ipv6 interface** command to query the MTU value of the IPv6 interface.

----End

3.1.5 Configuring TCP6

By setting TCP6 packets, you can improve the performance of the network.

Procedure

- Configure TCP6 timers.

  Configuring two TCP6 timers in global config mode helps to control the TCP6 connection time. It is recommended that you configure the TCP6 timers by following the instructions of technical support engineers.

  1. Run the **tcp ipv6 timer syn-timeout** command to configure the Transfer Control Protocol (TCP) SYN-WAIT timer.

     By default, the SYN-WAIT timer is 75s.

  2. Run the **tcp ipv6 timer fin-timeout** command to configure the TCP FIN-WAIT timer.

     By default, the FIN-WAIT timer is 675s.

- Configure the size of the TCP6 sliding window.

  In the global config mode, run the **tcp ipv6 window** command to configure the size of the TCP6 sliding window, that is, the sizes of the receiving buffer and transmitting buffer in the socket.

  By default, the size of the TCP6 sliding window is 8 KB.

- Query the TCP6 configuration information.
  - Run the **display tcp ipv6 statistics** command to query the TCP6 statistics.
  - Run the **display tcp ipv6 status** command to query the TCP6 connection status.
  - Run the **display ipv6 socket** command to query the socket information.

----End

3.2 Configuring the IP-aware Bridge

After the IP-aware bridge function is enabled on the MA5600T/MA5603T, in the upstream direction of the MA5600T/MA5603T, user data can be forwarded to different upper-layer devices according to the destination IP address and the configured static route. With the IP-aware bridge function enabled, the MA5600T/MA5603T features the ARP proxy function: shielding the MAC address of the network-side device for the user side and shielding the user-side MAC address for the network side.

Context

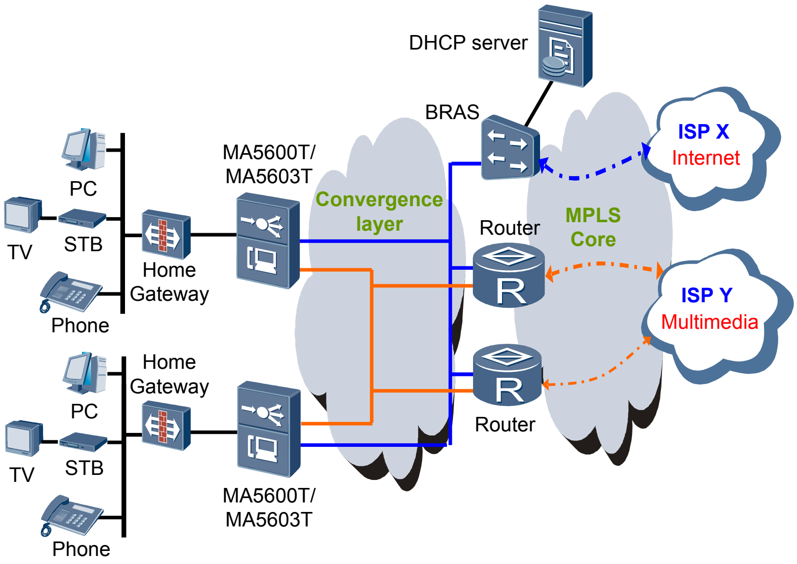
- The IP address of the VLAN L3 interface need not be configured if the IP-aware bridge function is enabled for the VLAN. Therefore, only the IP address of the convergence layer interface needs to be planned. The data, however, can still be forwarded at L3 on the MA5600T/MA5603T. This solves the problem of insufficient IP addresses.
- After the IP-aware bridge function is enabled, the system automatically performs ARP processing. The ARP proxy function between users, however, is not supported. To enable the communication between isolated ports in the same broadcast domain or ports in different broadcast domains, run the **arp proxy** command to enable the ARP proxy function of the user side.
- The VLAN L3 interface has no IP address after the IP-aware bridge function is enabled for the VLAN. Therefore, the dynamic routing protocol cannot be used and only static routes can be configured. If the static route of the configured IP-aware bridge feature conflicts with the static route of a normal L3 interface, the first configured static route takes effect. It is recommended that you ensure no conflict between configurations and delete the original configuration if necessary.

Networking

Figure 3-1 shows an example network of the IP-aware bridge function.

Internet access service are in ISP X and Unicast services such as VOD are in ISP Y. To differentiate the Internet access service and VOD service, private routes need to be planned. The data of these two services are forwarded through different routes.

Figure 3-1 Example network of the IP-aware bridge function



Procedure

Step 1 (Optional) Create a VPN instance.

When it need to allocate different VRF (Virtual Route Forward) for different ISP, run the command **ip vpn-instance** to create a VPN instance or into the VPN instance mode. You can configure related parameters in this mode. If not configured, all the IP forwarding will be in the default VRF.

Step 2 Create a VLAN and add the upstream port to the VLAN.

Run the **vlan** command to create a VLAN, and then run the **port vlan** command to add an upstream port to the VLAN. The VLAN can be a smart VLAN, MUX VLAN, or standard VLAN. The attribute of the VLAN must be common.

Step 3 Enable the IP-aware bridge function.

Run the **ip-aware vlan** command to enable the IP-aware bridge function of the VLAN. The VLAN here corresponds to the SVLAN of the service port.

NOTE

In the VLAN whose IP-aware bridge function is enabled, the VLAN L3 interface cannot be configured; in the VLAN whose L3 interface is created, the IP-aware bridge cannot be enabled.

Step 4 Configure the obtaining mode of the source IP address in the ARP request.

In the VLAN whose IP-aware bridge function is enabled, the MAC address of the gateway needs to be obtained from the ARP request.

The obtaining mode of the source IP address in the ARP request can be configured through the **ip-aware vlan** *vlanid* **source-ip-mode** { **client-ip** | **virtual-ip** } command.

- **client-ip**: Configures the obtaining mode of the source IP address as client IP address. When the ARP request is sent, the user IP address is used as the source IP address of the ARP request. In certain networks, the upper-layer device responds only when the source IP address in the sent ARP request is the user IP address. In this case, select this mode according to the requirement of the upper-layer device. This is the default mode of the system.
- **virtual-ip**: Configures the obtaining mode of the source IP address as virtual IP address. The server for the Internet access service and that for the VOD service may be in different network segments, but the sent ARP request must reach gateways of the two servers. Therefore, the virtual IP address and the gateway address must be configured in the same network segment so that the ARP request can be transmitted correctly. You can run the **ip-aware vlan virtual-ip** command to configure the virtual IP address of the VLAN as the source IP address of the ARP request.

  NOTE

  Each VLAN whose IP-aware bridge function is enabled can be configured with multiple virtual IP addresses (because multiple next hops may be in different network segments). Each VLAN supports up to eight virtual IP addresses.

Step 5 (Optional)configure the period for sending the VLAN ARP request.

You can also run the **ip-aware vlan arp-send-period** command to configure the period for sending the VLAN ARP request. By default, the ARP request is sent every 180s. You can adjust the period according to actual requirements.

Step 6 Configure the IP-aware bridge static route.

Because the VLAN L3 interface has no IP address, the dynamic routing protocol cannot be used and only static routes can be configured. Configure routing entries for access nodes so that packets can be forwarded to identified IP address according to the destination IP address and routing information of the packet.

Run the **ip-aware route-static** command to configure the IP-aware bridge function. You can configure a default route for the Internet access service (next hop 0.0.0.0) and another private route for the VOD service.

Step 7 Create a service port.

Run the **service-port** command to create a service port to establish the service channel between the user and the MA5600T/MA5603T.

----End

Example

Assumption:

- Gateway address to ISP X (Internet access service): 10.1.1.2.
- Gateway address to ISP Y (multimedia service): 10.1.1.250, server network segment: 195.6.7.0/24.

Configure the IP-aware bridge function for VLAN 100 with the default VRF, configure the upstream port to 0/19/0, and configure the obtaining mode of the source IP address in the ARP request as client IP address. The user adopts the GPON access mode through port 0/18/0, adopts the default value for the period of sending the ARP request (no need to configure), and creates a private route to ISP X and ISP Y. To perform these operations, do as follows:

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/19 0
huawei(config)#ip-aware vlan 100
huawei(config)#ip-aware vlan 100 source-ip-mode client-ip
huawei(config)#ip-aware route-static 0.0.0.0 0 vlan 100 10.1.1.2
huawei(config)#ip-aware route-static 195.6.7.0 24 vlan 100 10.1.1.250
huawei(config)#service-port 100 vlan 100 gpon 0/18/0 gemport 128 multi-service user-
vlan 100 rx-cttr 6 tx-cttr 6
```

3.3 Configuring DHCP

The MA5600T/MA5603T can implement DHCP relay and DHCP proxy on a network. Configuring DHCP relay is applicable to the scenario where users dynamically obtain IP addresses from the DHCP server through DHCP. In DHCP proxy, the MA5600T/MA5603T proxy can implement certain functions of the DHCP server.

Context

The MA5600T/MA5603T can work in the Layer 2 DHCP relay mode or Layer 3 DHCP relay mode to forward the DHCP packets exchanged between the user and the DHCP server. By default, the MA5600T/MA5603T works in the Layer 2 DHCP relay mode. In this mode, the MA5600T/MA5603T transparently transmits the DHCP packets initiated by the user and configurations are not required. If the MA5600T/MA5603T works in the Layer 3 mode, the DHCP server must support DHCP relay and you must perform corresponding configurations on the DHCP server. The Layer 3 DHCP relay mode can be classified into three working modes:

- DHCP standard mode

  In this mode, the MA5600T/MA5603T identifies the VLAN to which the user belongs and binds different VLANs to the corresponding DHCP server groups.

  Configure the DHCP standard mode as follows: Configure the working mode of the DHCP relay. Configure the DHCP server group. Bind VLANs to DHCP server groups.

- DHCP option 60 mode

The MA5600T/MA5603T differentiates the DHCP packets transmitted from the user terminal according to the DHCP option 60 field in the packets, and binds different DHCP option 60 domains to the corresponding DHCP server groups.

Configure the DHCP option 60 mode as follows: Configure the working mode of the DHCP relay. Configure the DHCP server group. Create DHCP option 60 field. Bind DHCP option 60 domains to DHCP server groups.

- MAC address segment mode

  The MA5600T/MA5603T differentiates users according to the MAC address segment of the user terminals, and binds different MAC address segments to the corresponding DHCP server group.

  Configure the MAC address segment mode as follows: Configure the working mode of the DHCP relay. Configure the DHCP server group. Define the MAC address segment. Bind MAC address segments to DHCP server groups.

If the MA5600T/MA5603T works in the Layer 3 DHCP relay mode, the MA5600T/MA5603T supports the DHCP proxy function in addition to the DHCP relay function. That is, the MA5600T/MA5603T functions as a proxy to implement certain functions of the DHCP server. A DHCP proxy can implement the functions of server ID proxy and lease-time proxy.

- The server ID proxy is a function for modifying option 54 field in DHCP packets so that the IP address of the DHCP server is unavailable to the client. This prevents the attacks initiated by the DHCP client to the DHCP server.
- With the lease-time proxy, the information related to the lease-time in the DHCP packets is modified by MA5600T/MA5603T so that the client can obtain a lease time. This lease time is shorter than the lease time directly allocated by the DHCP server. This facilitates the lease-time management.

NOTE

The MA5600T/MA5603T supports the DHCP option 82 to ensure the security of the DHCP function. For the configuration related to the DHCP option 82 feature, see **2.7.2 Configuring Anti-Theft and Roaming of User Accounts Through DHCP**.

3.3.1 Configuration Difference Between DHCPv4 and DHCPv6

Dynamic Host Control Protocol version 6 (DHCPv6) is a DHCP protocol in IPv6. This section describes differences regarding to functions and commands between DHCPv4 and DHCPv6. It is recommended that you know well about how to configure DHCPv4 services and then configure DHCPv6 services based on their differences.

Context

The configuration differences between DHCPv4 and DHCPv6 are as follows:

- When DHCPv6 works in Layer 3 forwarding mode, you can run the **dhcpv6 mode { layer-2 | layer-3 }** command to configure the DHCPv6 working mode to Layer 2 forwarding or Layer 3 forwarding. DHCPv4 supports the standard, media access control (MAC) address segment, and DHCP option 60 modes. You can run the **dhcp mode { layer-2 | layer-3 { mac-range | option60 | standard } }** command to configure the DHCPv4 working mode.
- DHCPv6 does not support DHCP proxy.
- For commands, DHCPv4 uses keyword **dhcp** while DHCPv6 uses keyword **dhcpv6**. For example, the **dhcp-server** command is used to configure DHCPv4 server groups while the **dhcpv6-server** command is used to configure DHCPv6 server groups.

For the differences of other configuration commands, see "DHCPv6 Configuration" in the *Command Line Reference*. Some commands need to be executed in diagnose mode. For details about these commands, see "Diagnose Command".

3.3.2 Configuring the Standard DHCP Mode

This topic is applicable to the scenario for specifying the corresponding Dynamic Host Configuration Protocol (DHCP) server groups for different users of a virtual local area network (VLAN) that is used when the service ports are created.

Prerequisites

A VLAN must be created. For details, see **2.6 Configuring a VLAN**.

Procedure

Step 1 Configure the DHCP forwarding mode.

Choose one from the following two methods for configuring the DHCP forwarding mode:

- In the global config mode, run the **dhcp mode layer-3 standard** command to configure the DHCP relay mode to standard Layer 3 DHCP relay mode (Layer-3, standard). If keyword **vlan** is selected and *vlanid* is entered, this configuration takes effect to only this VLAN.
- Perform the following configuration in the VLAN service profile:
  1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
  2. Run the **dhcp mode layer-3 standard** command to configure the DHCP mode.
  3. Run the **commit** command to make the configuration parameters of the profile take effect. The configuration of the VLAN service profile takes effect only after you run this command.
  4. Run the **quit** command to quit the VLAN service profile mode.
  5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in **1.1**.

Step 2 Configure the DHCP server group.

1. In the global config mode, run the **dhcp-server** command to create a DHCP server group.
   - *igroup-number*: Indicates the number of the DHCP server group. It identifies a server group. You can run the **display dhcp-server all-group** command to query the DHCP server groups that are already configured and select a DHCP server group number that is not used by the system.
   - *ip-addr*: Indicates the Internet Protocol (IP) address of the DHCP server in the DHCP server group. A maximum of four IP addresses can be entered.

   ⚠ **CAUTION**

   The IP address of the DHCP server configured here must be the same as the IP address of the DHCP server in the network side.

2. (Optional) Run the **dhcp server mode** command to configure the working mode of the DHCP server.

The DHCP servers in the DHCP server group can work in the load balancing mode or active/standby mode. By default, they work in the load balancing mode.

Step 3 Bind the VLAN to the DHCP server.

1. In the global config mode, run the **interface vlanif** command to create a VLAN Layer 3 interface.

   The VLAN ID must be the same as the ID of the VLAN described in the prerequisite.

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

   After the configuration is completed, this IP address is used as the source IP address for forwarding the IP packets in the VLAN at Layer 3.

⚠ **CAUTION**

- If only a Layer 2 device exists between the MA5600T/MA5603T and the DHCP server, the IP address of the VLAN Layer 3 interface should be in the same subnet as the IP address of the DHCP server.
- If the upper-layer device of the MA5600T/MA5603T is a Layer 3 device, the IP address of the VLAN Layer 3 interface and the IP address of the DHCP server can be in different subnets; however, a route must exist between the VLAN Layer 3 interface and the DHCP server. For details, see **3.4 Configuring the Route**.

3. In the VLAN interface mode, run the **dhcp-server** command to bind the DHCP server to the VLAN.

   This command requires parameter **group-number**, the value of which is the number of the created DHCP server group.

Step 4 (Optional) Configure the DHCP proxy.

To hide the IP address of the DHCP server (preventing attacks to the DHCP server from the client), or to configure the MA5600T/MA5603T to allocate a shorter lease time to the client (compared with the lease time directly allocated by the DHCP server), configure the DHCP proxy.

1. Enable the DHCP proxy function. When DHCP proxy is enabled, the DHCP server ID proxy and the lease-time proxy are enabled.

   Choose one from the following two methods for enabling DHCP proxy:

   - In the global config mode, run the **dhcp proxy enable** command to enable DHCP proxy.
   - Perform the configuration in the VLAN service profile.

     a. Run the **vlan service-profile** command to enter the VLAN service profile mode.

     b. Run the **dhcp proxy enable** command to enable DHCP proxy.

     c. Run the **commit** command to make the configuration parameters of the profile take effect. The configuration of the VLAN service profile takes effect only after you run this command.

     d. Run the **quit** command to quit the VLAN service profile mode.

     e. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in **4.1.a**.

2. In the global config mode, run the **dhcp proxy lease-time** command to configure the global proxy lease time.

   The proxy lease time configured here should be shorter than the lease time allocated by the DHCP server.

----End

Example

Assume that server group 1 contains two DHCP servers working in active/standby mode, with the maximum response time of 20s, the maximum count of response timeout of 10, the IP address of the primary server 10.1.1.9 and the IP address of the secondary server 10.1.1.10. To bind server group 1 to users in VLAN 2 (with the IP address of the Layer 3 interface 10.1.1.101/24), run the following commands:

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp server mode backup 20 10
huawei(config)#dhcp-server 1 ip 10.1.1.9 10.1.1.10
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.1.101 24
huawei(config-if-vlanif2)#dhcp-server 1
```

3.3.3 Configuring the DHCP Option60 Mode

This topic is applicable to the scenario for specifying the corresponding DHCP servers for different option60 domain users.

Prerequisites

- A VLAN must be created. For details, see **2.6 Configuring a VLAN**.
- Before the configuration, confirm the option60 domain name of the user terminal.

Context

When multiple services such as video multicast and IP telephone services are provisioned on the MA5600T/MA5603T, the services are provided by different service providers. The service providers may use different relay IP addresses of the same DHCP server or different DHCP servers to allocate IP addresses to users. Therefore, configure the users to apply for IP addresses from the DHCP server in the DHCP option60 mode.

In the DHCP option60 mode, the DHCP server group is selected according to the character string (namely domain name) in the option60 of DHCP packets. The option60 domain name and the DHCP server group to which the domain name is bound need to be configured beforehand. In this mode, users are actually differentiated according to the domain information in the packet, and different service types in the same VLAN can also be differentiated.

Procedure

Step 1 Configure the DHCP forwarding mode.

Choose one from the following two methods for configuring the DHCP forwarding mode:

- In the global config mode, run the **dhcp mode layer-3 option60** command to configure the DHCP relay mode to Layer 3 option60 mode (layer-3, option60). If keyword **vlan** is selected and *vlanid* is entered, this configuration takes effect to only this VLAN.

- Perform the configuration in the VLAN service profile:
  1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
  2. Run the **dhcp mode layer-3 option60** command to configure the DHCP mode.
  3. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after execution of this command.
  4. Run the **quit** command to quit the VLAN service profile mode.
  5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in **1.1**.

Step 2 Configure the DHCP server group.

1. In the global config mode, run the **dhcp-server** command to create a DHCP server group.
   - *igroup-number*: Indicates the number of the DHCP server group. It identifies a server group. You can run the **display dhcp-server all-group** command to query the DHCP server groups that are already configured and select a DHCP server group number that is not used by the system.
   - *ip-addr*: Indicates the IP address of the DHCP server in the DHCP server group. Up to four IP addresses can be entered.

   CAUTION

   The IP address of the DHCP server configured here must be the same as the IP address of the DHCP server in the network side.
2. (Optional) Run the **dhcp server mode** command to configure the working mode of the DHCP server.

   The DHCP servers in the DHCP server group can work in the load balancing mode or active/standby mode. By default, they work in the load balancing mode.

Step 3 Create a DHCP option60 domain.

In the global config mode, run the **dhcp domain** command to create a DHCP domain, and then enter the DHCP domain mode. The option60 domain name should be configured according to the type of the terminal connected to the device. For the DHCP client installed with the Windows 98/2000/XP/NT series of OSs, the domain name must be **msft**.

Step 4 Bind the DHCP option60 domain to the DHCP server group.

In the option60 domain mode, run the **dhcp-server** command to bind the DHCP domain to the DHCP server group. After the configuration is completed, the DHCP clients belonging to the DHCP correspond to the DHCP server group.

Step 5 Configure the IP address of the gateway corresponding to the DHCP domain.

1. In the global config mode, run the **interface vlanif** command to create a VLAN Layer 3 interface.

   The VLAN ID must be the same as the ID of the VLAN described in the prerequisite.
2. In the VLANIF mode, run the **ip address** command to configure the IP address of the VLAN Layer 3 interface.

   After the configuration is completed, this IP address is used as the source IP address for forwarding the IP packets in the VLAN at L3.

CAUTION

- If only a Layer 2 2 device exists between the MA5600T/MA5603T and the DHCP server, the IP address of the VLAN Layer 3 interface should be in the same subnet as the IP address of the DHCP server.
- If the upper-layer device of the MA5600T/MA5603T is a Layer 3 device, the IP address of the VLAN Layer 3 interface and the IP address of the DHCP server can be in different subnets; however, a route must exist between the VLAN Layer 3 interface and the DHCP server. For details, see **3.4 Configuring the Route**.

3. In the VLANIF mode, run the **dhcp domain gateway** command to configure the IP address of the gateway corresponding to the DHCP domain.

   The IP address of the gateway must be a configured IP address of the VLAN interface. Under the same VLAN interface, different option60 domains can be configured with different gateways. Therefore, different DHCP servers can be selected according to the domain information in the packet.

Step 6 (Optional) Configure the DHCP proxy.

To hide the IP address of the DHCP server (preventing attacks to the DHCP server from the client), or to configure the MA5600T/MA5603T to allocate a shorter lease time to the client (compared with the lease time directly allocated by the DHCP server), configure the DHCP proxy.

1. Enable the DHCP proxy function. When DHCP proxy is enabled, the DHCP server ID proxy and the lease-time proxy are enabled.

   Choose one from the following two methods for enabling DHCP proxy:

   - In the global config mode, run the **dhcp proxy enable** command to enable DHCP proxy.
   - In VLAN service profile configuration mode, to configure the VLAN forwarding policy, do as follows:
     a. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
     b. Run the **dhcp proxy enable** command to enable DHCP proxy.
     c. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after execution of this command.
     d. Run the **quit** command to quit the VLAN service profile mode.
     e. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in **6.1.a**.
2. In the global config mode, run the **dhcp proxy lease-time** command to configure the global proxy lease time.

   The proxy lease time configured here should be shorter than the lease time allocated by the DHCP server.

----End

Example

Assume that server group 2 contains two DHCP servers working in the load balancing mode, with the IP address of the primary server 10.10.10.10 and the IP address of the secondary server

10.10.10.11. To bind server group 2 to users whose option60 domain name is **msft** in VLAN 2 (with the IP address of the Layer 3 interface 10.1.2.1/24), do as follows:

```
huawei(config)#dhcp mode layer-3 Option60
huawei(config)#dhcp-server 2 ip 10.10.10.10 10.10.10.11
huawei(config)#dhcp domain msft
huawei(config-dhcp-domain-msft)#dhcp-server 2
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.2.1 24
huawei(config-if-vlanif2)#dhcp domain msft gateway 10.1.2.1
```

3.3.4 Configuring the DHCP MAC Address Segment Mode

This topic is applicable to the scenario for specifying the corresponding DHCP servers for users in different MAC address segments.

Prerequisites

A VLAN must be created. For details, see **2.6 Configuring a VLAN**.

Context

In the networking, devices of various manufacturers may exist in the network. The devices of each manufacturer have a fixed MAC address segment. In this case, the IP address can be obtained from the DHCP server through DHCP relay in the MAC address segment mode.

The MA5600T/MA5603T can select the DHCP server based on the MAC address segment. After the configuration is completed, clients in this MAC address segment obtain IP addresses from the corresponding DHCP server.

Procedure

Step 1 Configure the DHCP forwarding mode.

Choose one from the following two methods for configuring the DHCP forwarding mode:

- In the global config mode, run the **dhcp mode layer-3 mac-range** command to configure the DHCP relay mode to Layer 3 MAC address segment mode (layer-3, mac-range). If keyword **vlan** is selected and *vlanid* is entered, this configuration takes effect to only this VLAN.
- Perform the following configuration in the VLAN service profile:
  1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
  2. Run the **dhcp mode layer-3 mac-range** command to configure the DHCP mode.
  3. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after execution of this command.
  4. Run the **quit** command to quit the VLAN service profile mode.
  5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in **1.1**.

Step 2 Configure the DHCP server group.

1. In the global config mode, run the **dhcp-server** command to create a DHCP server group.

- *igroup-number*: Indicates the number of the DHCP server group. It identifies a server group. You can run the **display dhcp-server all-group** command to query the DHCP server groups that are already configured and select a DHCP server group number that is not used by the system.
- *ip-addr*: Indicates the IP address of the DHCP server in the DHCP server group. Up to four IP addresses can be entered.

CAUTION

The IP address of the DHCP server configured here must be the same as the IP address of the DHCP server in the network side.

2. (Optional) Run the **dhcp server mode** command to configure the working mode of the DHCP server.

   The DHCP servers in the DHCP server group can work in the load balancing mode or active/standby mode. By default, they work in the load balancing mode.

Step 3 Define the MAC address segment.

1. In the global config mode, run the **dhcp mac-range** to create a MAC address segment, and then enter the MAC address segment mode.

   range-name indicates the name of the MAC address segment. It functions as a comment and has no other special meanings.
2. In the MAC address segment mode, run the **mac-range mac-address-start to mac-address-end** command to configure the MAC address range.

Step 4 Bind the DHCP server group to the MAC address segment.

In the MAC address segment mode, run the **dhcp-server** command to bind a DHCP server group to the MAC address segment.

Step 5 Configure the IP address of the gateway corresponding to the MAC address segment.

1. In the global config mode, run the **interface vlanif** command to create a VLAN Layer 3 interface.

   The VLAN ID must be the same as the ID of the VLAN described in the prerequisite.
2. In the VLANIF mode, run the **ip address** command to configure the IP address of the VLAN Layer 3 interface.

   After the configuration is completed, this IP address is used as the source IP address for forwarding the IP packets in the VLAN at L3.

CAUTION

- If only a Layer 2 2 device exists between the MA5600T/MA5603T and the DHCP server, the IP address of the VLAN Layer 3 interface should be in the same subnet as the IP address of the DHCP server.
- If the upper-layer device of the MA5600T/MA5603T is a Layer 3 device, the IP address of the VLAN Layer 3 interface and the IP address of the DHCP server can be in different subnets; however, a route must exist between the VLAN Layer 3 interface and the DHCP server. For details, see **3.4 Configuring the Route**.

3. In the VLANIF mode, run the **dhcp mac-range gateway** command to configure the IP address of the gateway corresponding to the DHCP domain.

   The IP address of the gateway must be a configured IP address of the VLAN interface. Under the same VLAN interface, different MAC address segments can be configured with different gateways. Therefore, different DHCP servers can be selected according to the MAC address segment information in the packet.

Step 6 (Optional) Configure the DHCP proxy.

To hide the IP address of the DHCP server (preventing attacks to the DHCP server from the client), or to configure the MA5600T/MA5603T to allocate a shorter lease time to the client (compared with the lease time directly allocated by the DHCP server), configure the DHCP proxy.

1. Enable the DHCP proxy function. When DHCP proxy is enabled, the DHCP server ID proxy and the lease-time proxy are enabled.

   Choose one from the following two methods for enabling DHCP proxy:

   - In the global config mode, run the **dhcp proxy enable** command to enable DHCP proxy.
   - Perform the configuration in the VLAN service profile:

     a. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.

     b. Run the **dhcp proxy enable** command to enable DHCP proxy.

     c. Run the **commit** command to make the profile configuration take effect. The configuration of the VLAN service profile takes effect only after execution of this command.

     d. Run the **quit** command to quit the VLAN service profile mode.

     e. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in **6.1.a**.

2. In the global config mode, run the **dhcp proxy lease-time** command to configure the global proxy lease time.

   The proxy lease time configured here should be shorter than the lease time allocated by the DHCP server.

----End

Example

Assume that server group 2 contains two DHCP servers working in the load balancing mode, with the IP address of the primary server 10.10.10.10 and the IP address of the secondary server 10.10.10.11. To bind server group 2 to certain users (whose MAC address is in the range from 0000-0000-0001 to 0000-0000-0100) in VLAN 2, do as follows:

```
huawei(config)#dhcp mode layer-3 mac-range
huawei(config)#dhcp-server 2 ip 10.10.10.10 10.10.10.11
huawei(config)#dhcp mac-range huawei
huawei(config-mac-range-huawei)#mac-range 0000-0000-0001 to 0000-0000-0100
huawei(config-mac-range-huawei)#dhcp-server 2
huawei(config)#quit
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.2.1 24
huawei(config-if-vlanif2)#dhcp mac-range huawei gateway 10.1.2.1
```

3.4 Configuring the Route

This topic describes the routing policy supported by the MA5600T/MA5603T and how to configure the routing protocol.

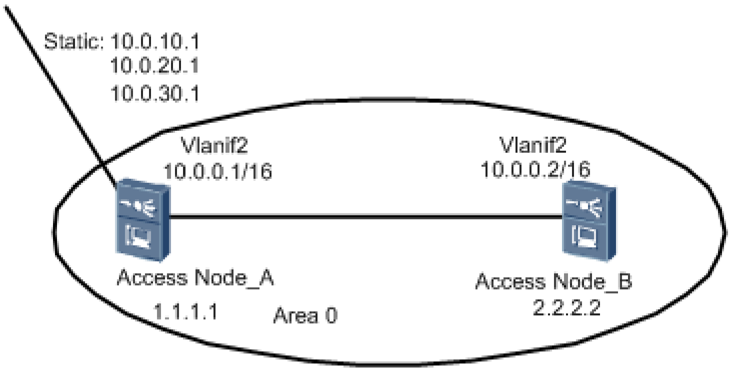
3.4.1 Configuration Example of the Routing Policy

This topic provides an example for configuring a routing policy for imported routes.

Service Requirements

- Consider two MA5600T/MA5603Ts with routing function enabled, namely MA5600T/MA5603T_A and MA5600T/MA5603T_B. Both of them are running the OSPF routing protocol, and within area 0.
- MA5600T/MA5603T_A imports static routes, and MA5600T/MA5603T_B is configured with the routing filtering policy.

Figure 3-2 Example network for configuring the routing policy



Procedure

Step 1 Configuring MA5600T/MA5603T_A.

1. Configure the IP address of the Layer 3 interface on MA5600T/MA5603T_A.

```
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.0.0.1 24
huawei(config-if-vlanif2)#quit
```

2. Enable OSPF on MA5600T/MA5603T_A and specify the area ID to which the interface belongs.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.0.0.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

3. Configure the OSPF router ID on MA5600T/MA5603T_A.

```
huawei(config)#router id 1.1.1.1
```

4. Configure three static routes.

```
huawei(config)#ip route-static 20.0.0.1 32 vlanif 2 10.0.0.1
huawei(config)#ip route-static 30.0.0.1 32 vlanif 2 10.0.0.1
huawei(config)#ip route-static 40.0.0.1 32 vlanif 2 10.0.0.1
```

5. Import static routes into the OSPF routing table to improve its capability of obtaining routes.

```
huawei(config)#ospf
hawei(config-ospf-1)#import-route static
hawei(config-ospf-1)#quit
```

6. Save the data.

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

Step 2 Configuring MA5600T/MA5603T_B.

1. Configure the IP address of the Layer 3 interface on MA5600T/MA5603T_B.

```
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.0.0.2 24
huawei(config-if-vlanif2)#quit
```

2. Configure the ACL.

```
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule deny source 30.0.0.0 255.255.255.0
huawei(config-acl-basic-2000)#rule permit source any
huawei(config-acl-basic-2000)#quit
```

3. Enable OSPF on MA5600T/MA5603T_B and specify the area id to which the interface belongs.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.0.0.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Configure the OSPF router ID of MA5600T/MA5603T_B.

```
huawei(config)#router id 2.2.2.2
```

5. Filter imported routes.

```
huawei(config)#ospf
uawei(config-ospf-1)#filter-policy 2000 import
huawei(config-ospf-1)#quit
```

6. Save the data.

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

----End

Result

1. MA5600T/MA5603T_A and MA5600T/MA5603T_B run OSPF successfully, and they can communicate well with each other.
2. After a filter is configured on MA5600T/MA5603T_B, parts of the three imported static routes are available while part of them is screened on MA5600T/MA5603T_B. That is, routes from segments 20.0.0.0 and 40.0.0.0 are available, while the route from segment 30.0.0.0 is screened.

Configuration File

Configuration on MA5600T/MA5603T_A.

```
vlan 2 smart
port vlan 2 0/19 0
```

```
interface vlanif 2
ip address 10.0.0.1 24
quit
ospf
area 0
network 10.0.0.0 0.0.0.255
quit
quit
router id 1.1.1.1
ip route-static 20.0.0.1 32 vlanif 2 10.0.0.1
ip route-static 30.0.0.1 32 vlanif 2 10.0.0.1
ip route-static 40.0.0.1 32 vlanif 2 10.0.0.1
ospf
import-route static
quit
save
```

Configuration on MA5600T/MA5603T_B.

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 10.0.0.1 24
acl 2000
rule deny source 30.0.0.0 255.255.255.0
rule permit source any
quit
ospf
area 0
network 10.0.0.0 0.0.0.255
quit
quit
router id 2.2.2.2
ospf
filter-policy 2000 import
quit
save
```

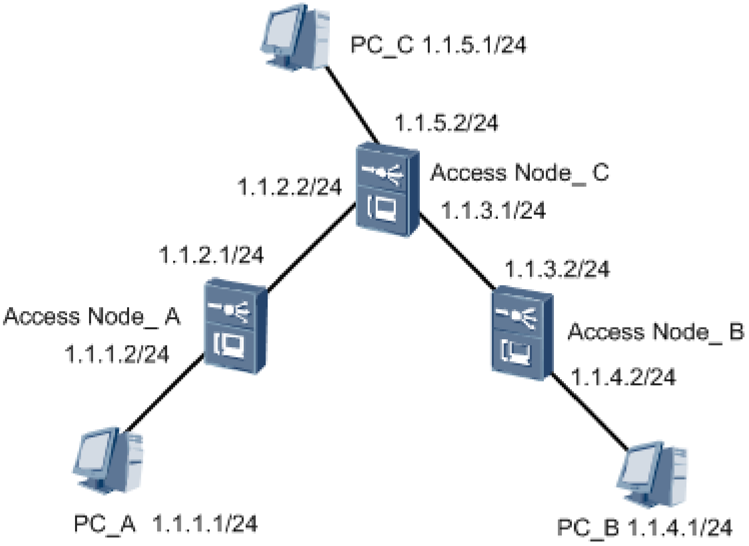
3.4.2 Configuration Example of the IPv4 Static Route

This topic describes how to manually add the IPv4 static route to implement the interconnection between MA5600T/MA5603T.

Service Requirements

In this example network, MA5600T/MA5603T_A, MA5600T/MA5603T_B, and MA5600T/MA5603T_C have the routing function. It is expected that after the configuration, any two PCs can communicate with each other.

Figure 3-3 Example network for configuring the IPv4 static route



Procedure

Step 1 Configure the IP address of the Layer 3 interface.

The configurations for the three MA5600T/MA5603T devices are the same. The configuration of the MA5600T/MA5603T is considered as an example.

```
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 1.1.1.2 24
huawei(config-if-vlanif2)#ip address 1.1.2.1 24 sub
huawei(config-if-vlanif2)#quit
```

Step 2 Configure IPv4 static routes.

1. Configure an IPv4 static route for MA5600T/MA5603T_A.

```
huawei(config)#ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
huawei(config)#ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

2. Configure an IPv4 static route for MA5600T/MA5603T_B.

```
huawei(config)#ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
huawei(config)#ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

3. Configure IPv4 static routes for MA5600T/MA5603T_C.

```
huawei(config)#ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
huawei(config)#ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

Step 3 Configure the host gateways.

1. Configure the default gateway of Host A to 1.1.1.2.
2. Configure the default gateway of Host B to 1.1.4.2.
3. Configure the default gateway of Host C to 1.1.5.2.

Step 4 Save the data.

```
huawei#save
```

----End

Result

After the configuration, an interconnection can be set up between all the hosts and between all the MA5600T/MA5603T devices. Run the **ping** and **tracert** command to check the network connectivity.

Run the **display ip routing-table** command to query the IPv4 routing table which contains the static routing information that is configured.

Configuration File

Configuration example of MA5600T/MA5603T_A.

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 1.1.1.2 24
ip address 1.1.2.1 24 sub
quit
ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

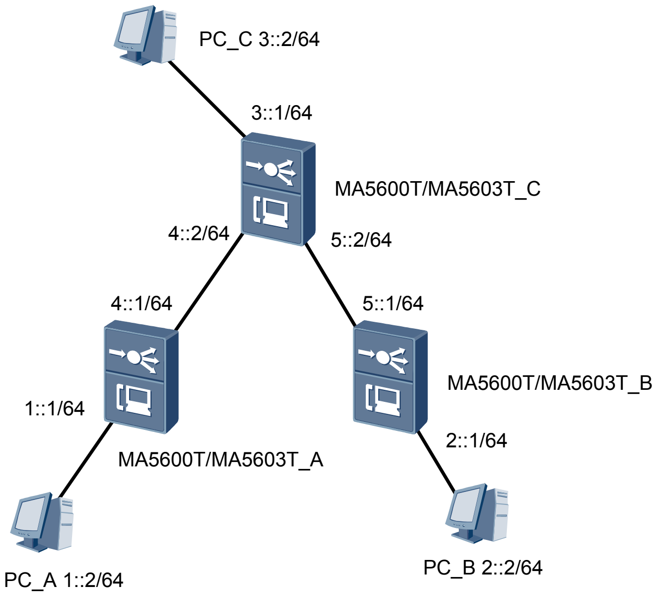
3.4.3 Configuration Example of the IPv6 Static Route

This topic describes how to manually add the IPv6 static route to implement the interconnection between MA5600T/MA5603T.

Service Requirements

In this example network, MA5600T/MA5603T_A, MA5600T/MA5603T_B, and MA5600T/MA5603T_C have the routing function. It is expected that after the configuration, any two PCs can communicate with each other.

Figure 3-4 Example network for configuring the IPv6 static route



Procedure

Step 1 Configure the IPv6 address of the Layer 3 interface.

The configurations for the three MA5600T/MA5603T devices are the same. The configuration of the MA5600T/MA5603T is considered as an example.

```
huawei(config)#ipv6
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ipv6 enable
huawei(config-if-vlanif2)#ipv6 address 1::1 64
huawei(config-if-vlanif2)#quit
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/19 1
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ipv6 enable
huawei(config-if-vlanif3)#ipv6 address 4::1 64
huawei(config-if-vlanif3)#quit
```

Step 2 Configure IPv6 static routes.

1. Configure IPv6 static route for MA5600T/MA5603T_A.
   ```
   huawei(config)#ipv6 route-static :: 0 4::2
   ```
2. Configure IPv6 static route for MA5600T/MA5603T_B.
   ```
   huawei(config)#ipv6 route-static :: 0 5::2
   ```
3. Configure IPv6 static routes for MA5600T/MA5603T_C.
   ```
   huawei(config)#ipv6 route-static 1::1 64 4::1
   huawei(config)#ipv6 route-static 2::1 64 5::1
   ```

Step 3 Configure the host gateways.

1. Configure the default gateway of Host A to 1::1.
2. Configure the default gateway of Host B to 2::1.
3. Configure the default gateway of Host C to 3::1.

Step 4 Save the data.

```
huawei#save
```

----End

Result

After the configuration, an interconnection can be set up between all the hosts and between all the MA5600T/MA5603T devices. Run the **ping ipv6** and **tracert ipv6** commands to query the network connectivity.

Run the **display ipv6 routing-table** command to query the IPv6 routing table which contains the static routing information that is configured.

Configuration File

Configuration example of MA5600T/MA5603T_A.

```
ipv6
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ipv6 enable
ipv6 address 1::1/64
```

```
quit
vlan 3 smart
port vlan 3 0/19 1
interface vlanif 3
ipv6 enable
ipv6 address 4::1/64
quit
ipv6 route-static :: 0 4::2
```

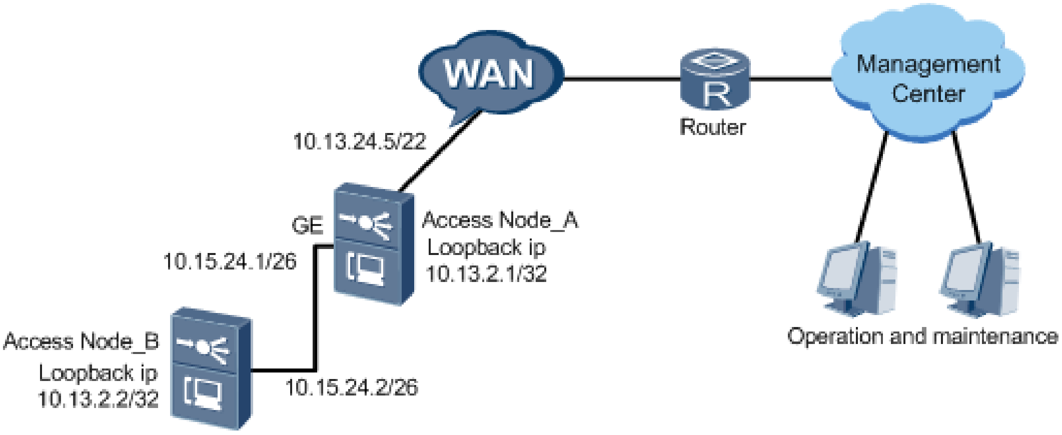
3.4.4 Configuration Example of RIP

This topic provides an example for configuring RIP on the MA5600T/MA5603T.

Service Requirements

- MA5600T/MA5603T_A is subtended with MA5600T/MA5603T_B through port 0/19/1, and uses port 0/19/0 to transmit services in the upstream. Besides, it connects to the management center network through the WAN.
- RIP is enabled on MA5600T/MA5603T_A and MA5600T/MA5603T_B so that the administrator can access MA5600T/MA5603T_A and MA5600T/MA5603T_B through the RIP route. Then, you can operate and maintain MA5600T/MA5603T_A and MA5600T/MA5603T_B.

Figure 3-5 Example network for configuring RIP



Data Plan

Table 3-2 provides the data plan for configuring RIP.

Table 3-2 Data plan for configuring RIP

Item	Data
MA5600T/ MA5603T_A	Upstream port: 0/19/0 Administration VLAN: smart VLAN 100 IP address of the Layer 3 interface in the administration VLAN: 10.13.24.5/22 Loopback interface address: 10.13.2.1/32

Item	Data
	RIP version: V2 RIP route filtering policy: filtering routes based on the IP address prefix list "abc". Only the routes with the IP addresses 10.13.2.1 and 10.13.2.2 can be advertised through the Layer 3 interface of VLAN 100.
	Subtending port: 0/19/0 Subtending administration VLAN: smart VLAN 10 IP address of the Layer 3 interface in the subtending administration VLAN: 10.15.24.1/26
MA5600T/ MA5603T_B	Subtending port: 0/19/1 Administration VLAN: smart VLAN 10 IP address of the Layer 3 interface in the administration VLAN: 10.15.24.2/26 Loopback interface address: 10.13.2.2/32
	RIP version: V2 RIP route filtering policy: filtering routes based on the IP address prefix list "abc". Only the route with the IP address 10.13.2.2 can be advertised through the Layer 3 interface of VLAN 10.

Procedure

- Configure MA5600T/MA5603T_A.

1. Configure the RIP-supported Layer 3 interface.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/19 0
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.13.24.5 22
huawei(config-if-vlanif100)#quit
huawei(config)#interface loopBack 0
huawei(config-if-loopback0)#ip address 10.13.2.1 32
huawei(config-if-loopback0)#quit
```

2. Enable RIP.

```
huawei(config)#rip 1
huawei(config-rip-1)#network 10.13.24.0
huawei(config-rip-1)#network 10.13.2.0
huawei(config-rip-1)#version 2
huawei(config-rip-1)#quit
```

3. Configure the route filtering policy.

```
huawei(config)#ip ip-prefix abc permit 10.13.2.1 32
huawei(config)#ip ip-prefix abc permit 10.13.2.2 32
huawei(config)#rip 1
huawei(config-rip-1)#filter-policy ip-prefix abc export vlanif 100
huawei(config-rip-1)#quit
```

4. Configure the subtending port.

```
huawei(config)#vlan 10 smart
huawei(config)#port vlan 10 0/19 1
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#network-role 1 cascade
huawei(config-if-giu-0/19)#quit
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.15.24.1 26
huawei(config-if-vlanif10)#quit
```

5. Enable RIP on the subtending port.

```
huawei(config)#rip 1
huawei(config-rip-1)#network 10.15.24.0
huawei(config-rip-1)#quit
```

6. Save the data.

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

- Configure MA5600T/MA5603T_B.

1. Configure the RIP-supported Layer 3 interface.

```
huawei(config)#vlan 10 smart
huawei(config)#port vlan 10 0/19 0
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.15.24.2 26
huawei(config-if-vlanif10)#quit
huawei(config)#interface loopBack 0
huawei(config-if-loopback0)#ip address 10.13.2.2 32
huawei(config-if-loopback0)#quit
```

2. Enable RIP.

```
huawei(config)#rip 1
huawei(config-rip-1)#network 10.15.24.0
huawei(config-rip-1)#network 10.13.2.0
huawei(config-rip-1)#version 2
huawei(config-rip-1)#quit
```

3. Configure the route filtering policy.

```
huawei(config)#ip ip-prefix abc permit 10.13.2.2 32
huawei(config)#rip 1
huawei(config-rip-1)#filter-policy ip-prefix abc export vlanif 10
huawei(config-rip-1)#quit
```

4. Save the data.

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

----End

Result

The maintenance terminal of the administration center can access MA5600T/MA5603T_A and MA5600T/MA5603T_B, and operate and maintain the two devices.

Configuration File

Configuration on MA5600T/MA5603T_A

```
vlan 100 smart
port vlan 100 0/19 0
interface vlanif 100
ip address 10.13.24.5 22
quit
interface loopBack 0
ip address 10.13.2.1 32
quit
rip 1
network 10.13.24.0
network 10.13.2.0
version 2
quit
ip ip-prefix abc permit 10.13.2.1 32
ip ip-prefix abc permit 10.13.2.2 32
rip 1
filter-policy ip-prefix abc export vlanif 100
```

```
quit
vlan 10 smart
port vlan 10 0/19 1
interface giu 0/19
network-role 1 cascade
quit
interface vlanif 10
ip address 10.15.24.1 26
quit
rip 1
network 10.15.24.0
quit
save
```

Configuration on MA5600T/MA5603T_B

```
vlan 10 smart
port vlan 10 0/19 0
interface vlanif 10
ip address 10.15.24.2 26
quit
interface loopBack 0
ip address 10.13.2.2 32
quit
rip 1
network 10.15.24.0
network 10.13.2.0
version 2
quit
ip ip-prefix abc permit 10.13.2.2 32
rip 1
filter-policy ip-prefix abc export vlanif 10
quit
save
```

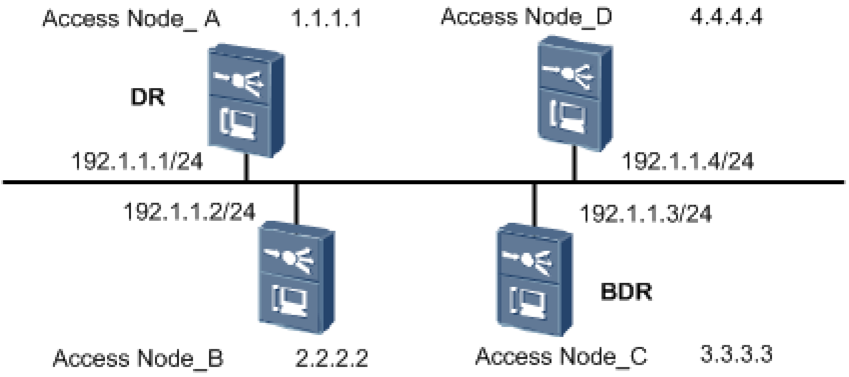
3.4.5 Configuration Example of OSPF

This topic provides an example for configuring OSPF on the MA5600T/MA5603T.

Service Requirements

- OSPF is enabled on the four MA5600T/MA5603Ts.
- MA5600T/MA5603T_A is configured with the highest designated router (DR) priority, MA5600T/MA5603T_C is configured with the second highest DR priority, and MA5600T/MA5603T_A implements the broadcast of network link status for the DR.

Figure 3-6 Example network for configuring OSPF



Data Plan

Table 3-3 provides the data plan for configuring OSPF.

Table 3-3 Data plan for configuring OSPF

Item	Data	Remarks
MA5600T/MA5603T_A	IP address of the Layer 3 interface: 192.1.1.1/24	-
	Priority: 100	-
	VLAN ID: 2	-
	Router ID: 1.1.1.1	-
MA5600T/MA5603T_B	IP address of the Layer 3 interface: 192.1.1.2/24	-
	Priority: 80	-
	VLAN ID: 2	-
	Router ID: 2.2.2.2	-
MA5600T/MA5603T_C	IP address of the Layer 3 interface: 192.1.1.3/24	-
	Priority: 90	-
	VLAN ID: 2	-
	Router ID: 3.3.3.3	-
MA5600T/MA5603T_D	IP address of the Layer 3 interface: 192.1.1.4/24	-
	Priority: not configured	Default: 1
	VLAN ID: 2	-
	Router ID: 4.4.4.4	-

Context

- The native VLAN of each interface of the MA5600T/MA5603T must be configured to ensure a normal communication.
- The OSPF area IDs of the MA5600T/MA5603T devices must be consistent.

Procedure

Step 1 Configure MA5600T/MA5603T_A.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.1 24
huawei(config-if-vlanif2)#quit
```

2. Configure the OSPF Router ID.

```
huawei(config)#router id 1.1.1.1
```

3. Enable OSPF.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 1.1.1.1 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Configure the OSPF priority.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 100
huawei(config-if-vlanif2)#quit
```

5. Save the data.

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

Step 2 Configure MA5600T/MA5603T_B.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 2 mux
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.2 24
huawei(config-if-vlanif2)#quit
```

2. Configure the OSPF Router ID.

```
huawei(config)#router id 2.2.2.2
```

3. Enable OSPF.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 2.2.2.2 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Configure the OSPF priority.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 80
huawei(config-if-vlanif2)#quit
```

5. Save the data.

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

Step 3 Configure MA5600T/MA5603T_C.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 2 mux
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.3 24
huawei(config-if-vlanif2)#quit
```

2. Configure the OSPF Router ID.

```
huawei(config)#router id 3.3.3.3
```

3. Enable OSPF.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Configure the OSPF priority.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 90
huawei(config-if-vlanif2)#quit
```

5. Save the data.

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

Step 4 Configure MA5600T/MA5603T_D.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 2 mux
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.4 24
huawei(config-if-vlanif2)#quit
```

2. Configure the OSPF Router ID.

```
huawei(config)#router id 4.4.4.4
```

3. Enable OSPF.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 4.4.4.4 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Save the data.

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

----End

Result

Run the **display ip routing-table** command and you can find the learnt route table. Hosts can communicate with each other.

Configuration File

Configuration on each MA5600T/MA5603T is similar. Take MA5600T/MA5603T_A for example.

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 192.1.1.1 24
quit
router id 1.1.1.1
ospf
area 0
network 192.1.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
quit
quit
interface vlanif 2
ospf dr-priority 100
quit
save
```

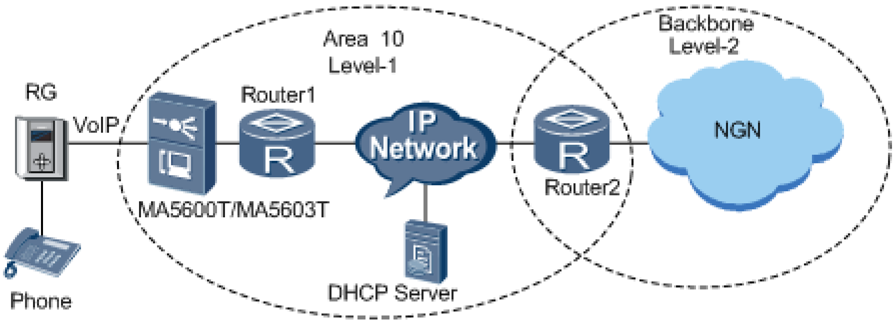
3.4.6 Configuration Example of IS-IS

This operation enables the corresponding device configured data to run the IS-IS protocol on the MA5600T. Only the MA5600T support the IS-IS protocol and the MA5603T do not support the IS-IS protocol.

Service Requirements

- The MA5600T forwards the access VoIP service through the Layer 3 interface to the NGN network.
- The MA5600T obtains the routes of the NGN networking through the IS-IS protocol. The area ID of the Level-2 router differs from the area ID of the Level-1-2 router to which the Level-2 router connects.

Figure 3-7 Example network for configuring IS-IS



Data Plan

Table 3-4 provides the data plan for configuring IS-IS.

Table 3-4 Data plan for configuring IS-IS

Item	Data
MA5600T	IS-IS process ID: 1
	NET (Network entity title): 10.0000.0000.0001.00, where: ● Area ID: 10 ● System ID: 0000.0000.0001 ● Level: Level-1 ● Host name: MA5600T
	IS-IS interface: ● Port number: 0/20/0 ● VLAN ID: 20 ● IP address: 5.5.5.5/16
Router1	IS-IS process ID: 1

Item	Data
	NET (Network entity title): 10.0000.0000.0002.00, where: ● Area ID: 10 ● System ID: 0000.0000.0002 ● Level: Level-1 ● Host name: Router1
	IS-IS interface: 1/0/0 IP address: 8.8.8.8/16
Router2	IS-IS process ID: 1
	NET (Network entity title): 10.0000.0000.0005.00, where: ● Area ID: 10 ● System ID: 0000.0000.0005 ● Level: Level-1-2 ● Host name: Router2
	IS-IS interface: 1/0/0 IP address: 9.9.9.9/16

Procedure

- Configure IS-IS on the MA5600T.

  1. Configure the Layer 3 interface.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/20 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 5.5.5.5 16
huawei(config-if-vlanif20)#quit
```

  2. Start the IS-IS process.

```
huawei(config)#isis 1
huawei(config-isis-1)#
```

  3. Configure the NET.

```
huawei(config-isis-1)#network-entity 10.0000.0000.0001.00
```

  4. Configure the router level.

```
huawei(config-isis-1)#is-level level-1
```

  5. Configure the local host name.

```
huawei(config-isis-1)#is-name MA5600T
huawei(config-isis-1)#quit
```

  6. Enable the IS-IS function on an interface.

```
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#isis enable 1
```

- Configure IS-IS on Router1.

  The process of configuring IS-IS on Router1 is similar to that of configuring IS-IS on the MA5600T. The details are not provided in this chapter.

- Configure IS-IS on Router2.

  The process of configuring IS-IS on Router2 is similar to that of configuring IS-IS on the MA5600T. The details are not provided in this chapter.

----End

Result

- Run the **display isis lsdb** command and you can query the IS-IS LSDB.
- Run the **display isis route** command and you can query the IS-IS route. The routing table of the Level-1 router should have a default route, and the next hop should be the Level-1-2 router. The Level-2 router should have the routes to all the Level-1 routers and the Level-2 routers.

Configuration File

```
vlan 20 standard
port vlan 20 0/20 0
interface vlanif 20
ip address 5.5.5.5 16
quit
isis 1
network-entity 10.0000.0000.0001.00
is-level level-1
is-name MA5600T
quit
interface vlanif 20
isis enable 1
```

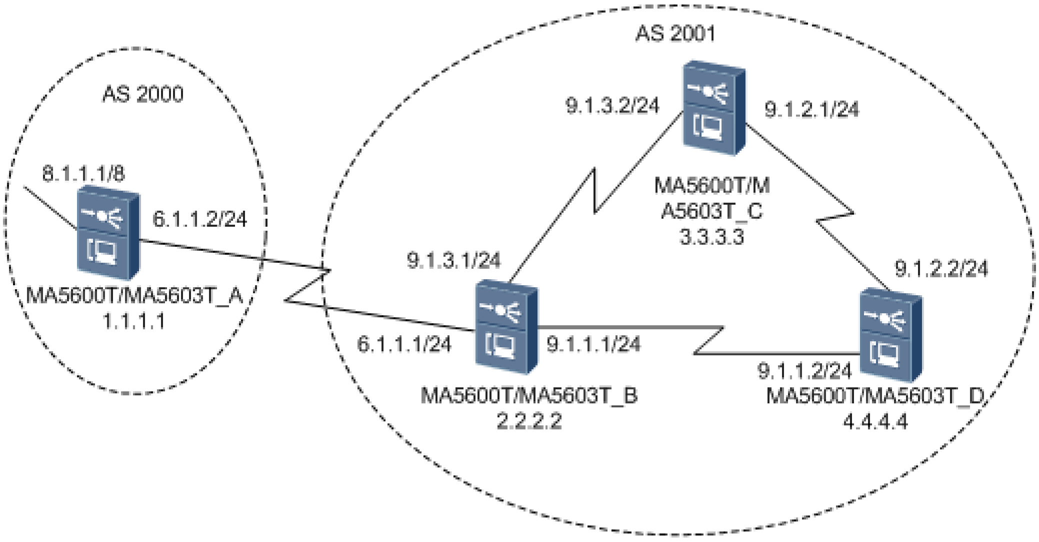
3.4.7 Configuration Example of BGP

This topic provides an example for configuring the BGP on the device.

Service Requirements

In this example network, an EBGP connection is set up between MA5600T_A and MA5600T_B, and an IBGP connection is set up among MA5600T_B, MA5600T_C, and MA5600T_D.

Figure 3-8 Example network for configuring the BGP



Data Plan

Table 3-5 provides the data plan for configuring the BGP.

Table 3-5 Data plan for configuring the BGP

Item	Data	Remarks
MA5600T_A	IP address of VLAN interface 6: 6.1.1.2/24	It is used for the EBGP connection to AS 2001.
	IP address of VLAN interface 2: 8.1.1.1/8	-
	Router ID: 1.1.1.1	-
	AS number: 2000	-
MA5600T_B	IP address of VLAN interface 6: 6.1.1.1/24	It is used for the EBGP connection to AS 2000.
	IP address of VLAN interface 3: 9.1.3.1/24	It is used for the IBGP connection to the MA5600T_C.
	IP address of VLAN interface 4: 9.1.1.1/24	It is used for the IBGP connection to the MA5600T_D.
	Router ID: 2.2.2.2	-
	AS number: 2001	-
MA5600T_C	IP address of VLAN interface 3: 9.1.3.2/24	It is used for the IBGP connection to the MA5600T_B.
	IP address of VLAN interface 5: 9.1.2.1/24	It is used for the IBGP connection to the MA5600T_D.
	Router ID: 3.3.3.3	-
	AS number: 2001	-
MA5600T_D	IP address of VLAN interface 5: 9.1.2.2/24	It is used for the IBGP connection to the MA5600T_C.
	IP address of VLAN interface 4: 9.1.1.2/24	It is used for the IBGP connection to the MA5600T_B.

Item	Data	Remarks
	Router ID: 4.4.4.4	-
	AS number: 2001	-

Procedure

Step 1 Configure MA5600T_A.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 6 smart
huawei(config)#port vlan 6 0/19 0
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ip address 6.1.1.2 24
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 8.1.1.1 8
huawei(config-if-vlanif2)#quit
```

2. Enable the BGP function.

```
huawei(config)#bgp 2000
huawei(config-bgp)#router-id 1.1.1.1
huawei(config-bgp)#peer 6.1.1.1 as-number 2001
huawei(config-bgp)#network 8.0.0.0 8
huawei(config-bgp)#quit
```

3. Save the data.

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

Step 2 Configure MA5600T_B.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 6 smart
huawei(config)#port vlan 6 0/19 0
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ip address 6.1.1.1 24
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/19 0
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 9.1.3.1 24
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 4 smart
huawei(config)#port vlan 4 0/19 0
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 9.1.1.1 24
huawei(config-if-vlanif4)#quit
```

2. Enable the BGP function.

```
huawei(config)#bgp 2001
huawei(config-bgp)#router-id 2.2.2.2
huawei(config-bgp)#peer 6.1.1.2 as-number 2000
huawei(config-bgp)#peer 9.1.3.2 as-number 2001
huawei(config-bgp)#peer 9.1.1.2 as-number 2001
huawei(config-bgp)#import-route direct
huawei(config-bgp)#quit
```

3. Save the data.

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

Step 3 Configure MA5600T_C.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/19 0
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 9.1.3.2 24
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 5 smart
huawei(config)#port vlan 5 0/19 0
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ip address 9.1.2.1 24
huawei(config-if-vlanif5)#quit
```

2. Enable the BGP function.

```
huawei(config)#bgp 2001
huawei(config-bgp)#router-id 3.3.3.3
huawei(config-bgp)#peer 9.1.3.1 as-number 2001
huawei(config-bgp)#peer 9.1.2.2 as-number 2001
huawei(config-bgp)#quit
```

3. Save the data.

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

Step 4 Configure MA5600T_D.

1. Configure the IP address of the Layer 3 interface.

```
huawei(config)#vlan 4 smart
huawei(config)#port vlan 4 0/19 0
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 9.1.1.2 24
huawei(config-if-vlanif4)#quit
huawei(config)#vlan 5 smart
huawei(config)#port vlan 5 0/19 0
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ip address 9.1.2.2 24
huawei(config-if-vlanif5)#quit
```

2. Enable the BGP function.

```
huawei(config)#bgp 2001
huawei(config-bgp)#router-id 4.4.4.4
huawei(config-bgp)#peer 9.1.2.1 as-number 2001
huawei(config-bgp)#peer 9.1.1.1 as-number 2001
huawei(config-bgp)#quit
```

3. Save the data.

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

----End

Result

- Run the **display bgp peer** command, and you can see that:
  - The EBGP connection is set up between MA5600T_A and MA5600T_B.
  - The IBGP connections are set up among MA5600T_B, MA5600T_C, and MA5600T_D.
  - The route with the destination subnet 8.0.0.0/8 exists on MA5600T_C and MA5600T_D, and the next hop of the route is the interface address of MA5600T_A
- Run the **ping** command on MA5600T_C and MA5600T_D to ping the Layer 3 interface (8.1.1.1/8) on MA5600T_A. The **ping** command is executed successfully.

Configuration File

Configuration on each MA5600T is similar. Take MA5600T_A for example.

```
vlan 6 smart
port vlan 6 0/19 0
interface vlanif 6
ip address 6.1.1.2 24
quit
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 8.1.1.1 8
quit
bgp 2000
router-id 1.1.1.1
peer 6.1.1.1 as-number 2001
network 8.0.0.0 8
quit
```

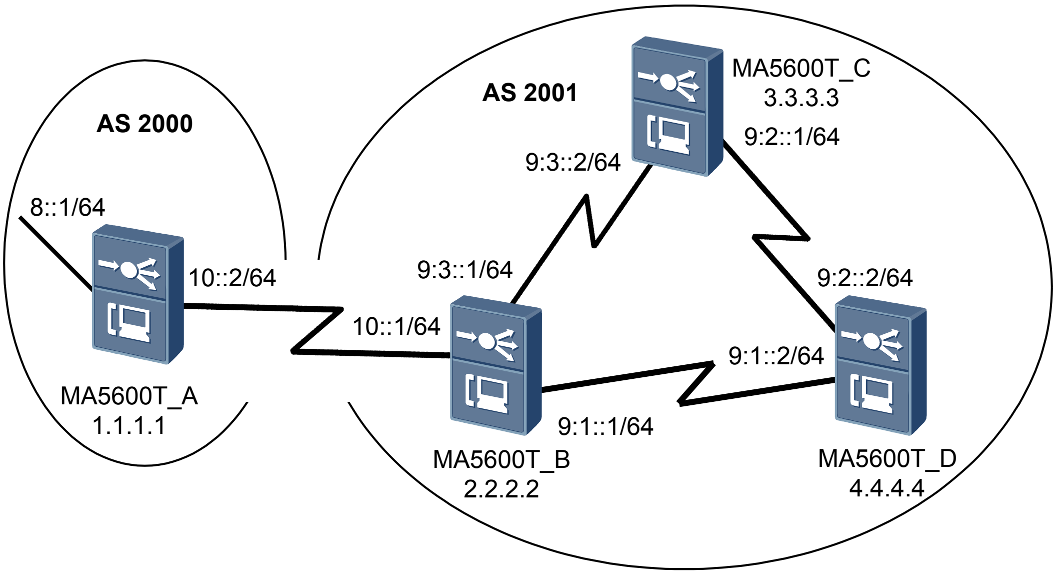
3.4.8 Configuration Example of BGP4+

This topic provides an example for configuring the BGP4+ on the device.

Service Requirements

In this example network, an external Border Gateway Protocol (EBGP) connection is set up between MA5600T_A and MA5600T_B, and an Interior Border Gateway Protocol (IBGP) connection is set up among MA5600T_B, MA5600T_C, and MA5600T_D.

Figure 3-9 Example network for configuring the BGP4+



Data Plan

Table 3-6 provides the data plan for configuring the BGP4+.

Table 3-6 Data plan for configuring the BGP4+

Item	Data	Remarks
MA5600T_A	IPv6 address of virtual local area network (VLAN) interface 6: 10::2/64	It is used for the EBGP connection to Autonomous System (AS) 2001.
	IPv6 address of VLAN interface 2: 8::1/64	-
	Router ID: 1.1.1.1	-
	AS number: 2000	-
MA5600T_B	IPv6 address of VLAN interface 6: 10::1/64	It is used for the EBGP connection to AS 2000.
	IPv6 address of VLAN interface 3: 9:3::1/64	It is used for the IBGP connection to the MA5600T_C.
	IPv6 address of VLAN interface 4: 9:1::1/64	It is used for the IBGP connection to the MA5600T_D.
	Router ID: 2.2.2.2	-
	AS number: 2001	-
MA5600T_C	IPv6 address of VLAN interface 3: 9:3::2/64	It is used for the IBGP connection to the MA5600T_B.
	IPv6 address of VLAN interface 4: 9:2::1/64	It is used for the IBGP connection to the MA5600T_D.
	Router ID: 3.3.3.3	-
	AS number: 2001	-
MA5600T_D	IPv6 address of VLAN interface 5: 9:2::2/64	It is used for the IBGP connection to the MA5600T_C.
	IPv6 address of VLAN interface 4: 9:1::2/64	It is used for the IBGP connection to the MA5600T_B.
	Router ID: 4.4.4.4	-
	AS number: 2001	-

Procedure

Step 1 Configure MA5600T_A.

1. Configure the IPv6 address of the Layer 3 interface.

```
huawei(config)#ipv6
huawei(config)#vlan 6 smart
huawei(config)#port vlan 6 0/19 0
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ipv6 enable
huawei(config-if-vlanif6)#ipv6 address 10::2 64
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/19 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ipv6 enable
huawei(config-if-vlanif2)#ipv6 address 8::1/64
huawei(config-if-vlanif2)#quit
```

2. Enable the Border Gateway Protocol (BGP) function and configure the EBGP neighbor between MA5600T_B.

```
huawei(config)#bgp 2000
huawei(config-bgp)#router-id 1.1.1.1
huawei(config-bgp)#peer 10::1 as-number 2001
huawei(config-bgp)#ipv6-family unicast
huawei(config-bgp-af-ipv6)#peer 10::1 enable
huawei(config-bgp-af-ipv6)#network 10:: 64
huawei(config-bgp-af-ipv6)#network 8:: 64
huawei(config-bgp-af-ipv6)#quit
huawei(config-bgp)#quit
```

3. Save the data.

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

Step 2 Configure MA5600T_B.

1. Configure the IPv6 address of the Layer 3 interface.

```
huawei(config)#ipv6
huawei(config)#vlan 6 smart
huawei(config)#port vlan 6 0/19 0
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ipv6 enable
huawei(config-if-vlanif6)#ipv6 address 10::1 64
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/19 0
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ipv6 enable
huawei(config-if-vlanif3)#ipv6 address 9:3::1 64
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 4 smart
huawei(config)#port vlan 4 0/19 0
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ipv6 enable
huawei(config-if-vlanif4)#ipv6 address 9:1::1 64
huawei(config-if-vlanif4)#quit
```

2. Enable the BGP function. Configure the EBGP neighbor between MA5600T_B and MA5600T_A, and the IBGP neighbor between MA5600T_B, MA5600T_C, and MA5600T_D.

```
huawei(config)#bgp 2001
huawei(config-bgp)#router-id 2.2.2.2
huawei(config-bgp)#peer 10::2 as-number 2000
huawei(config-bgp)#peer 9:3::2 as-number 2001
huawei(config-bgp)#peer 9:1::2 as-number 2001
huawei(config-bgp)#ipv6-family unicast
huawei(config-bgp-af-ipv6)#peer 10::2 enable
huawei(config-bgp-af-ipv6)#peer 9:3::2 enable
huawei(config-bgp-af-ipv6)#peer 9:1::2 enable
huawei(config-bgp-af-ipv6)#import-route direct
huawei(config-bgp-af-ipv6)#quit
huawei(config-bgp)#quit
```

3. Save the data.

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

Step 3 Configure MA5600T_C.

1. Configure the IPv6 address of the Layer 3 interface.

```
huawei(config)#ipv6
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/19 0
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ipv6 enable
huawei(config-if-vlanif3)#ipv6 address 9:3::2 64
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 5 smart
huawei(config)#port vlan 5 0/19 0
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ipv6 enable
huawei(config-if-vlanif5)#ipv6 address 9:2::1 64
huawei(config-if-vlanif5)#quit
```

2. Enable the BGP function. Configure the IBGP neighbor between MA5600T_B and MA5600T_D.

```
huawei(config)#bgp 2001
huawei(config-bgp)#router-id 3.3.3.3
huawei(config-bgp)#peer 9:3::1 as-number 2001
huawei(config-bgp)#peer 9:2::2 as-number 2001
huawei(config-bgp)#ipv6-family unicast
huawei(config-bgp-af-ipv6)#peer 9:3::1 enable
huawei(config-bgp-af-ipv6)#peer 9:2::2 enable
huawei(config-bgp-af-ipv6)#import-route direct
huawei(config-bgp-af-ipv6)#quit
huawei(config-bgp)#quit
```

3. Save the data.

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

Step 4 Configure MA5600T_D.

1. Configure the IPv6 address of the Layer 3 interface.

```
huawei(config)#ipv6
huawei(config)#vlan 4 smart
huawei(config)#port vlan 4 0/19 0
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ipv6 enable
huawei(config-if-vlanif4)#ipv6 address 9:1::2 64
huawei(config-if-vlanif4)#quit
huawei(config)#vlan 5 smart
huawei(config)#port vlan 5 0/19 0
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ipv6 enable
huawei(config-if-vlanif5)#ipv6 address 9:2::2 64
huawei(config-if-vlanif5)#quit
```

2. Enable the BGP function. Configure the IBGP neighbor between MA5600T_B and MA5600T_C.

```
huawei(config)#bgp 2001
huawei(config-bgp)#router-id 4.4.4.4
huawei(config-bgp)#peer 9:1::2 as-number 2001
huawei(config-bgp)#peer 9:2::1 as-number 2001
huawei(config-bgp)#ipv6-family unicast
huawei(config-bgp-af-ipv6)#peer 9:1::2 enable
huawei(config-bgp-af-ipv6)#peer 9:2::1 enable
huawei(config-bgp-af-ipv6)#import-route direct
huawei(config-bgp-af-ipv6)#quit
huawei(config-bgp)#quit
```

3. Save the data.

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

----End

Result

- Run the **display bgp peer** command, and you can see that:
  - The EBGP connection is set up between MA5600T_A and MA5600T_B.
  - The IBGP connections are set up among MA5600T_B, MA5600T_C, and MA5600T_D.
  - The route with the destination subnet 8::/64 exists on MA5600T_C and MA5600T_D, and the next hop of the route is the interface address of MA5600T_A
- Run the **ping ipv6** command on MA5600T_C and MA5600T_D to ping the Layer 3 interface (8::1/64) on MA5600T_A. The **ping ipv6** command is executed successfully.

Configuration File

Configuration on each MA5600T is similar. Take MA5600T_A for example.

```
ipv6
vlan 6 smart
port vlan 6 0/19 0
interface vlanif 6
ipv6 enable
ipv6 address 10::2 64
quit
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ipv6 enable
ipv6 address 8::1 64
quit
bgp 2000
router-id 1.1.1.1
peer 10::1 as-number 2001
ipv6-family unicast
network 8.0.0.0 8
peer 10::1 enable
network 10:: 64
network 8:: 64
quit
quit
```

3.4.9 Configuring IPv4 in VPN

This topic describes how to categorize virtual private network (VPN) instances by VLANs, and realize the virtual IPv4 static route forwarding in different VPN instances.

Context

- A VPN instance is also called a VPN Routing and Forwarding (VRF) table. VRF is a Layer 3 virtual private network (L3 VPN). VRF is a mechanism in which a device works as multiple virtual routing devices. After the Layer 3 interfaces of the device are divided into different VRFs, multiple route forwarding instances can be emulated on the device.
- Multiple virtual routing devices can be created on the MA5600T/MA5603T. That is, multiple L3VPNs can be established to implement the Layer 3 isolation and independent

packet forwarding among different VRFs. MA5600T/MA5603T supports the following VRF functions:

- In different VRF instances, the IP address can be reused. It means that the IP addresses of the Layer 3 interfaces which belong to different VRF instances can be the same.
- The ping and trace route functions are supported in a VRF.
- The users of different VRF instances can obtain the IP addresses through the Dynamic Host Control Protocol (DHCP) relay or the DHCP proxy.
- The static routes and the dynamic routes in a VRF instance do not affect each other, and the routing entry in each VRF instance supports the routing function independently.

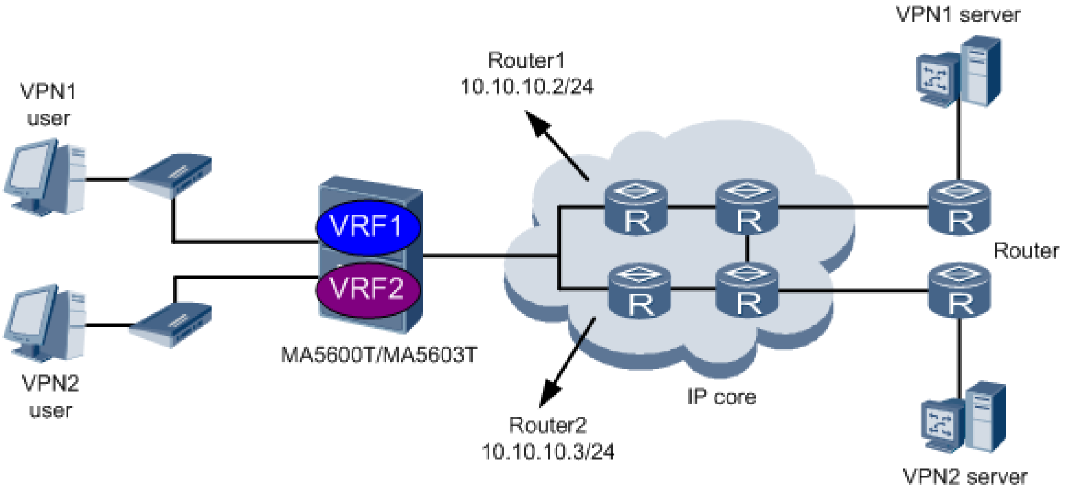
Networking

Figure 3-10 shows an example network for configuring IPv4 in VPN.

The MA5600T/MA5603T categorizes VRF instances by VLANs to provide L3VPN solutions. In this example, VPN instance VRF1 is categorized by virtual local area network (VLAN) 200, and IPv4 static routes are added in the virtual route forwarding entries of VRF1. The MA5600T/MA5603T selects the routes for the users of VPN1 by querying the routing entries of VRF1. Similarly, VPN instance VRF2 is categorized by VLAN 300 and is used to select the routes for the users of VPN2. The MA5600T/MA5603T implements the Layer 3 isolation and independent packet forwarding through different VRF instances.

This example describes how to configure the function of virtual static route forwarding by adding IPv4 static routes application on the instance. The function of virtual dynamic route forwarding can be realized by enabling the process of the dynamic routing protocols such as the open shortest path first (OSPF), Routing Information Protocol (RIP), intermediate system to intermediate system (IS-IS), and Border Gateway Protocol (BGP) in a VRF instance.

Figure 3-10 Example network for configuring IPv4 in VPN



Data Plan

Table 3-7 provides the data plan for configuring IPv4 in VPN.

Table 3-7 Data plan for configuring IPv4 in VPN

Item	Data
VRF1 (for VPN1)	Name of the VPN instance: vpn1 Route distinguisher (RD) of the VPN instance: 100:1
	Upstream port: 0/19/0 VLAN: 200 VLAN type: smart VLAN VPN1 user: ● Gigabit-capable passive optical network (GPON) port: 0/2/0 ● ONT ID: 0 ● GEM Port ID: 0
	IP address of the Layer 3 interface of VLAN 200: 10.10.10.1/24 IP address of router1: 10.10.10.2/24 IP address of the VPN1 server: 10.10.20.1/24
VRF2 (for VPN2)	Name of the VPN instance: vpn2 RD of the VPN instance: 100:2
	Upstream port: 0/19/0 VLAN: 300 VLAN type: smart VLAN VPN2 user: ● GPON port: 0/2/1 ● ONT ID: 1 ● GEM Port ID: 1
	IP address of the Layer 3 interface of VLAN 300: 10.10.10.1/24 IP address of router2: 10.10.10.3/24 IP address of the VPN2 server: 10.10.30.1/24

Procedure

- Configure VRF1 (for VPN1).
  1. Create a VPN instance of the IPv4 address family.
     ```
     huawei(config)#ip vpn-instance vpn1
     huawei(config-vpn-instance-vpn1)#ipv4-family
     ```
  2. Configure the RD of the VPN instance.
     ```
     huawei(config-vpn-instance-vpn1-af-ipv4)#route-distinguisher 100:1
     huawei(config-vpn-instance-vpn1-af-ipv4)#quit
     huawei(config-vpn-instance-vpn1)#quit
     ```
  3. Create a smart VLAN and add the upstream port and the service port to it.
     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

```
huawei(config)#service-port vlan 200 gpon 0/2/0 ont 0 gemport 0 multi-
service user-8021p 0 user-vlan 200 rx-cttr 5 tx-cttr 5
```

4. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip binding vpn-instance vpn1
  Info: All IPv4 related configurations on this interface are removed
  Info: All IPv6 related configurations on this interface are removed
```

5. Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif200)#ip address 10.10.10.1 24
huawei(config-if-vlanif200)#quit
```

6. Configure the IPv4 static route.

```
huawei(config)#ip route-static vpn-instance vpn1 10.10.20.0 24 10.10.10.2
```

7. Save the data.

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

- Configure VRF2 (for VPN2).

1. Create a VPN instance of the IPv4 address family.

```
huawei(config)#ip vpn-instance vpn2
huawei(config-vpn-instance-vpn2)#ipv4-family
```

2. Configure the RD of the VPN instance.

```
huawei(config-vpn-instance-vpn1-af-ipv4)#route-distinguisher 100:2
huawei(config-vpn-instance-vpn1-af-ipv4)#quit
huawei(config-vpn-instance-vpn1)#quit
```

3. Create a smart VLAN and add the upstream port and the service port to it.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 1 multi-
service user-8021p 0 user-vlan 300 rx-cttr 6 tx-cttr 6
```

4. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#ip binding vpn-instance vpn2
  Info: All IPv4 related configurations on this interface are removed
  Info: All IPv6 related configurations on this interface are removed
```

5. Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif300)#ip address 10.10.10.1 24
huawei(config-if-vlanif300)#quit
```

6. Configure the IPv4 static route.

```
huawei(config)#ip route-static vpn-instance vpn2 10.10.30.0 24 10.10.10.3
```

7. Save the data.

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

----End

Result

Run the **display ip vpn-instance** command to query the VPN configuration.

```
huawei(config)#display ip vpn-instance
{ <cr>|import-vt<K>|interface<K>|STRING<1-31>|verbose<K>||<K> }:

  Command:
          display ip vpn-instance
 Total VPN-Instances configured : 2

  VPN-Instance Name              Address-family
  vpn1                           ipv4
  vpn2                           ipv4
```

Run the following commands to verify that the VRF instances are configured successfully. The two IPv4 static routes are added to the IP routing table of VPN1 and VPN2.

```
huawei(config)#display ip routing-table vpn-instance vpn1
{ <cr>|verbose<K>|statistics<K>|protocol<K>|acl<K>|ip-prefix<K>|ip_addr<I><X.X.X
.X> }:

  Command:
          display ip routing-table vpn-instance vpn1
Routing Tables: vpn1
        Destinations : 3        Routes : 3

Destination/Mask    Proto  Pre  Cost       NextHop         Interface

     10.10.10.0/24  Direct 0    0          10.10.10.1      vlanif200
     10.10.10.1/32  Direct 0    0          127.0.0.1       InLoopBack0
     10.10.20.0/24  Static 60   0          10.10.10.2      vlanif200
huawei(config)#display ip routing-table vpn-instance vpn2
{ <cr>|verbose<K>|statistics<K>|protocol<K>|acl<K>|ip-prefix<K>|ip_addr<I><X.X.X
.X> }:

  Command:
          display ip routing-table vpn-instance vpn2
Routing Tables: vpn2
        Destinations : 3        Routes : 3

Destination/Mask    Proto  Pre  Cost       NextHop         Interface

     10.10.10.0/24  Direct 0    0          10.10.10.1      vlanif300
     10.10.10.1/32  Direct 0    0          127.0.0.1       InLoopBack0
     10.10.30.0/24  Static 60   0          10.10.10.3      vlanif300
```

Run the **ping** and **tracert** commands to check the VPN connectivity.

The MA5600T/MA5603T categorizes VRF instances by VLANs to provide L3VPN solutions, realizing the Layer 3 isolation of users or services.

- For the users of VPN1, the MA5600T/MA5603T selects the routes by querying the routing entries of VPN1. For example, for the packets to be sent to the VPN1 server (with IP address 10.10.20.1), the MA5600T/MA5603T selects its next hop router (with IP address 10.10.10.2) to forward the packets.
- For the users of VPN2, the MA5600T/MA5603T selects the routes by querying the routing entries of VPN2. For example, for the packets to be sent to the VPN2 server (with IP address 10.10.30.1), the MA5600T/MA5603T selects its next hop router (with IP address 10.10.10.3) to forward the packets.
- For the users outside the VPNs, the route to the VPN1 server or the VPN2 server is not available.

Configuration File

Only the configuration files related to the VPN are listed.

```
ip vpn-instance vpn1
ipv4-family
route-distinguisher 100:1
quit
quit
ip vpn-instance vpn2
ipv4-family
route-distinguisher 100:2
quit
quit
interface vlanif200
ip binding vpn-instance vpn1
ip address 10.10.10.1/24
quit
interface vlanif300
ip binding vpn-instance vpn2
ip address 10.10.10.1/24
quit
ip route-static vpn-instance vpn1 10.10.20.0 24 10.10.10.2
ip route-static vpn-instance vpn2 10.10.30.0 24 10.10.10.3
```

3.4.10 Configuring IPv6 in VPN

This topic describes how to categorize virtual private network (VPN) instances by virtual local area networks (VLANs), and implement the virtual IPv6 static route forwarding in different VPN instances.

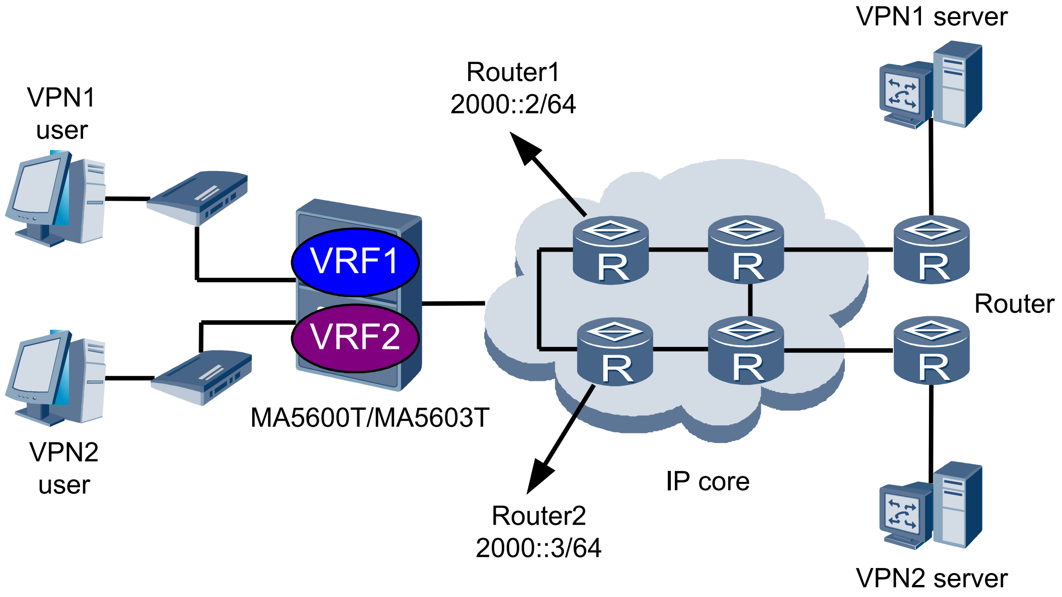
Networking

The MA5600T/MA5603T supports virtual route forwarding (VRF) in the IPv6 network. The VRF principle and functions in the IPv6 network are the same as those in the IPv4 network.**Figure 3-11** shows an example network for configuring IPv6 in VPN.

The MA5600T/MA5603T categorizes VRF instances by VLANs to provide L3 VPN solutions. In this example, VPN instance VRF1 is categorized by virtual local area network (VLAN) 200, and IPv6 static routes are added in the virtual route forwarding entries of VRF1. The MA5600T/MA5603T selects the routes for the users of VPN1 by querying the routing entries of VRF1. Similarly, VPN instance VRF2 is categorized by VLAN 300 and is used to select the routes for the users of VPN2. The MA5600T/MA5603T implements the Layer 3 isolation and independent packet forwarding through different VRF instances.

This example describes how to configure the function of virtual static route forwarding by adding IPv6 static routes application on the instance. In addition, virtual dynamic route forwarding can be implemented by using BGP4+. For details about BGP4+ configurations, see **Configuration Example of BGP4+**

Figure 3-11 Example network for configuring IPv6 in VPN



Data Plan

Table 3-8 provides the data plan for configuring IPv6 in VPN.

Table 3-8 Data plan for configuring IPv6 in VPN

Item	Data
VRF1 (for VPN1)	Name of the VPN instance: vpn1 Route distinguisher (RD) of the VPN instance: 100:1
	Upstream port: 0/19/0 VLAN: 200 VLAN type: smart VLAN VPN1 user: ● Gigabit-capable passive optical network (GPON) port: 0/2/0 ● ONT ID: 0 ● GEM Port ID: 0
	IPv6 address of the Layer 3 interface of VLAN 200: 2000::1/64 IPv6 address of router1: 2000::2/64 IPv6 address of the VPN1 server: 2001::1/64
VRF2 (for VPN2)	Name of the VPN instance: vpn2 Route distinguisher (RD) of the VPN instance: 100:2
	Upstream port: 0/19/0 VLAN: 300 VLAN type: smart VLAN VPN2 user: ● GPON port: 0/2/1 ● ONT ID: 1 ● GEM Port ID: 1
	IPv6 address of the Layer 3 interface of VLAN 300: 2000::1/64 IPv6 address of router2: 2000::3/64 IPv6 address of the VPN2 server: 2002::1/64

Procedure

- Configure VRF1 (for VPN1).
  1. Enable IPv6.
     ```
     huawei(config)#ipv6
     ```
  2. Create a VPN instance of the IPv6 address family.
     ```
     huawei(config)#ip vpn-instance vpn1
     huawei(config-vpn-instance-vpn1)#ipv6-family
     ```
  3. Configure the RD of the VPN instance.

```
huawei(config-vpn-instance-vpn1-af-ipv6)#route-distinguisher 100:1
```

4. (Optional) Configure the IPv6 routing specifications of the VPN instance.

```
huawei(config-vpn-instance-vpn1-af-ipv6)#prefix limit 1000 simply-alert
huawei(config-vpn-instance-vpn1-af-ipv6)#routing-table limit 1000 simply-
alert
huawei(config-vpn-instance-vpn1-af-ipv6)#quit
huawei(config-vpn-instance-vpn1)#quit
```

5. Create a smart VLAN and add the upstream port and the service port to it.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
huawei(config)#service-port vlan 200 gpon 0/2/0 ont 0 gemport 0 multi-
service user-8021p 0 user-vlan 200 rx-cttr 5 tx-cttr 5
```

6. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip binding vpn-instance vpn1
  Info: All IPv4 related configurations on this interface are removed
  Info: All IPv6 related configurations on this interface are removed
```

7. Configure the IPv6 address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif200)#ipv6 enable
huawei(config-if-vlanif200)#ipv6 address 2000::1 64
huawei(config-if-vlanif200)#quit
```

8. Configure the IPv6 static route.

```
huawei(config)#ipv6 route-static vpn-instance vpn1 2001:: 64 2000::2
```

9. Save the data.

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

- Configure VRF2 (for VPN2).

1. Enable IPv6.

```
huawei(config)#ipv6
```

2. Create a VPN instance of the IPv6 address family.

```
huawei(config)#ip vpn-instance vpn2
huawei(config-vpn-instance-vpn2)#ipv6-family
```

3. Configure the RD of the VPN instance.

```
huawei(config-vpn-instance-vpn2-af-ipv6)#route-distinguisher 100:2
```

4. (Optional) Configure the IPv6 routing specifications of the VPN instance.

```
huawei(config-vpn-instance-vpn2-af-ipv6)#prefix limit 1000 simply-alert
huawei(config-vpn-instance-vpn2-af-ipv6)#routing-table limit 1000 simply-
alert
huawei(config-vpn-instance-vpn2-af-ipv6)#quit
huawei(config-vpn-instance-vpn2)#quit
```

5. Create a smart VLAN and add the upstream port and the service port to it.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 1 multi-
service user-8021p 0 user-vlan 300 rx-cttr 6 tx-cttr 6
```

6. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#ip binding vpn-instance vpn2
  Info: All IPv4 related configurations on this interface are removed
  Info: All IPv6 related configurations on this interface are removed
```

7. Configure the IPv6 address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif300)#ipv6 enable
huawei(config-if-vlanif300)#ipv6 address 2000::1 64
huawei(config-if-vlanif300)#quit
```

8. Configure the IPv6 static route.

```
huawei(config)#ipv6 route-static vpn-instance vpn2 2002:: 64 2000::3
```

9. Save the data.

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

----End

Result

Run the **display ip vpn-instance** command to query the VPN configurations.

```
huawei(config)#display ip vpn-instance
{ <cr>|import-vt<K>|interface<K>|STRING<1-31>|verbose<K>||<K> }:

  Command:
          display ip vpn-instance
 Total VPN-Instances configured : 2

  VPN-Instance Name               Address-family
  vpn1                            ipv6
  vpn2                            ipv6
```

Run the following commands to verify that the configurations are successful and the IPv6 static route is added to the IPv6 routing table of VPN1 and VPN2.

```
huawei(config)#display ipv6 routing-table vpn-instance vpn1
{ <cr>|acl<K>|ipv6-prefix<K>|protocol<K>|statistics<K>|verbose<K>|x:x::x:x<IPv6>
<x:x::x:x>||<K> }:

  Command:
          display ipv6 routing-table vpn-instance vpn1
Routing Table : vpn1
        Destinations : 4        Routes : 4

 Destination  : 2000::                          PrefixLength : 64
 NextHop      : 2000::1                         Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : vlanif200                       Flags        : D

 Destination  : 2000::1                         PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : InLoopBack0                     Flags        : D

 Destination  : 2001::                          PrefixLength : 64
 NextHop      : 2000::2                         Preference   : 60
 Cost         : 0                               Protocol     : Static
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : vlanif200                       Flags        : RD

 Destination  : FE80::                          PrefixLength : 10
 NextHop      : ::                              Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : null0                           Flags        : D
huawei(config)#display ipv6 routing-table vpn-instance vpn2
{ <cr>|acl<K>|ipv6-prefix<K>|protocol<K>|statistics<K>|verbose<K>|x:x::x:x<IPv6>
<x:x::x:x>||<K> }:

  Command:
          display ipv6 routing-table vpn-instance vpn2
Routing Table : vpn2
        Destinations : 4        Routes : 4

 Destination  : 2000::                          PrefixLength : 64
 NextHop      : 2000::1                         Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : vlanif200                       Flags        : D

 Destination  : 2000::1                         PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : InLoopBack0                     Flags        : D

 Destination  : 2002::                          PrefixLength : 64
 NextHop      : 2000::3                         Preference   : 60
 Cost         : 0                               Protocol     : Static
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : vlanif300                       Flags        : RD

 Destination  : FE80::                          PrefixLength : 10
 NextHop      : ::                              Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : null0                           Flags        : D
```

Run the **ping ipv6** and **tracert ipv6** commands to check the VPN connectivity.

The MA5600T/MA5603T categorizes VRF instances by VLANs to provide L3 VPN solutions, realizing the Layer 3 isolation of users or services.

- For the users of VPN1, the MA5600T/MA5603T selects the routes by querying the routing entries of VPN1. For example, for the packets to be sent to the VPN1 server (with IPv6 address 2001::1), the MA5600T/MA5603T selects its next hop router (with IPv6 address 2000::2) to forward the packets.
- For the users of VPN2, the MA5600T/MA5603T selects the routes by querying the routing entries of VPN2. For example, for the packets to be sent to the VPN2 server (with IPv6 address 2002::1), the MA5600T/MA5603T selects its next hop router (with IPv6 address 2000::3) to forward the packets.
- For the users outside the VPNs, the route to the VPN1 server or the VPN2 server is not available.

Configuration File

Only the configuration files related to the VPN are listed.

```
ipv6
ip vpn-instance vpn1
ipv6-family
route-distinguisher 100:1
routing-table limit 1000 simply-alert
prefix limit 1000 simply-alert
quit
quit
ip vpn-instance vpn2
ipv6-family
route-distinguisher 100:2
routing-table limit 1000 simply-alert
prefix limit 1000 simply-alert
quit
quit
interface vlanif200
ip binding vpn-instance vpn1
ipv6 enable
ipv6 address 2000::1/64
quit
interface vlanif300
ip binding vpn-instance vpn2
ipv6 enable
```

```
ipv6 address 2000::1/64
quit
ipv6 route-static vpn-instance vpn1 2001:: 64 2000::2
ipv6 route-static vpn-instance vpn2 2002:: 64 2000::3
```

4 Configuring the xDSL Internet Access Service

About This Chapter

xDSL broadband Internet access is applicable in the scenario where the Internet service is provided through the ordinary twisted pairs. In this scenario, a user can access Internet in IPoE, PPPoE, IPoA or PPPoA. This topic describes how to configure an xDSL Internet access service on the MA5600T/MA5603T.

Prerequisite

The Authentication, Authorization and Accounting (AAA) function is required only when the Internet access mode is PPPoE or PPPoA.

- To enable the AAA function on the device, see **2.11 Configuring AAA**.
- If the AAA function is implemented by the broadband remote access server (BRAS), a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Users connect to the Internet in IPoE, PPPoE, IPoA, or PPPoA mode.

- In IPoE mode, the MA5600T/MA5603T encapsulates the IP packet payload to Ethernet frames and sends the Ethernet packets to the upper layer network. IPoE is mostly used on a private line network to meet operators' IP access requirements. An authentication is generally not required for IPoE users.
- In PPPoE mode, the MA5600T/MA5603T transmits PPPoE user packets to the upper layer Ethernet-based PPPoE server (BRAS). PPPoE is a common mode for Internet access. In this mode, PPPoE users must be authenticated using Authentication, Authorization and Accounting (AAA) policies before connecting to the Internet.
- In IPoA mode, the MA5600T/MA5603T encapsulates the IP packet payload to Ethernet frames and sends the Ethernet packets to the upper layer network. In the downstream, the MA5600T/MA5603T decapsulates the IPoE packets to IPoA packets and sends the packets to users. IPoA is generally used on a private line network to meet operators' requirements

for transferring from an ATM network to the IP network. An authentication is generally not required for IPoA users.

- In PPPoA mode, the MA5600T/MA5603T transmits PPPoA user packets to the upper layer Ethernet-based PPPoE server (BRAS) to meet operators' requirements for transferring from an ATM network to the IP network. PPPoA users must be authenticated using Authentication, Authorization and Accounting (AAA) policies before connecting to the Internet.

Data Plan

Before configuring an xDSL Internet access service, plan the data items as listed in **Table 4-1**.

Table 4-1 Data plan for the xDSL Internet access service

Item	Data	Remarks
MA5600T / MA5603T	Access rate	Specify an access rate according to the user requirement.
	Access port	Specify an access port according to the specific network planning.
	VPI/VCI	The VPI/VCI is valid only for the ATM access and must be the same as the VPI/VCI of the interconnected device.
	VLAN planning	The VLAN planning must ensure proper cooperation with the upper-layer device and therefore the upstream VLAN must be consistent with the upstream VLAN of the upper-layer device.
	QoS policy	According to the general QoS policy for the entire network, the priority of an ordinary Internet access service is lower than the priority of a voice or video service.
	IP address	The IP address must be consistent with the IP address of the upper-layer route.
Upper-layer LAN switch	The LAN switch transparently transmits the service packets of the MA5600T/MA5603T on Layer 2. The VLAN ID must be consistent with the VLAN ID of the upstream service packets of the MA5600T/MA5603T.	-

Item	Data	Remarks
BRAS	The BRAS performs the related configurations according to the authentication and accounting requirements for dial-up users. For example, the BRAS configures the access user domain (including the authentication plan, accounting plan, and authorization plan bound to the domain) and specifies the RADIUS server. If the BRAS is used to authenticate users, you need to configure the user name and the password for each user on the BRAS. If the BRAS is used to allocate IP addresses, you must configure an IP address pool on the BRAS.	-

Procedure

1. 4.1 Configuring an xDSL Profile
   When configuring a service, you need to configure the service and quality parameters for an x digital subscriber line (xDSL) port according to the service type, and also need to plan other parameters such as activation and rate. An xDSL profile defines all required parameters for activating an xDSL port. This topic describes how to configure asymmetric digital subscriber line 2 plus (ADSL2+), single-pair high-speed digital subscriber line (SHDSL), very-high-speed digital subscriber line 2 (VDSL2) profiles and x digital subscriber line (xDSL) profiles (TR165 Mode).
2. 4.2 Creating a VLAN
   Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.
3. 4.3 Configuring an Upstream Port
   The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.
4. 4.4 (Optional) Configuring Line Bonding
   To increase the network bandwidth of a user, you can bind multiple ports together.
5. 4.5 Configuring an xDSL Port
   An xDSL port can transmit services only when it is activated. This topic describes how to activate an xDSL port and bind an xDSL profile to the port.
6. 4.6 Creating an xDSL Service Port
   A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.
7. 4.7 (Optional) Configuring the xPoA-xPoE Protocol Conversion
   xPoA to xPoE conversion involves the conversion from IP over ATM (IPoA) to IP over Ethernet (IPoE) and the conversion from Point-to-Point Protocol over ATM (PPPoA) to Point-to-Point Protocol over Ethernet (PPPoE). ATM is the abbreviation for asynchronous transfer mode (ATM). xPoA packets cannot be transmitted on an IP network and must be

converted into xPoE packets. IPoA packets must be converted into IPoE and PPPoA packets must be converted into PPPoE packets to be transmitted on an IP network. Protocol conversion is required when the packet encapsulation mode is IPoA or PPPoA and is not required when the packet encapsulation mode is IPoE or PPPoE.

8. 4.8 (Optional) Configuring the VDSL2 Vectoring Function
   This topic describes how to configure the vectoring function on a very-high-speed digital subscriber line 2 (VDSL2). This technology can greatly cancel the far-end crosstalk (FEXT) on a VDSL2 line and increases VDSL2 rates.

4.1 Configuring an xDSL Profile

When configuring a service, you need to configure the service and quality parameters for an x digital subscriber line (xDSL) port according to the service type, and also need to plan other parameters such as activation and rate. An xDSL profile defines all required parameters for activating an xDSL port. This topic describes how to configure asymmetric digital subscriber line 2 plus (ADSL2+), single-pair high-speed digital subscriber line (SHDSL), very-high-speed digital subscriber line 2 (VDSL2) profiles and x digital subscriber line (xDSL) profiles (TR165 Mode).

4.1.1 Configuring an ADSL2+ Template

When configuring an asymmetric digital subscriber line 2 plus (ADSL2+) service, you need to configure the service and quality parameters for an ADSL2+ port according to the service type, and also need to plan other parameters such as activation and rate. An ADSL2+ profile defines all required parameters for activating an ADSL2+ port. This topic describes how to configure ADSL2+ profiles in different modes.

Prerequisites

The ADSL mode must be switched to rfc4706.

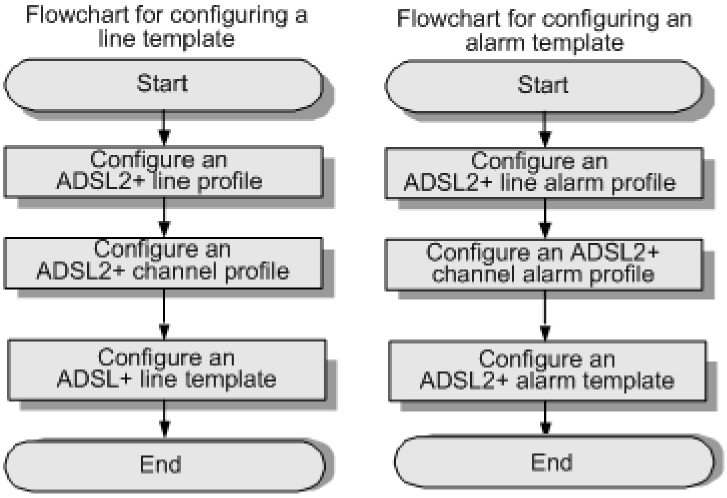
Context

- The device supports three ADSL2+ modes: normal mode (RFC2662), new generation asymmetric digital subscriber lines (NG-ADSL) mode (RFC4706), and TR165 mode. You can run the **switch adsl mode to** command to select a mode. By default, the normal mode is used.
  - Normal mode: This mode is used for common ADSL2+ profiles, including ADSL2+ line profiles, ADSL2+ line alarm profiles, and ADSL2+ extended line profiles.
  - NG-ADSL mode: In this mode, ADSL2+ line profile parameters are reorganized, and a line template and a line alarm template are used. The line template uses the line profile and the channel profile as references, and the line alarm template uses the line alarm profile and the channel alarm profile as references.
  - TR165 mode: A line profile consists of 10 profiles, which are: xDSL rate profile, power spectrum density (PSD) profile, xDSL spectrum profile, xDSL upstream power backoff (UPBO) profile, xDSL downstream power backoff (DPBO) profile, radio frequency interference (RFI) profile, xDSL noise margin profile, xDSL virtual noise profile, xDSL impulsive noise protection profile, and xDSL impulsive noise monitoring profile. All these profiles must be bound to an x digital subscriber line (xDSL) port for activating the xDSL port. For the configuration of TR165 profiles, see **Configuring xDSL Profiles (TR165 Mode)**.
  - In this task, the configuration specified is based on the NGADSL mode.
    - When activating an ADSL2+ port, you need to bind the ADSL2+ line template and alarm template to the port.
    - An ADSL2+ line template should be formed by binding an ADSL2+ line profile with an ADSL2+ channel profile.

- An ADSL2+ line alarm template should be formed by binding an ADSL2+ line alarm profile with an ADSL2+ channel alarm profile.

- **Figure 4-1** shows the flow for configuring an ADSL2+ template.

Figure 4-1 Flowchart for configuring an ADSL2+ template


Flowchart for configuring a line template
Start
Configure an ADSL2+ line profile
Configure an ADSL2+ channel profile
Configure an ADSL+ line template
End
Flowchart for configuring an alarm template
Start
Configure an ADSL2+ line alarm profile
Configure an ADSL2+ channel alarm profile
Configure an ADSL2+ alarm template
End

Procedure

- Configure an ADSL2+ line template.

1. Run the **adsl line-profile quickadd** command to quickly add an ADSL2+ line profile, or run the interactive **adsl line-profile add** command to add an ADSL2+ line profile.

   Main parameters:

   - **transmode**: indicates the line transmission mode. By default, the system supports all transmission modes. The user can adopt the default value for auto-adaptation.
   - **snr**: indicates the SNR margin, which refers to the idle space for carrying noise, excluding the space for carrying signals. In general, the SNR margin of the minimum tone is considered as the SNR margin of the entire ADSL connection.

2. Run the **adsl channel-profile quickadd** command to quickly add an ADSL2+ channel profile, or run the interactive **adsl channel-profile add** command to add an ADSL2 + channel profile.

   Main parameters:

   - **interleaved-delay** and **interleaving delay** (in interactive mode): Indicates the interleave delay. A zero interleave delay corresponds to the fast mode. In fast mode, the interleave delay is short, but the error correction capability is weak. A non-zero interleave delay corresponds to the interleave mode. The larger the interleave delay is, the deeper the interleave depth is, and the stronger the error correction capability is.
   - **inp**: indicates impulse noise protection. As a parameter that describes the line capability of resisting impulse interference, INP affects the port rate. If INP is 1, the current channel can resist the impulse noise in 1 DMT character length. The interleave delay is related to INP. In the fast mode, INP does not apply.

  - **rate**: indicates the line rate. During line activation, a proper rate between the preset maximum rate and minimum rate is determined through automatic negotiation according to the line condition and the profile configuration. The user rate can be restricted by this line rate or the rate set in the traffic profile bound to the user. When both rates function, the lower one is adopted as the user rate.

3. Run the **adsl line-template quickadd** command to quickly add an ADSL+ line template, or run the interactive **adsl line-template add** command to add an ADSL2+ line template.

   An ADSL2+ line template is formed by binding an ADSL2+ line profile with an ADSL2+ channel profile. An ADSL2+ port needs to be bound to only an ADSL2+ line template.

- Configure an ADSL2+ alarm template.
  1. Run the **adsl alarm-profile quickadd** command to quickly add an ADSL2+ alarm profile, or run the interactive **adsl alarm-profile add** command to add an ADSL2+ alarm profile.
  2. Run the **adsl channel-alarm-profile quickadd** command to quickly add an ADSL channel alarm profile, or run the interactive **adsl channel-alarm-profile add** command to add an ADSL2+ channel alarm profile.
  3. Run the **adsl alarm-template quickadd** command to quickly add an ADSL2+ alarm template, or run the interactive **adsl alarm-template add** command to add an ADSL2+ alarm template.

     An ADSL2+ alarm template is formed by binding an ADSL2+ line alarm profile with an ADSL2+ channel alarm profile. An ADSL2+ port needs to be bound with only an ADSL2+ alarm template.

----End

Example

Assume that an ADSL2+ line template with an index number of 3 is to be added. For the ADSL2+ line template, the downstream rate is 2048 kbit/s, the channel mode is the interleave mode, the maximum interleave delay is 10 ms, and the SNR margin is 6 dB. To configure such an ADSL2+ line template, do as follows:

```
huawei(config)#adsl line-profile quickadd 3 snr 60 30 120 60 30 120
huawei(config)#adsl channel-profile quickadd 3 interleaved-delay 10 10 rate 1024
 2048 3096 1024 2048 3096
huawei(config)#adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2 3
```

4.1.2 Configuring SHDSL Profiles

This topic describes how to configure the SHDSL line profile and alarm profile.

Context

The SHDSL line profile and alarm profile can be directly bound to an SHDSL port.

Table 4-2 lists the default SHDSL profiles.

Table 4-2 Default SHDSL profiles

Parameter	Default Setting
SHDSL line profile	Profile IDs: 1, 100, 101, 102, 103, 104, 105, 106, and 107. Where, ● Profile 1 is used to activate 2-wire SHDSL ports in the ATM mode. ● Profile 100 is used to activate 4-wire SHDSL ports in the ATM mode. ● Profile 101 is used to activate 6-wire SHDSL ports in the ATM mode. ● Profile 102 is used to activate 8-wire SHDSL ports in the ATM mode. ● Profile 103 is used to activate the SHDSL port bound to the EFM. ● Profile 104 is used to activate 4-wire SHDSL ports in the TDM mode, and the frame encapsulation format is E1. ● Profile 105 is used to activate 4-wire SHDSL ports in the TDM mode, and the frame encapsulation format is V35. ● Profile 106 is used to activate 2-wire SHDSL ports in the TDM mode, and the frame encapsulation format is E1. ● Profile 107 is used to activate 2-wire SHDSL ports in the TDM mode, and the frame encapsulation format is V35.
SHDSL alarm profile	Profile ID: 1

Procedure

- Configure an SHDSL line profile.

  Run the **shdsl line-profile quickadd** command to quickly add an SHDSL line profile, or run the interactive **shdsl line-profile add** command to add an SHDSL line profile.

  Main parameters:

  - **data path mode**: Indicates the data path mode. Configure the data path mode according to the actual application scenario of the line. Three modes, namely ATM, PTM, and TDM modes are supported.
  - **rate**: indicates the line rate. During line activation, a proper rate between the preset maximum rate and minimum rate is determined through automatic negotiation according to the line condition and the profile configuration. The user rate can be restricted by this rate or the rate set in the traffic profile that is bound to the user. When both rates function, the lower rate is selected as the user rate.

  - **transmission**: indicates the transmission mode. Set the transmission mode according to line conditions and actual planning. Three transmission modes are supported: annex A, annex L, and annex A&B.
  - **snr-margin**: The larger the SNR margin, the better the line stability, and meanwhile the lower the physical connection rate of the line after activation. For common Internet access users, set the target SNR margin to 3; for users with higher priorities, set the target SNR margin to 5.

  NOTE

  When the board supports G.SHDSL.bis (including the extended standard annex F), the maximum rate can reach 5696 kbit/s.

- Configure an SHDSL alarm profile.

  Run the **shdsl alarm-profile quickadd** command to quickly add an SHDSL alarm profile, or run the interactive **shdsl line-profile add** command to add an SHDSL alarm profile.

----End

Example

To add SHDSL line profile 3 with the line rate of 4096 kbit/s, which is used to activate the 4-wire SHDSL port, do as follows:

```
huawei(config)#shdsl line-profile quickadd 3 line four-wire rate 4096
```

Assume that the loop attenuation threshold is 10 dB, SNR margin is 0 dB, ES threshold is 100s, SES threshold is 100s, CRC abnormality duration threshold is 10000, LOSWS threshold is 100s, UAS threshold is 100s. To quickly add SHDSL line alarm profile 3 with these parameters, do as follows:

```
huawei(config-if-shl-0/3)#shdsl alarm-profile quickadd 3 loop-attenuation 10 snr-
margin
 0 es 100 ses 100 crc-anomaly 10000 losws 100 uas 100
```

4.1.3 Configuring VDSL2 Profiles

When configuring a very-high-speed digital subscriber line 2 (VDSL2) service, you need to configure the service and quality parameters for a VDSL2 port according to the service type, and also need to plan other parameters such as activation and rate. A VDSL2 profile defines all required parameters for activating a VDSL2 port. This topic describes how to configure VDSL2 profiles in different modes.

Context

The MA5600T/MA5603T supports three VDSL2 modes, normal(TR129 mode), TI, and TR165, which are selected by running **switch vdsl mode to** command. By default, the system supports the normal VDSL2 mode(TR129 mode).

In the TR129 mode, TI mode, and TR165 mode, there is no difference in the alarm profile, but there are differences in the line profile.

- Normal mode: It is the mode for VDSL2 general profiles. VDSL2 general profiles are classified into the VDSL2 line profile, VDSL2 channel profile, and VDSL2 line template.
- TI mode: In TI mode, the parameters in the VDSL2 profile are re-organized. Specifically, the parameters are classified by type and frequency used. In TI mode, VDSL2 profiles are classified into six types: VDSL2 service profile, VDSL2 frequency spectrum profile,

VDSL2 UPBO profile, VDSL2 DPBO profile, VDSL2 SNR margin profile, and VDSL2 delay INP profile.

- TR165 mode: In TR165 mode, a line profile consists of 9 profiles: xDSL rate profile, power spectrum density (PSD) profile, xDSL frequency spectrum profile, xDSL upstream power back-of (UPBO) profile, xDSL downstream power back-of (DMBO) profile, radio frequency interference (RFI) profile, xDSL signal to noise ratio (SNR) margin profile, xDSL virtual noise profile, xDSL delay impulse noise protection (INP) profile. You must bind these profiles to an xDSL port before activating the port.

Configuring VDSL2 Profiles (TR129 Mode)

Before configuring very-high-speed digital subscriber line 2 (VDSL2) services, you need to determine the management mode for VDSL2 lines. The management mode for VDSL2 lines is TR129, TI, or TR165. When configuring the VDSL2 services, you need to configure a line profile. By doing so, you can set service parameters and channel quality parameters for VDSL2 ports based on the service type, and plan parameters for activation mode and frequency spectrum. When the TR129 management mode is used, you need to configure a VDSL2 mode in normal mode.

Prerequisites

The VDSL2 mode has been switched to TR129 by running the **switch vdsl mode to tr129** command.

Context

The system supports the TR129 mode by default.

- The VDSL2 line template binds to a VDSL2 line profile and a VDSL2 channel profile. When activating a VDSL2 port, you need to bind the VDSL2 line template to the port.
- Before activating a VDSL2 port, bind a VDSL2 line template to the port.
- The VDSL2 alarm template binds to a VDSL2 line alarm profile and a VDSL2 channel alarm profile. When activating a VDSL2 port, you need to bind the VDSL2 alarm template to the port.

Table 4-3 lists the default settings of VDSL2 profiles.

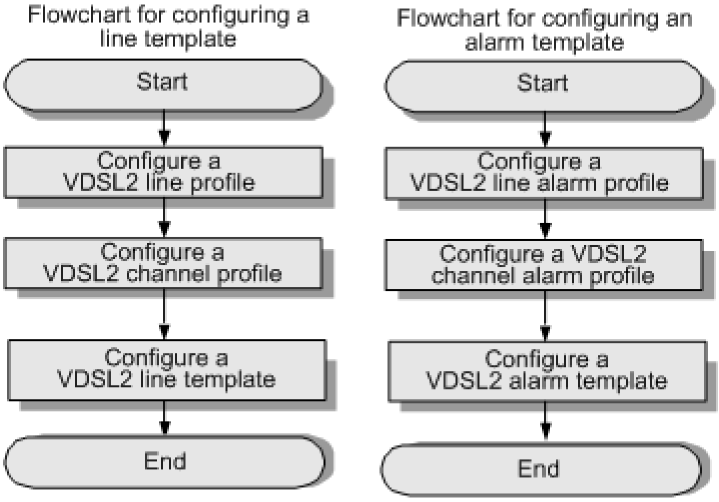
Table 4-3 Default settings of VDSL2 profiles

Parameter	Default Value
VDSL2 line profile	Profile ID: 1 The settings in the default profile are for reference.
VDSL2 channel profile	Profile ID: 1 The settings in the default profile are for reference.
VDSL2 line alarm profile	Profile ID: 1 In the default profile, the terminal power-off alarm reporting function is enabled, and other parameters are set to 0.

Parameter	Default Value
VDSL2 channel alarm profile	Profile ID: 1 All parameters in the default profile are set to 0, indicating that alarms will not be reported.

Figure 4-2 provides the configuration flow of a VDSL2 profile.

Figure 4-2 Flowchart for configuring a VDSL2 profile


Flowchart for configuring a line template
Start
Configure a VDSL2 line profile
Configure a VDSL2 channel profile
Configure a VDSL2 line template
End
Flowchart for configuring an alarm template
Start
Configure a VDSL2 line alarm profile
Configure a VDSL2 channel alarm profile
Configure a VDSL2 alarm template
End

Procedure

- Configure a VDSL line template.
  1. Run the **vdsl line-profile quickadd** command to quickly add a VDSL line profile, or run the interactive **vdsl line-profile add** command to add a VDSL line profile.

     Main parameters:

     – **transmode**: indicates the line transmission mode. By default, the system supports all transmission modes. The default setting can be used. Then, the system automatically adapts to the transmission mode of the peer end.

     – **SNR margin**: indicates the SNR margin. It refers to the remaining space for carrying noise, excluding the space for carrying signals. In general, the SNR margin of the minimum tone is used as the SNR margin of the entire VDSL2 connection.
  2. Run the **vdsl channel-profile quickadd** command to quickly add a VDSL channel profile, or run the interactive **vdsl channel-profile add** command to add a VDSL channel profile.

     Main parameters:

     – **path-mode**: Indicates the path mode. There are two VDSL path modes: ATM mode and PTM mode. By default, the system supports both modes and automatically adapt the path mode according to the modem. You may not configure the path mode. If the modem supports the ATM mode, select **ATM**; if the modem supports the PTM, select **PTM**; if the modem supports both modes and the path mode is set to **Both**, the **PTM** mode is preferred to activate the line.

NOTE

For H805VDMF, H805VDRD, H80BVDPE and H80BVDPM boards, only ATM is supported in ADSL mode and only PTM is supported in VDSL mode.

- **interleaved-delay**: indicates the interleave delay. A zero interleave delay corresponds to the fast mode. In the fast mode, the interleave delay is short, but the error correction capability is weak. A non-zero interleave delay corresponds to the interleave mode. The longer the interleave delay, the greater the interleave depth. In the interleave mode, the greater the interleave depth, the stronger the error correction capability, but the longer the delay.
- **inp**: indicates the impulse noise protection. The INP is a parameter that describes the line capability of resisting impulse interference. The INP affects the port rate. If the INP is 1, the current channel can resist the impulse noise in 1 DMT character length. The interleave delay is related to the INP. In the fast mode, the INP is meaningless.
- **rate**: indicates the line rate. During line activation, a proper rate between the preset maximum rate and minimum rate is determined through automatic negotiation according to the line condition and the profile configuration. The user rate can be restricted by this rate or the rate set in the traffic profile bound to the user. When both rates function, the lower rate is selected as the user rate.

3. Run the **vdsl line-template quickadd** command to quickly add a VDSL2 line template, or run the interactive **vdsl line-template add** command to add a VDSL2 line template.

   A VDSL2 line template consists of a VDSL2 line profile and a VDSL2 channel profile. To activate a VDSL2 port, bind a VDSL2 line template to the port.

- Configure a VDSL2 alarm template.
  1. Run the **vdsl alarm-profile quickadd** command to quickly add a VDSL2 line alarm profile, or run the interactive **vdsl alarm-profile add** command to add a VDSL2 line alarm profile.
  2. Run the **vdsl channel-alarm-profile quickadd** command to quickly add a VDSL2 channel alarm profile, or run the interactive **vdsl channel-alarm-profile add** command to add a VDSL2 channel alarm profile.
  3. Run the **vdsl alarm-template quickadd** command to quickly add a VDSL2 alarm template, or run the interactive **vdsl alarm-template add** command to add a VDSL2 alarm template.

     After the VDSL2 line template is configured, VDSL2 ports can be bound to the profile.

----End

Example

Assume that:

- Downstream rate: 2048 kbit/s
- Channel mode: interleaved-delay
- Downstream maximum interleave delay: 8 ms
- Upstream maximum interleave delay: 2 ms

- SNR margin: 6 dB
- Downstream minimum INP: 4
- Upstream minimum INP: 2

To add VDSL2 profile 3 with these parameters, do as follows:

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

Configuring VDSL2 Profiles (TI Mode)

Before configuring very-high-speed digital subscriber line 2 (VDSL2) services, you need to determine the management mode for VDSL2 lines. The management mode for VDSL2 lines is TR129, TI, or TR165. When configuring the VDSL2 services, you need to configure a line profile. By doing so, you can set service parameters and quality related parameters for VDSL2 ports based on service type, and plan parameters for activation mode and frequency spectrum. When the TI management mode is used, you need to configure a VDSL2 mode in TI mode.

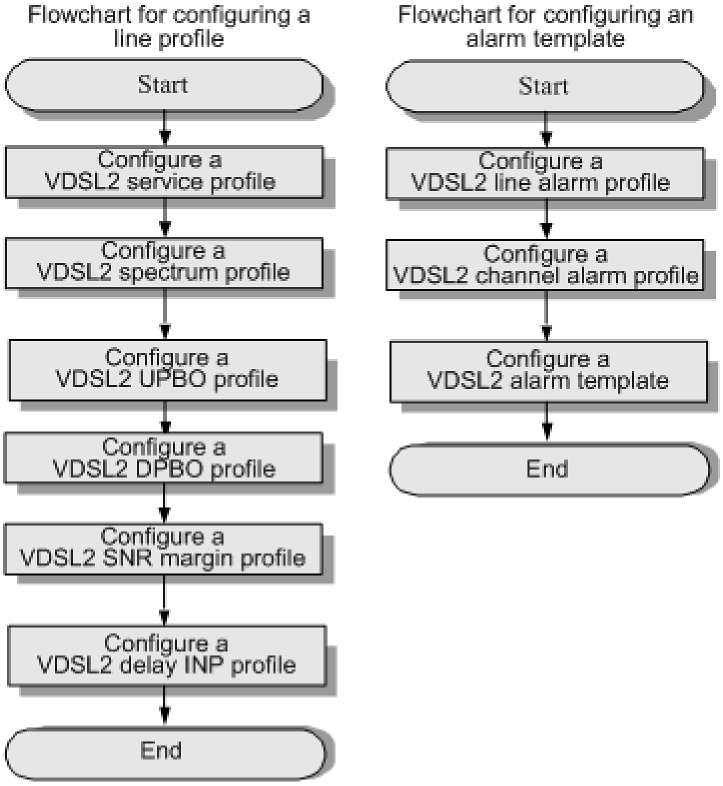
Prerequisites

The VDSL2 mode has been switched to TI by running the **switch vdsl mode to timode** command.

Context

The VDSL2 line profile is re-organized to form six types of profiles. Before activating a VDSL2 port, bind six types of VDSL2 line configurations to the VDSL2 port. A VDSL2 alarm template is formed by binding a VDSL2 line alarm profile with a VDSL2 channel alarm profile. Bind a VDSL2 alarm template rather than a VDSL2 line alarm profile or a VDSL2 channel alarm profile to the port. **Figure 4-3** provides the configuration flow of a VDSL2 profile.

Figure 4-3 Flowchart for configuring a VDSL2 profile


Flowchart for configuring a line profile
Start
Configure a VDSL2 service profile
Configure a VDSL2 spectrum profile
Configure a VDSL2 UPBO profile
Configure a VDSL2 DPBO profile
Configure a VDSL2 SNR margin profile
Configure a VDSL2 delay INP profile
End
Flowchart for configuring an alarm template
Start
Configure a VDSL2 line alarm profile
Configure a VDSL2 channel alarm profile
Configure a VDSL2 alarm template
End

Procedure

- Configure a VDSL line profile.

  1. Run the **vdsl service-profile quickadd** command to quickly add a VDSL2 service profile, or run the interactive **vdsl service-profile add** command to add a VDSL2 service profile.

     A VDSL2 service profile contains the most common parameters of a VDSL2 line. In general, only the configuration of a VDSL2 service profile is required. In the case of other profiles, adopt the default profiles. Main parameters:

     - **path-mode**: Indicates the path mode. There are two VDSL path modes: ATM mode and PTM mode. By default, the system supports both modes and automatically adapt the path mode according to the modem. You may not configure the path mode. If the modem supports the ATM mode, select **ATM**; if the modem supports the PTM, select **PTM**; if the modem supports both modes and the path mode is set to **Both**, the **PTM** mode is preferred to activate the line.

       NOTE

       For H805VDMF, H805VDRD, H80BVDPE and H80BVDPM boards, only ATM is supported in ADSL mode and only PTM is supported in VDSL mode.

     - **rate**: indicates the line rate. During line activation, a proper rate between the preset maximum rate and minimum rate is determined through automatic negotiation according to the line condition and the profile configuration. The user rate can be restricted by this rate or the rate set in the traffic profile bound to the user. When both rates function, the lower rate is selected as the user rate.

2. Run the **vdsl delay-inp-profile quickadd** command to quickly add a VDSL2 delay INP profile, or run the interactive **vdsl delay-inp-profile add** command to add a VDSL2 delay INP profile. The main parameters are as follows:
   - **bearer1-inp**: The INP is a parameter that describes the line capability of resisting impulse interference. The INP affects the port rate. If the INP is 1, the current channel can resist the impulse noise in 1 DMT character length. The interleave delay is related to the INP. In the fast mode, the INP is meaningless.
   - **bearer1-interleaved-delay**: A zero interleave delay corresponds to the fast mode. In the fast mode, the interleave delay is short, but the error correction capability is weak. A non-zero interleave delay corresponds to the interleave mode. The longer the interleave delay, the greater the interleave depth. In the interleave mode, the greater the interleave depth, the stronger the error correction capability, but the longer the delay.
3. Run the **vdsl noise-margin-profile quickadd** command to quickly add a VDSL2 SNR margin profile, or run the interactive **vdsl noise-margin-profile add** command to add a VDSL2 SNR margin profile. The main parameters are as follows:

   snr-margin: indicates the SNR margin. It refers to the remaining space for carrying noise, except the space for carrying signals. In general, the SNR margin of the minimum tone is used as the SNR margin of the entire VDSL2 connection.
4. Run the **vdsl spectrum-profile quickadd** command to quickly add a VDSL2 spectrum profile, or run the interactive **vdsl spectrum-profile add** command to add a VDSL2 spectrum profile. The main parameters are as follows:

   transmode: indicates the line transmission mode. By default, the system supports all transmission modes. The default setting can be used. Then, the system automatically adapts to the transmission mode of the peer end.
5. Run the **vdsl upbo-profile quickadd** command to quickly add a VDSL2 UPBO profile, or run the interactive **vdsl upbo-profile add** command to add a VDSL2 UPBO profile.
6. Run the **vdsl dpbo-profile quickadd** command to quickly add a VDSL2 DPBO profile, or run the interactive **vdsl dpbo-profile add** command to add a VDSL2 DPBO profile.

- Configure a VDSL2 alarm template.
  1. Run the **vdsl alarm-profile quickadd** command to quickly add a VDSL2 line alarm profile, or run the interactive **vdsl alarm-profile add** command to add a VDSL2 line alarm profile.
  2. Run the **vdsl channel-alarm-profile quickadd** command to quickly add a VDSL2 channel alarm profile, or run the interactive **vdsl channel-alarm-profile add** command to add a VDSL2 channel alarm profile.
  3. Run the **vdsl alarm-template quickadd** command to quickly add a VDSL2 alarm template, or run the interactive **vdsl alarm-template add** command to add a VDSL2 alarm template.

     After the VDSL2 line template is configured, VDSL2 ports can be bound to the profile.

----End

Example

Assume that:

- Path mode: PTM mode
- Downstream minimum reserved rate: 4096 kbit/s
- Channel mode: interleave mode
- Downstream maximum interleave delay: 8 ms
- Upstream minimum interleave delay: 2 ms
- SNR margin: 6 dB
- Downstream minimum INP: 4
- Upstream minimum INP: 2

To add VDSL2 profile 3 with these parameters, do as follows:

```
huawei(config)#vdsl service-profile 3 quickadd path-mode ptm bearer1-rate 512
 4096 8192 128 128 128 100000 128
huawei(config)#vdsl delay-inp-profile quickadd 3 bearer1-interleaved-delay 8 2
bearer1-inp 4 2
huawei(config)#vdsl noise-margin-profile quickadd 3 snr-margin 60 0 100 60 0
100
```

Configuring xDSL Profiles (TR165 Mode)

This topic describes how to configure various xDSL profiles in the TR165 mode. The TR165 mode can be used for ADSL2+ and VDSL2 and is compatible with ADSL and ADSL2.

Prerequisites

The ADSL2+ profile mode has been switched to TR165 by running the **switch adsl mode to tr165** command and the VDSL2 profile mode has been switched to TR165 by running the **switch vdsl mode to tr165** command.

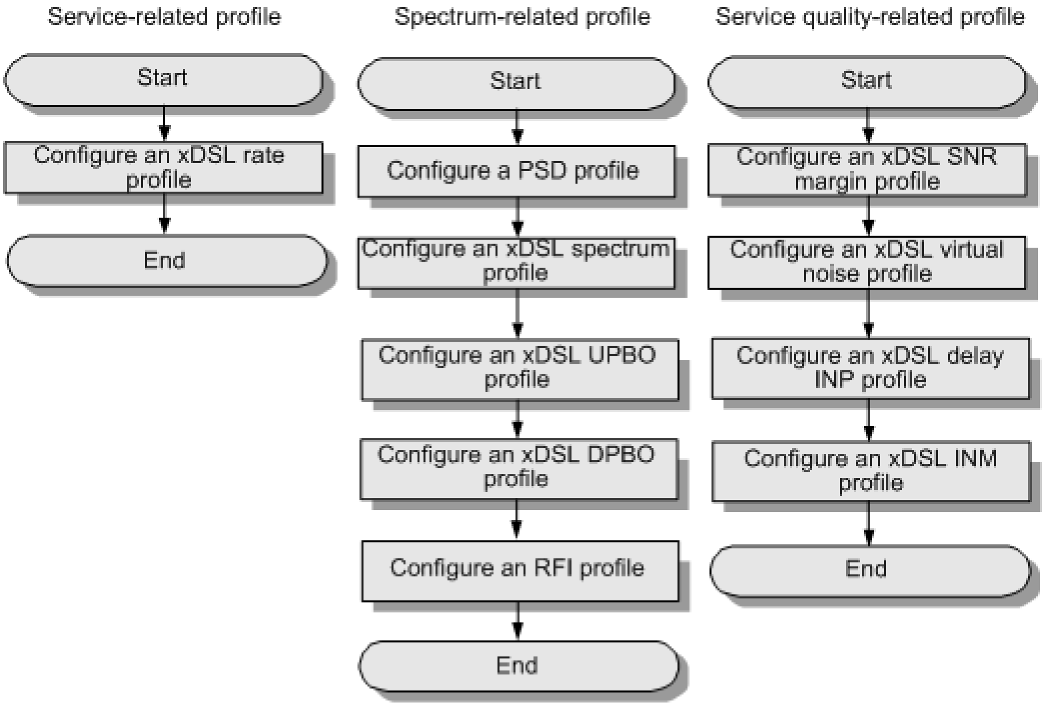
NOTE

When both the ADSL2+ and VDSL2 work in the TR165 mode, a configured profile can be used by both the ADSL2+ and VDSL2; if only one of them works in the TR165 mode, a configured profile is available for only the one in the TR165 mode.

Context

In the TR165 mode, a line profile consists of nine profiles. To activate an xDSL port, nine line configurations must be bound. **Figure 4-4** shows the flow for configuring xDSL profiles.

Figure 4-4 Flowchart for configuring xDSL profiles


Service-related profile
Spectrum-related profile
Service quality-related profile
Start
Configure an xDSL rate profile
End
Start
Configure a PSD profile
Configure an xDSL spectrum profile
Configure an xDSL UPBO profile
Configure an xDSL DPBO profile
Configure an RFI profile
End
Start
Configure an xDSL SNR margin profile
Configure an xDSL virtual noise profile
Configure an xDSL delay INP profile
Configure an xDSL INM profile
End

Procedure

- Configure service-related profiles.
  1. Run the **xdsl data-rate-profile quickadd** command to quickly add an xDSL rate profile, or run the interactive **xdsl data-rate-profile add** command to add an xDSL rate profile.

     A rate profile contains the most common parameters on a xDSL line. The main parameters are as follows:

     - **path mode**: Indicates the path mode. There are two VDSL2 path modes: ATM mode and PTM mode. By default, the system supports both modes and automatically adapt the path mode according to the modem. You may not configure the path mode. If the modem supports the ATM mode, select **ATM**; if the modem supports the PTM, select **PTM**; if the modem supports both modes and the path mode is set to **Both**, the **PTM** mode is preferred to activate the line. The ADSL2 + line works in only the ATM mode.

       NOTE

       - For H805VDMF, H805VDRD, H80BVDPE and H80BVDPM boards, only ATM is supported in ADSL mode and only PTM is supported in VDSL mode.
       - The **path mode** in the upstream and downstream data-rate-profiles bound to a port must be the same.
     - **rate**: Indicates the line rate. During line activation, an appropriate rate between the preset maximum rate and minimum rate is automatically negotiated according to the line condition and profile configuration. The user rate can be restricted by this rate or the rate preset in the traffic profile bound to the user. When both rates function, the user rate adopts the smaller value.
- Configure service quality-related profiles.

1. Run the **xdsl noise-margin-profile quickadd** command to quickly add an xDSL SNR margin profile, or run the interactive **xdsl noise-margin-profile add** command to add an xDSL SNR margin profile. The main parameters are as follows:

   snr-margin: Indicates the SNR margin. It is the remaining space for carrying noise, except the space for carrying signals. The SNR margin of the minimum tone is generally considered as the SNR margin of the entire xDSL connection.
2. Run the **xdsl virtual-noise-profile quickadd** command to quickly add an xDSL virtual noise profile, or run the interactive **xdsl virtual-noise-profile add** command to add an xDSL virtual noise profile.
3. Run the **xdsl inp-delay-profile quickadd** command to quickly add an xDSL delay INP profile, or run the interactive **xdsl inp-delay-profile add** command to add an xDSL delay INP profile. The main parameters are as follows:
   - **impulse noise protection**: Indicates the impulse noise protection. The INP is a parameter that describes the line capability of resisting impulse interference. The INP affects the port rate. INP = 1 indicates that the current channel can resist the pulse noise with 1 DMT character length. The interleave delay is relevant to the INP. In the fast mode, the INP is meaningless.
   - **interleaving delay**: Indicates the interleave delay. A zero interleave delay corresponds to the fast mode. In the fast mode, the interleave delay is short, but the error correction capability is weak. A non-zero interleave delay corresponds to the interleave mode. The longer the interleave delay, the greater the interleave depth. In the interleave mode, the greater the interleave depth, the stronger the error correction capability, but the larger the delay.
4. Run the **xdsl inm-profile quickadd** command to quickly add an xDSL impulse noise monitor profile or run the interactive **xdsl inm-profile add** command to add an xDSL pulse noise monitor profile. The main parameters are as follows:
   - **INM inter arrival time offset**: indicates the INM inter-arrival time offset (INMIATO). It determines the INMAIATi histogram parameter range with INMIATS. It also determines the start point of IAT.
   - **INM inter arrival time step**: indicates the INM inter-arrival time step (INMIATS). It determines the INMAIATi histogram parameter range with INMIATO. It also determines the precision of IAT.
   - **INM cluster continuation value**: indicates the INM cluster continuation (INMCC) value. It identifies a cluster and indicates the maximum number of consecutive undamaged DMT symbols allowed in a cluster.
   - **INM equivalent INP mode**: Indicates the INM equivalent impulse noise protection (INP) mode. The method of calculating the equivalent INP varies according to the mode. Mode 3 is recommended because the algorithm for the mode is better than the algorithms for modes 0, 1, and 2.

- Configure spectrum-related profiles.
  1. Run the **xdsl mode-specific-psd-profile quickadd** command to quickly add an xDSL-related PSD profile, or run the interactive **xdsl mode-specific-psd-profile add** command to add an xDSL-related PSD profile.
  2. Run the **xdsl line-spectrum-profile quickadd** command to quickly add an xDSL spectrum profile, or run the interactive **xdsl line-spectrum-profile add** command to add an xDSL spectrum profile. The main parameters are as follows:

   - **transmode**: Indicates the line transmission mode. By default, the system supports all transmission modes. This parameter can adopt the default value for automatic adaptation.
   - **mode specific PSD profile index**: Indicates the PSD profile index. It specifies the index of the PSD profile to be used.
3. Run the **xdsl upbo-profile quickadd** command to quickly add an xDSL UPBO profile, or run the interactive **xdsl upbo-profile add** command to add an xDSL UPBO profile.
4. Run the **xdsl dpbo-profile quickadd** command to quickly add an xDSL DPBO profile, or run the interactive **xdsl dpbo-profile add** command to add an xDSL DPBO profile.
5. Run the **xdsl rfi-profile quickadd** command to quickly add an xDSL RFI profile, or run the interactive **xdsl rfi-profile add** command to add an xDSL RFI profile.

----End

Example

The data is planned as follows:

- Channel mode: PTM
- Minimum reserved downstream rate: 4096 kbit/s
- Channel mode: interleave
- Maximum downstream interleave delay: 8 ms
- Maximum upstream interleave delay: 2 ms
- SNR margin: 6 dB
- Minimum downstream INP: 4
- Minimum upstream INP: 2

To add xDSL profiles with index 3, do as follows:

```
huawei(config)#xdsl data-rate-profile quickadd 3 path-mode 2 rate 4096 4096 4096
4096 4096 4096
huawei(config)#xdsl inp-delay-profile quickadd 3 interleaved-delay 8 2
huawei(config)#xdsl noise-margin-profile quickadd 3 snr-margin 6 6 6 6 6 6
```

4.2 Creating a VLAN

Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see **Table 4-4**.

Table 4-4 VLAN planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN type: smart
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S +C.	
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	

Default Configuration

Table 4-5 lists the default parameter settings of VLAN.

Table 4-5 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart VLAN	You can run the **defaultvlan modify** command to modify the VLAN type but cannot delete the VLAN.
Reserved VLAN of the system	VLAN ID range: 4079-4093	You can run the **vlan reserve** command to modify the VLAN reserved by the system.

Prerequisite

- The VLAN to be added should not exist in the system.
- Service VLAN cannot be reserve VLAN.

Procedure

Step 1 Create a VLAN.

Run the **vlan** to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 4-6 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the **vlan** ***vlanid*** **standard** command.	Standard VLAN. Ethernet ports in a standard VLAN are interconnected with each other but Ethernet ports in different standard VLANs are isolated from each other.	Only available to Ethernet ports and specifically to network management and subtending.
Smart VLAN	To add a smart VLAN, run the **vlan** ***vlanid*** **smart** command.	One VLAN may contain multiple xDSL service ports or xPON service ports. The traffic streams of these ports, however, are isolated from each other. In addition, the traffic streams of different VLANs are also isolated. One smart VLAN provides access for multiple users and therefore saves VLAN resources.	Smart VLANs can be applied in residential communities to provide xDSL or xPON service access.
MUX VLAN	To add a MUX VLAN, run the **vlan** ***vlanid*** **mux** command.	One MUX VLAN contains only one xDSL service port or xPON service port. The traffic streams in different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. Hence, a MUX VLAN can identify an access user.	MUX VLANs are applicable to xDSL or xPON service access. For example, MUX VLANs can be used to distinguish users.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Super VLAN	To add a super VLAN, run the **vlan** ***vlanid*** **super** command.	The super VLAN is based on Layer 3. One super VLAN contains multiple sub-VLANs. Through an ARP proxy, the sub-VLANs in a super VLAN can be interconnected at Layer 3.	Super VLANs save IP addresses and improve the utilization of IP addresses. For a super VLAN, sub-VLANs must be configured. You can run the **supervlan** command to add a sub-VLAN to a specified super VLAN. A sub-VLAN must be a smart VLAN or MUX VLAN.

NOTE

- To add VLANs with consecutive IDs in batches, run the **vlan** ***vlanid*** **to** ***end-vlanid*** command.
- To add VLANs with inconsecutive IDs in batches, run the **vlan** ***vlan-list*** command.

----End

Example

Create VLAN 50 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 50 smart
```

Create VLAN 55-60 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 55 to 60 smart
```

Create VLAN 65, 73 and 52 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 65,73,52 smart
```

4.3 Configuring an Upstream Port

The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.

Prerequisites

The planned virtual local area network (VLAN) is already configured.

Procedure

Step 1 Configure an upstream port for the VLAN.

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

Step 2 Configure the attribute of the upstream port.

If the default attribute of the upstream port does not meet the requirement for interconnection of the upstream port with the upper-layer device, you need to configure the attribute. For configuration details, see **2.5 Configuring the Attributes of an Upstream Ethernet Port**.

Step 3 (Optional) Configure redundancy backup for the uplink.

To ensure reliability of the uplink, two upstream ports must be available. That is, redundancy backup of the upstream ports needs to be configured. For details, see **14.1 Configuring Ethernet Link Aggregation**.

----End

Example

Assume that the 0/19/0 and 0/19/1 upstream ports are to be added to VLAN 50. The 0/19/0 and 0/19/1 need to be configured into an aggregation group for double upstream accesses. For the two upstream ports, the working mode is full-duplex (full) and the port rate is 100 Mbit/s. To configure such upstream ports, do as follows:

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#duplex 0 full
huawei(config-if-giu-0/19)#duplex 1 full
huawei(config-if-giu-0/19)#speed 0 100
huawei(config-if-giu-0/19)#speed 1 100
huawei(config-if-giu-0/19)#quit
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

4.4 (Optional) Configuring Line Bonding

To increase the network bandwidth of a user, you can bind multiple ports together.

Prerequisites

No traffic is carried on the ports to be bonded.

Context

The purpose of line bonding is to aggregate the services on multiple links to meet the high bandwidth requirement of a single user. The following types of line bonding are supported:

- ADSL2+ port bonding: Adds two ADSL2+ ports on the same board into a bonding group. The operations on an ADSL2+ bonding group are performed on the primary port in the group. Currently, the ATM-based bonding is supported: It complies with ITU-T G998.1, which defines an xDSL access bonding based on the ATM traffic stream.
- VDSL2 port bonding: Adds two VDSL2 ports on the same board into a bonding group. The operations on a VDSL2 bonding group are performed on the primary port in the group.
- SHDSL port bonding.
  - EFM bonding: applicable to the board whose chipset works in the PTM mode.
  - M-pair bonding: applicable to the board whose chipset works in the ATM mode.
- IMA bonding: The Inverse Multiplexing for ATM (IMA) is a kind of technology used to demultiplex an ATM cell flow into multiple low-speed links, while multiplex and reassemble the cell flow at the far end.

Procedure

- Configuring the ADSL2+/VDSL2 line bonding.

  When the bandwidth of an ADSL2+/VDSL2 line cannot meet the actual user requirements, bind multiple lines to increase bandwidth.

  1. In global config mode, run the **xdsl bonding-group-profile add** command to create a bonding group profile and configure line parameters in the profile.
  2. Run the **bonding-group add** command to add a bonding group.

     NOTE

     - When a bonding group is enabled, its member ports must exist.
     - When a bonding group is enabled, a SELT or DELT test cannot be performed on any port in the bonding group.
     - When a bonding group is enabled, loopback cannot be set to any port in the bonding group.
     - A bonding group to be deleted must be in the disabled state.

     Table 4-7 Boards that support bonding

Board	Ports to Be Added to a Bonding Group	Bonding Specification	Bonding Mode
ADPD, ADQD, ADPE, and CAME	Two adjacent ports 2n and 2n + 1 (n = 0, 1, 2, ...) can be added to a bonding group, and any of the two ports can be the primary port. Only two bonding groups can be configured inside a chipset that has four consecutive ports.	2-pair	ADSL ATM
VDMF and VDRD	Two adjacent ports 2n and 2n + 1 (n = 0, 1, 2, ...) can be added to a bonding group, and any of the two ports can be the primary port. Only two bonding groups can be configured inside a chipset that has four consecutive ports.	2-pair	VDSL PTM
VCMM, VDPE, and VDPM	Any two ports 2n and 2m + 1 (n = 0, 1, 2, ...; m = 0, 1, 2, ...) can be added to a bonding group, and only port 2n can be the primary port.	2-pair	VDSL PTM

  3. Run the **bonding-group link add** command to add member ports to the bonding group.
  4. Run the **active bonding-group** command to enable the bonding group and specify its bonding group profile.
  5. Run the **display bonding-group** command to query the bonding group information.
  6. Run the **display bonding-group operation** to query the bonding group operation information.

- Configure the SHDSL line bonding.

  When the bandwidth of an SHDSL line cannot meet the actual user requirements, bind multiple lines to increase bandwidth.

  1. In the global config mode, run the **interface shl** command to enter the SHDSL mode.
  2. Run the **port bind m-pair** command to configure the SHDSL M-pair bonding. Run the **port bind efm** command to configure the SHDSL EFM M-pair bonding.

     NOTE

     - Inter-chip bonding is not supported. On an SHDSL board, ports 0-3 share one chip, ports 4-7 share one chip, ports 8-11 share one chip, and ports 12-15 share one chip. The ports to be bonded must be activated at the same time and must use the same line profile.
     - Different line profiles can be applied to the ports in an EFM bonding group. When one port goes offline, the status of the entire binding group remains unchanged.
     - When the SHDSL board supports G.SHDSL.bis (including the extended standard annex F), 1-pair bonding, 2-pair bonding, 3-pair bonding, and 4-pair bonding are supported, corresponding to the maximum available bandwidth of 5696 x M (M is the pair number; M is 1, 2, 3, or 4.) kbit/s. When the SHDSL board supports only G.991.2 (version 1), 2-pair bonding and 4-pair bonding are supported.
     - After ports are bonded, all operations must be performed on the primary port.
     - To delete a bonding group, only the ID of the primary port can be input.
- Configuring IMA bonding.
  1. In the global config mode, run the **interface shl** command to enter the SHDSL mode.
  2. Run the **ima group add** command to create an IMA group.
  3. Run the **ima link add** command to add an IMA link to a specified IMA group.
  4. Run the **display ima config** command to query the IMA configuration of a board.

  NOTE

  - Only the H80ASHLM board supports the function currently.
  - Parameters of the local IMA group must be the same as those of the peer IMA group.
  - When the IMA groups at both ends are interconnected, ensure that the clock of one IMA group is the system clock and the clock of other IMA group is the line clock. When an IMA group is created, its default clock is the system clock. You can run the **ima group mode clockmode** command to change the clock.
  - When an IMA group is created, its scramble function is disabled by default. You can run the **ima group mode scramble** command to enable the scramble function.
  - If the deleted IMA group includes the IMA link, this link will be deleted simultaneously.

----End

Example

Assume that ADSL2+ ports 0/2/0 and 0/2/1 are added to bonding group 1, with the discovery code 0100-0011-0110. The primary port is port 0/2/0. Profile **huawei** is bound to bonding group 1. In the profile, the upstream and downstream maximum interleave delay is 16, the upstream and downstream minimum impulse noise protection (INP) is 2, the upstream and downstream minimum transmission rate is 64, the upstream and downstream maximum transmission rate is 200000, the upstream and downstream target rate is 20000, the upstream and downstream rate threshold is 20000, and the rate threshold-crossing alarm is enabled. To achieve the preceding configurations, do as follows:

```
huawei(config)#xdsl bonding-group-profile add delay 16 16 inp 2 2 rate 64 200000
 20000 20000 64 200000 20000 20000 monitoring-switch enable name huawei
huawei(config)#bonding-group add 1 primary-port 0/2/0 scheme atm peer-scheme atm
```

```
 discovery-code 0100-0011-0110
huawei(config)#bonding-group link add 1 0/2/1
huawei(config)#active bonding-group 1 profile-name huawei
```

To create IMA group 18, and add IMA link 10 to IMA group 18, do as follows:

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#ima group add 18 version1.0 2 2 itc 255 128 2 3 3
huawei(config-if-shl-0/3)#ima link add 18 10
```

4.5 Configuring an xDSL Port

An xDSL port can transmit services only when it is activated. This topic describes how to activate an xDSL port and bind an xDSL profile to the port.

Prerequisites

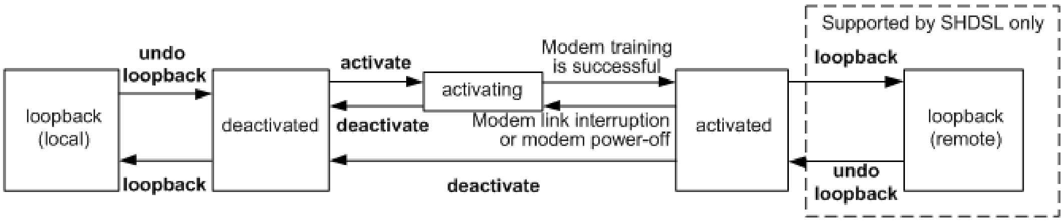
An xDSL profile is created based on the data plan.

- **Configuring an ADSL2+ Template**
- **Configuring SHDSL Profiles**
- **Configuring VDSL2 Profiles (TR129 Mode)**
- **Configuring VDSL2 Profiles (TI Mode)**
- **Configuring xDSL Profiles (TR165 Mode)**

Context

- Activating (or activation) refers to the training between the xTU-C and the xTU-R. During the training process, the system checks the line distance and conditions and performs a negotiation between the xTU-C and the xTU-R to determine whether the port can work under the conditions as preset in the line profile, such as upstream and downstream line rates and noise margin.
- If the training is successful, the communication connection is set up between the xTU-C and the xTU-R, and the devices are ready for service transmission. This state is called the activated state of a port. That is, services can be transmitted between the xDSL port and the xTU-R.
- If the xTU-R is online (powered on), the activating process is completed after the training is successful. If the xTU-R is offline (powered on), the communication connection that is set up during activation is terminated, and the xTU-C is in the listening state. When the xTU-R goes online again, the training process begins automatically. When the training is successful, the port is activated.
- An xDSL port may be in the activating, activated, deactivated, or loopback state. **Figure 4-5** shows the inter-conversion between xDSL port states.

Figure 4-5 Inter-conversion between xDSL port states



NOTE

By default, the xDSL port is disconnected from the modem and is in the activating state. To bind an xDSL port to an xDSL profile, deactivate the port first.

Procedure

- Configure an asymmetric digital subscriber line 2 plus (ADSL2+) user port.
  1. Run the **interface adsl** command to enter the ADSL mode.
  2. Activate an ADSL2+ port and bind a profile to the port.
     - In common ADSL mode (RFC2662 mode), run the **activate** command to activate the ADSL2+ port and bind the port to an ADSL2+ line configuration profile.
     - In NGADSL mode (RFC4706 mode), run the **activate** command to activate the ADSL2+ port and bind the port to the ADSL2+ line template.
     - In ADSL TR165 mode, run the **activate** command to activate the ADSL2+ port and bind the port to an ADSL2+ profile.
  3. Run the **alarm-config** command to bind an alarm template to the port.
- Configure a single-pair high-speed digital subscriber line (SHDSL) user port.
  1. Run the **interface shl** command to enter the SHDSL mode.
  2. Run the **activate** command to activate an SHDSL port and bind an SHDSL line profile to the port.
  3. Run the **alarm-config** command to bind an alarm profile to the port.
- Configure a very-high-speed digital subscriber line 2 (VDSL2) user port.
  1. Run the **interface vdsl** command to enter the VDSL mode.
  2. Activate a VDSL port and bind a profile to the port.
     - In common mode (TR129 mode), run the **activate** command to activate a VDSL2 port and bind a VDSL2 line template to the port.
     - In TI mode, run the **activate** command to activate a VDSL2 port and bind profiles to the port.
     - In TR165 mode, run the **activate** command to activate a VDSL2 port and bind profiles to the port.
  3. In common mode, run the **alarm-config** command to bind the VDSL2 port to the line alarm template.

----End

Example

To activate ADSL2+ port 0/2/0 and bind line template 2 and alarm template 2 to the port, do as follows:

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 2
huawei(config-if-adsl-0/2)#alarm-config 0 2
```

To activate SHDSL port 0/3/0 and bind line profile 2 and alarm profile 2 to the port, do as follows:

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 0
huawei(config-if-shl-0/3)#activate 0 2
huawei(config-if-shl-0/3)#alarm-config 0 2
```

In common VDSL mode, to activate VDSL2 port 0/4/0 and bind line template 2 and alarm template 2 to the port, do as follows:

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 0
huawei(config-if-vdsl-0/4)#activate 0 template-index 2
huawei(config-if-vdsl-0/4)#alarm-config 0 2
```

In TR165 mode, to activate ADSL2+ port 0/4/0 and bind DPBO profile 3, downstream rate profile 3, INP profile 3, and alarm profile 2 to the port, do as follows:

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 0
huawei(config-if-vdsl-0/4)#activate 0 prof-idx dpbo 3 ds-rate 3 inm 3 inp-delay 3
huawei(config-if-vdsl-0/4)#alarm-config 0 2
```

4.6 Creating an xDSL Service Port

A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

Context

A service flow can carry a single service or multiple services. A multi-service flow is generally used in the triple play service. A service port can carry a single service flow or multiple service flows. The MA5600T/MA5603T can differentiate users or services based on the following modes if a service port carries multiple service flows:

- Based on the user virtual local area network (VLAN).
- Based on the user packet encapsulation type. For example, the encapsulation type of the dialup Internet service packet is Point-to-Point Protocol over Ethernet (PPPoE), and the encapsulation type of the multicast service packet is Internet Protocol over Ethernet (IPoE).
- Based on VLAN+user packet priority. For example, the priority of multicast services is higher than that of the Internet access service.
- Based on VLAN+user service encapsulation type.

Before creating a service port, run the **display traffic table** command to query whether the expected service port already exists in the system. The system provides seven default traffic profiles. The IDs of these profiles are numbered from 0 to 6.

If an expected service port does not exist in the system, run the **traffic table ip** command to create a traffic profile based on site requirements. For details about how to configure a traffic profile, see **17.3.12 Configuring VAGs**.

Table 4-8 lists the default settings of a service port.

Table 4-8 Default settings of a service port

Parameter	Default Setting
Traffic profile ID	0-6
Administration status	Activated

Parameter	Default Setting
Maximum number of learnable MAC addresses	255

Procedure

Step 1 Create service ports.

You can choose to create a single service port or multiple service ports in batches according to requirements.

- Run the **service-port** command to create a service port.
  - Single-service service ports:

    Select **single-service** or do not input **multi-service** to create a single-service service port.
  - Multi-service service port based on the user-side VLAN:

    Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** | **other-all** }.
    - **untagged**: If this parameter is specified, user packets do not carry a tag.
    - *user-vlanid*: If this parameter is specified, user packets carry a tag, which is the customer VLAN (C-VLAN).
    - **priority-tagged**: If this parameter is specified, the VLAN tag is 0 and the priorities of user packets range from 0 to 7. (The highest priority is 7.)
    - **other-all**: If this parameter is specified, the created service port carries QinQ transparent LAN service (TLS) services for enterprises. User packets are matched based on the specified user VLAN (or untagged attribute) first. The unmatched packets are transmitted on the TLS service port to the upstream network..
  - By user-side service encapsulation mode

    Select **multi-service user-encap***user-encap* .
  - By VLAN + user-side packet priority (802.1p)

    Select **multi-service user-8021p***user-8021p* [**user-vlan***user-vlanid*].
  - By VLAN + user-side service encapsulation mode (user-encap)

    Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** } **user-encap** *user-encap*.

NOTE

- The system supports creating service ports by index. One index maps one service port and the input of a large number of traffic parameters is not required. Therefore, the configuration of service ports is simplified. During the creation of a service port, *index* indicates the index of the service port and it is optional. If it is not entered, the system starts to allocate an idle index from the currently configured maximum index (regardless of whether it is deleted). After the maximum value range is exceeded, the system searches from 0.
- **vlan** indicates the S-VLAN. An S-VLAN can only be a MUX VLAN or smart VLAN.
- The access mode can be ATM or PTM. In the ATM access mode, the VPI and VCI must be input and must be the same as the VPI and VCI of the access terminal.
- **rx-cttr** is the same as **outbound** in terms of meanings and functions. Either of them indicates the index of the traffic profile from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meanings and functions. Either of them indicates the index of the traffic profile from the user side to the network side.

- Run the **multi-service-port** command to create service ports in batches.

Step 2 (Optional) Run the **service-port desc** command to configure description information about the service port for facilitating maintenance. The information includes the use purpose and application scenario of the service port.

Step 3 (Optional) Run the **service-port *index* adminstatus** command to configure the management status of the service port. A service port is in activated state by default.

A service can be provided for a user only when the physical port connected to the user and the corresponding service port are activated.

Step 4 (Optional) Run the **mac-address max-mac-count service-port** command to configure the maximum number of MAC addresses that can be learned on the service port. This configuration is used to limit the maximum number of PCs that can connect to the Internet using the same account.

----End

Example

To plan data for a household user who accesses the Internet in the ADSL2+ mode, do as follows: The MA5600T/MA5603T provisions the Internet access service with the access rate 3072 kbit/s to the user and up to 2 users can use the same account to access the Internet. The query result shows that the system does not have a proper traffic profile and the user does not open an account. Therefore, the MA5600T/MA5603T does not provide the service to the user currently.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
     (kbps)    (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
huawei(config)#traffic table ip index 8 cir 3072 priority 4 priority-policy loca
```

```
l-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 8
  TD Name              : ip-traffic-table_8
  Priority             : 4
  Copy Priority        : -
  Mapping Index        : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                  : 3072 kbps
  CBS                  : 100304 bytes
  PIR                  : 6144 kbps
  PBS                  : 198608 bytes
  Color policy         : dei
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 3 vlan 100 adsl 0/2/1 vpi 1 vci 35 inbound traffic-
table
 index 8 outbound traffic-table index 8
huawei(config)#mac-address max-mac-count service-port 3 2
huawei(config)#service-port 3 adminstatus disable
```

A household user requests the Internet access service with the access rate 2048 kbit/s. To facilitate service expansion in the future, the MA5600T/MA5603T adopts the ADSL2+ mode to provide the Internet access service, uses CVLAN 10 to identify users, and uses SVLAN 50 to identify services. The query result shows that a proper traffic profile exists in the system. The system needs to provide the Internet access service to the user immediately. Add the description of the service port to facilitate maintenance. To perform these configurations, do as follows:

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
huawei(config)#service-port 4 vlan 50 adsl 0/2/1 vpi 1 vci 39 multi-service
user-vlan 10 inbound traffic-table index 5 outbound traffic-table index 5
huawei(config)#service-port desc 4 description HW_adsl/VlanID:50/uservlan/10
```

A household user requests the Internet access service with the access rate 2048 kbit/s. To facilitate service expansion in the future, the MA5600T/MA5603T adopts the SHDSL mode to provide the Internet access service to the user. The query result shows that a proper traffic profile exists in the system. The system needs to provide the Internet access service to the user immediately. Add the description of the service port to facilitate maintenance. To perform these configurations, do as follows:

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
```

```
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
huawei(config)#service-port 5 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 5 description HW_shdsl/singleservice/VlanID:50
```

A commercial user requests the Internet access service with the access rate 8192 kbit/s. To facilitate service expansion in the future, the MA5600T/MA5603T adopts the VDSL2 mode to provide the Internet access service, uses CVLAN 10 to identify users, and uses SVLAN 50 to identify services. The query result shows that no proper traffic profile exists in the system. The system needs to provide the Internet access service to the user immediately. Add the description of the service port to facilitate maintenance. To perform these configurations, do as follows:

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
     8 3072     100304   6144     198608     4 -                    local-pri
  ---------------------------------------------------------------------------
  Total Num : 8
huawei(config)#traffic table ip index 9 cir 8192 priority 4 priority-policy
 local-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 9
  TD Name              : ip-traffic-table_9
  Priority             : 4
  Copy Priority        : -
  Mapping Index        : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                  : 8192 kbps
  CBS                  : 264144 bytes
  PIR                  : 16384 kbps
  PBS                  : 526288 bytes
  Color policy         : dei
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 6 vlan 50 vdsl mode ptm 0/4/1 multi-service user-vlan
 10 inbound traffic-table index 9 outbound traffic-table index 9
huawei(config)#service-port desc 6 description HW_vdsl/VlanID:50/uservlan:10
```

4.7 (Optional) Configuring the xPoA-xPoE Protocol Conversion

xPoA to xPoE conversion involves the conversion from IP over ATM (IPoA) to IP over Ethernet (IPoE) and the conversion from Point-to-Point Protocol over ATM (PPPoA) to Point-to-Point Protocol over Ethernet (PPPoE). ATM is the abbreviation for asynchronous transfer mode (ATM). xPoA packets cannot be transmitted on an IP network and must be converted into xPoE packets. IPoA packets must be converted into IPoE and PPPoA packets must be converted into PPPoE packets to be transmitted on an IP network. Protocol conversion is required when the packet encapsulation mode is IPoA or PPPoA and is not required when the packet encapsulation mode is IPoE or PPPoE.

Context

The principle of the IPoA protocol is different from that of the PPPoA protocol. In the PPPoA mode, the BRAS automatically allocates a gateway address to the PPPoA user after the PPPoA user passes the authentication on the BRAS and dialup is successful. Therefore, the default gateway address does not need to be configured in the PPPoA mode. IPoA data is forwarded according to the route to the destination IP address and the next hop IP address needs to be configured. Therefore, the default gateway address needs to be configured in the IPoA mode.

Figure 4-6 provides the configuration flow for the xPoA-xPoE protocol conversion.

Figure 4-6 Flowchart for configuring the xPoA-xPoE protocol conversion

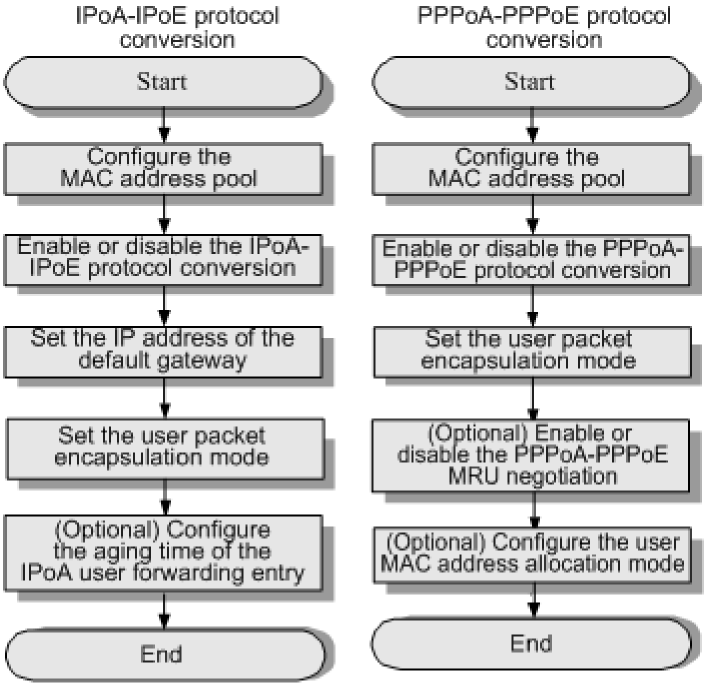

IPoA-IPoE protocol conversion
Start
Configure the MAC address pool
Enable or disable the IPoA-IPoE protocol conversion
Set the IP address of the default gateway
Set the user packet encapsulation mode
(Optional) Configure the aging time of the IPoA user forwarding entry
End
PPPoA-PPPoE protocol conversion
Start
Configure the MAC address pool
Enable or disable the PPPoA-PPPoE protocol conversion
Set the user packet encapsulation mode
(Optional) Enable or disable the PPPoA-PPPoE MRU negotiation
(Optional) Configure the user MAC address allocation mode
End

Table 4-9 lists the default settings of the xPoA-xPoE protocol conversion.

Table 4-9 Default settings of the xPoA-xPoE protocol conversion

Parameter	Default Setting
Maximum number of the MAC addresses in the MAC address pool	256
Status of the IPoA-IPoE protocol conversion	Disabled
Aging time of the IPoA user forwarding entry	1200s
Status of the PPPoA-PPPoE protocol conversion	Disabled
Status of the MRU negotiation function during the PPPoA-PPPoE protocol conversion	Disabled
User MAC address allocation mode for the PPPoA-PPPoE protocol conversion	**Multi-MAC** mode

Procedure

- Configure the IPoA-IPoE protocol conversion.

  A user can access the Internet in the IPoA mode only after the IPoA-IPoE protocol conversion is enabled.

  1. In the global config mode, run the **mac-pool** command to configure the MAC address pool, which is used to allocate source MAC addresses to IPoA users. By default, the number of the MAC addresses in the MAC address pool is 256, which can be changed by setting parameter *scope*.

     The MAC address encapsulated into packets during the IPoA-IPoE protocol conversion is the MAC address allocated to the user from the MAC address pool.
  2. Run the **ipoa enable** command to enable the IPoA-IPoE protocol conversion. By default, the IPoA-IPoE protocol conversion is disabled.
  3. Run the **encapsulation** command to set the user packet encapsulation mode (select **ipoa** as the encapsulation mode).

     NOTE

     - Configure either the **ipoa default gateway** command or the *dstip* parameter in the **encapsulation** command. If the MA5600T/MA5603T works in Layer 2 mode, set the IP address of the upper-layer router as the default gateway. If the MA5600T/MA5603T works in the Layer 3 mode, set the IP address of the Layer 3 interface corresponding to the MA5600T/MA5603T as the default gateway.
     - IPoA encapsulation is not supported in the single-PVC for multiple services application.
     - To switch the encapsulation mode from PPPoA to IPoA, you must change the encapsulation mode to llc bridge first and then perform switching.
  4. Run the **ipoa expire-time** command to set the aging time of the IPoA user forwarding entry. After receiving IPoA packets from users, the device refreshes IPoA forwarding entry for the user. If the IPoA forwarding entry of a user is not refreshed within the aging time, the device does not receive packets from the user and considers that the user has gone offline by default. Therefore, the device will delete the forwarding entry for the user. The default aging time of the IPoA user forwarding entry is 1200s. The default value is recommended.

- Configure the PPPoA-PPPoE protocol conversion.

  A user can access the Internet through the PPPoA dialup only after the PPPoA-PPPoE protocol conversion is enabled.

  1. In the global config mode, run the **mac-pool** command to configure the MAC address pool, which is used to allocate source MAC addresses to PPPoA users. By default, the number of the MAC addresses in the MAC address pool is 256, which can be changed by setting parameter *scope*.

     The MAC address encapsulated into packets during the PPPoA-PPPoE conversion is the MAC address allocated to the user from the MAC address pool.
  2. Run the **pppoa enable** command to enable the PPPoA-PPPoE protocol conversion. By default, the PPPoA-PPPoE protocol conversion is disabled.
  3. Run the **encapsulation** command to set the user packet encapsulation mode (select **pppoa** as the encapsulation mode).

     NOTE

     - PPPoA encapsulation is not supported in the single-PVC for multiple service or QinQ VLAN application.
     - To switch the encapsulation mode from IPoA to PPPoA, you must change the encapsulation mode to llc bridge first and then perform switching.
  4. Run the **pppoa mru** command to enable PPPoA-PPPoE MRU negotiation. By default, the PPPoA-PPPoE MRU negotiation is disabled. To avoid fragment and regrouping of the PPPoA packets, enable the MRU negotiation function. Enable or disable the PPPoA-PPPoE MRU negotiation according to the packet processing conditions.
     - When the MRU negotiation is disabled, the PC initiates the PPPoE connection and negotiates according to the 1492-byte MRU. In this case, packets need to be segmented and reassembled.
     - When the MRU negotiation is enabled, the MA5600T/MA5603T identifies the PPPoA-PPPoE converted packets, adds a tag to the packets and then sends them to the upper-layer BRAS. Then, the BRAS negotiates with the CPE according to the 1500-byte MRU. In this way, the MTU between the CPE and the BRAS is equal to the standard Ethernet MTU. In this case, the packets do not need to be segmented or reassembled.
  5. Run the **pppoa mac-mode** command to set the user MAC address allocation mode for the PPPoA-PPPoE protocol conversion. By default, the user MAC address allocation mode is the **multi-mac** mode. The **single-mac** mode can improve security. Select this mode according to the MAC address allocation mode of PPPoA users.
     - In the multi-MAC allocation mode (the **multi-mac** mode), PPPoE users are authenticated on the BRAS using their respective MAC addresses, and PPPoA users are allocated different MAC addresses and are authenticated on the BRAS using these MAC addresses as source MAC address.
     - In the single-MAC allocation mode (the **single-mac** mode), the system replaces the MAC address of each PPPoE user with the MAC address of the corresponding board, and allocates the same MAC address to all PPPoA users.

----End

Example

The MA5600T/MA5603T works in Layer 2 mode, the default gateway is the same as the IP address of the upper-layer router, which is 10.1.1.1, and the IPoA service encapsulation mode is LLC. To enable the IPoA-IPoE conversion with the start MAC address 0000-0000-0001 in the MAC address pool that contains 200 MAC addresses, do as follows:

```
huawei(config)#mac-pool xpoa 0000-0000-0001 200
huawei(config)#ipoa enable
huawei(config)#ipoa default gateway 10.1.1.1
huawei(config)#encapsulation 0/2/1 vpi 0 vci 35 type ipoa llc srcIP 10.1.1.20
```

The PPPoA service encapsulation mode is LLC, and, to improve security, the user MAC address allocation mode is the single-MAC mode. To enable the PPPoA-PPPoE protocol conversion with the start MAC address 0000-1010-1000 in the MAC address pool that contains 200 MAC addresses, do as follows:

```
huawei(config)#mac-pool xpoa 0000-1010-1000 200
huawei(config)#pppoa enable
huawei(config)#encapsulation 0/2/1 vpi 0 vci 35 type pppoa llc
huawei(config)#pppoa mac-mode single-mac
```

4.8 (Optional) Configuring the VDSL2 Vectoring Function

This topic describes how to configure the vectoring function on a very-high-speed digital subscriber line 2 (VDSL2). This technology can greatly cancel the far-end crosstalk (FEXT) on a VDSL2 line and increases VDSL2 rates.

Prerequisites

This feature requires hardware support. For details about the hardware support, see feature description Vectoring Feature Dependency and Limitation .

Context

- The vectoring technology uses vectoring groups to jointly transmit signals in the downstream direction and receive signals in the upstream direction of a VDSL2 line.
- The crosstalk on a VDSL2 line mainly comes from other lines in a bundle. Based on the collected crosstalk values (which are vectoring information), an access device performs matrix calculation and outputs vectored crosstalk cancellation signals.
- It is recommended that the vectoring technology applies to fiber to the building (FTTB) and fiber to the curb (FTTC) scenarios to increases VDSL2 rates, because this technology has the best effect in increasing rates on a VDSL2 line of 1000 meters or shorter.
- The crosstalk among lines in a bundle is large. It is recommended that you set the lines in a bundle to vectoring group members.

Table 4-10 describes the default settings of the vectoring function.

Table 4-10 Default settings of the vectoring function

Parameter	Default Settings
Global vectoring function	Disable
Global bandplan	998ade for bandplan type and type-a for US0 type

Parameter	Default Settings
Activation policy for vectoring legacy CPEs (CPE is the abbreviation for customer premises equipment. A vectoring legacy CPE is a CPE that does not support the vectoring function.)	Limit
Default vectoring group ID	1 **NOTE** ● The system supports only one vectoring group 1, which is used to cancel the crosstalk on all frequency bands of a VDSL2 line. The system currently does not support modification of a vectoring group. ● The system adds all VDSL2 ports to vectoring group 1 by default.
Default vectoring profile ID	1
Upstream crosstalk cancellation function specified in vectoring profile 1	Enable
Downstream crosstalk cancellation function specified in vectoring profile 1	Enable

Procedure

Step 1 Run the **xdsl vectoring bandplan-type** command to set global bandplan type.

- As required by the vectoring algorithm, the upstream and downstream frequency bands cannot have duplicate bands in the entire system. Therefore, the bandplan type must be configured globally.
- The global vectoring bandplan type can be used only when the global vectoring function is not enabled.
- After the vectoring function is enabled globally, if the bandplan in the line profile bound to a VDSL2 port is not compatible with the globally configured bandplan, the upstream and downstream frequency bands have duplicate bands, the port cannot be activated.

Step 2 (Optional) Run the **xdsl vectoring legacy-cpe activate-policy** command to configure the vectoring legacy CPE activation policy.

If a vectoring legacy CPE (supporting G.993.2 and not supporting G.993.5) that is activated in G.993.2 mode is connected to a vectoring-enabled device, the crosstalk produced by this CPE to other VDSL2 lines cannot be canceled, affecting the vectoring performance in the entire system. To minimize the impact, set the vectoring legacy CPE activation policy based on site requirements.

Step 3 Run the **xdsl vectoring enable** command to enable the global vectoring function.

----End

Example

Assume that a device uses default bandplan values (998ade for bandplan type and type-a for US0 type). In addition, the vectoring legacy CPE activation policy is auto. To configure the vectoring function for the device as above, do as follows:

```
huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
uawei(config)#xdsl vectoring legacy-cpe activate-policy auto
huawei(config)#xdsl vectoring enable
```

5 Configuring the GPON Internet Access Service (Distributed Mode)

About This Chapter

The Internet access service in GPON access resolves the bandwidth bottleneck and long-distance coverage problems that occur in twisted-pair access and meets the requirements for high bandwidth services.

Application Context

GPON is mainly used in the FTTx solution. The FTTx technology is mainly used for adopting optical network in the access network. Its coverage is from the CO device of the regional telecommunications room to the subscriber terminal. The optical line terminal (OLT) functions as the CO device. The optical network unit (ONU) or the optical network terminal (ONT) functions as the subscriber terminal.

- FTTH refers to fiber to the home. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the ONT at lower layer through the ODN. The ONT is connected to subscribers to provide the voice, Internet access, and IPTV services.
- FTTB refers to fiber to the building. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the MDU or ONUs of other types at lower layer through the ODN. The ONU or MDU is connected to subscribers. FTTB can be further classified into FTTB+DSL and FTTB+LAN. These two modes respectively use the home gateway with an RJ-11 upstream port and the home gateway with a LAN upstream port to provide the voice, Internet access, and IPTV services.
- FTTC refers to fiber to the curb. FTTC is mainly used to provide services for residential subscribers. The ONU is placed in the cabinet at the curb. It uses coaxial cables to transmit CATV signals or uses twisted pairs to transmit the voice and Internet access services. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the MDU or outdoor cabinets for ONUs of other types at lower layer through the ODN. The ONU or MDU is connected to subscribers. FTTC and FTTB are the same in configuration and differ from each other only in the networking mode.
- FTTO refers to fiber to the office. The Ethernet port of the ONU is connected to the LAN of subscribers so that subscribers can be directly connected to the Internet, or connected to the headquarters or branch offices through VPN. In this networking scenario, the

MA5600T/MA5603T functions as an OLT and is connected to the ONU at lower layer through the ODN. The ONU is connected to subscribers to provide the voice, Internet access, IPTV, and private line services.

Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.11 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.
- The GPON ONT profile is already created. **Configuring a GPON ONT Capability Profile**, **Configuring a GPON ONT Alarm Profile** are already completed.
- The GPON mode is already switched to the distributing-mode.

Data Plan

Before configuring the GPON Internet access service, plan the data items as listed in **Table 5-1**.

Table 5-1 Data plan for the GPON Internet access service

Item	Data	Remarks
MA5600T / MA5603T	Access rate	Configure the data according to the user requirements.
	Access port	Configure the data according to the network planning.
	VLAN planning	The cooperation with the upper-layer device should be considered in the VLAN planning. The upstream VLAN must be the same as that of the upper-layer device.
	QoS policy	Configure the data according to the QoS policy of the entire network. Generally, the priority of the Internet access service is lower than the priorities of the voice and video services.
	T-CONT ID	It is recommended that you do not use T-CONT 0 to transmit services.
	GEM port index	-
ONT	Capability set profile	The ONT capability set profile must be the same as the actual capacity set.

Item	Data	Remarks
	ONT index	GPON supports a split ratio of up to 1:128. You need to plan the ONTs connected to the MA5600T/ MA5603T to facilitate management.
	Authentication mode	The password, SN, and LOID +CHECKCODE can be used for authentication.
Upper-layer LAN switch	The LAN switch transparently transmits the service packets of the MA5600T/MA5603T on Layer 2. The VLAN ID must be the same as the upstream VLAN ID of the MA5600T/ MA5603T.	-
BRAS	The BRAS performs the related configurations according to the authentication and accounting requirements for dialup users, for example, configures the access user domain (including the authentication scheme, accounting scheme, and authorization scheme bound to the domain) and specifies the RADIUS server. If the BRAS is used to authenticate users, you need to configure the user name and the password for each user on the BRAS. If the BRAS is used to allocate IP addresses, you need to configure the corresponding IP address pool on the BRAS.	-

Procedure

1. 5.1 Configuring the GPON ONT Profile
   In the distributed mode, GPON ONT profiles include the GPON ONT capability profile and the GPON ONT alarm profile. This topic describes how to configure these profiles.
2. 5.2 Creating a VLAN
   Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.
3. 5.3 Configuring an Upstream Port
   The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.
4. 5.4 Configuring a GPON ONT

The MA5600T/MA5603T provides end users with services through the ONT. The MA5600T/MA5603T can manage the ONT and the ONT can work in the normal state only after the channel between the MA5600T/MA5603T and the ONT is available.

5. 5.5 Configuring a GPON Port
   To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.
6. 5.6 Creating a GPON Service Port
   A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

5.1 Configuring the GPON ONT Profile

In the distributed mode, GPON ONT profiles include the GPON ONT capability profile and the GPON ONT alarm profile. This topic describes how to configure these profiles.

Context

GPON ONT profiles contain the parameters required for configuring the GPON access service. Of which,

- The GPON ONT capability profile contains the physical port type and quantity of the ONU, mapping mode from service port to GEM port, and traffic control type.
- The GPON ONT alarm profile provides a series of alarm threshold parameters that are used for performance measurement and monitoring of activated ONU lines. After a GPON alarm profile is bound to an ONU, the ONU sends alarms to the log host and the NMS if the performance statistics of the line exceed the threshold that is specified in the profile.

NOTE

- In this document, MDU and ONT are called ONU collectively.
- The description in this topic is based on the GPON distributed mode. You can query the current GPON mode in the diagnose mode.

```
huawei(config)#diagnose
huawei(diagnose)%%display xpon mode
  --------------------------------------------------
        Current config mode: Distributing-mode
  --------------------------------------------------
```

5.1.1 Configuring a DBA Profile

A DBA profile defines the traffic parameters of xPON and can be bound to a T-CONT dynamically allocate the bandwidth and improve the usage of the upstream bandwidth.

Default Configuration

Table 5-2 lists the default settings of the DBA profiles.

Table 5-2 Default settings of the DBA profiles

Parameter	Default Setting	Remarks
Default DBA profile ID in the system	0-9	You can run the **display dba-profile all** command to query the parameter values of each default DBA profile.

Procedure

Step 1 Add a DBA profile.

Run the **dba-profile add** command to add a DBA profile.

NOTE

- By default, T-CONT is not bound to any DBA profile. Hence, you need to bind a DBA to a T-CONT.
- When you add a DBA profile, the bandwidth value must be a multiple of 64. If you enter a bandwidth value not of a multiple of 64, the system adopts the closest multiple of 64 that is smaller than the value you enter.

Step 2 Query a DBA profile.

Run the **display dba-profile** command to query a DBA profile.

----End

Example

Assume that the name and type of a DBA profile are "DBA_bandwidth" and "type3" respectively, and that the bandwidth required by a user is 100 Mbit/s. To add such a DBA profile, do as follows:

```
huawei(config)#dba-profile add profile-name DBA_100M type3 assure 102400 max
102400
huawei(config)#display dba-profile profile-name DBA_100M
  -----------------------------------------------------------------
  Profile-name :            DBA_100M
  Profile-ID:               10
  type:                     3
  Bandwidth compensation:   No
  Fix(kbps):                0
  Assure(kbps):             102400
  Max(kbps):                102400
  bind-times:               0
  -----------------------------------------------------------------
```

5.1.2 Configuring a GPON ONT Capacity Profile

A GPON ONT capability profile identifies the actual capability of a GPON ONU. After an ONT is added and bound to a GPON ONT capability profile, the ONU carries the corresponding services according to parameters configured in the capability profile.

Context

- All GPON ONUs must be bound to the GPON ONT capability profile. Specify the ONT capability profile when running the **ont add** command to add an ONU offline or running the **ont confirm** command to confirm an automatically discovered ONU.
- Currently, the system provides seven default ONT capability profiles that are solidified in the system. The default profiles cannot be modified. The default profile IDs range from 1-7. The reserved ONT capability profile IDs are 8-16.
- The contents of the capability profile restrict the port number that is used in commands for GEM port mapping, T-CONT/PQ mapping, and the ONT VLAN management.
- The ONT capability profile must be configured according to the actual capability of the ONU. Different the capability profile parameters vary according to different ONUs.

Procedure

Step 1 Run the **ont-profile add** command to configure an ONT capability profile.

When you add an ONT capability profile, if the profile ID is not specified, the system automatically allocates the least idle profile ID; if the profile name is not specified, the system adopts the default name **ont-profile_x**, where, x is the corresponding ONT capability profile ID.

The system supports up to 128 ONT capability profiles.

The system default profiles include the MDU profile and several common ONT (such as OT925, HG850, and HG810) profiles, which can be directly used. It is recommended to manually configure an ONT capability profile only when the default ONT capability profile fails to meet actual requirements.

Step 2 Run the **display ont-profile** command to query the ONT capability profile.

----End

Example

Assume the following parameters: profile ID 30, two POTS ports, four Ethernet ports, mapping mode VLAN ID, and flow control type PQ. To configure such an ONT capability profile for the ONT HG850a and query the capability profile after the configuration is completed, do as follows:

```
huawei(config)#ont-profile add profile-id 30
{ <cr>|profile-name<K> }:

  Command:
          ont-profile add profile-id 30
  Press 'Q' or 'q' to quit input
>  Are you sure you want to set the number of POTS ports to auto-adaptive? (y/n)
 [n]:
>  Number of POTS ports<0-8> [0]:2
>  Are you sure you want to set the number of ETH ports to auto-adaptive? (y/n)
[n]:
>  Number of ETH ports<0-8>  [0]:4
>  TDM port type<1-E1,2-T1> [1]:
>  TDM service type<1-TDMoGEM> [1]:
>  Number of TDM ports<0-8> [0]:
>  Number of MOCA ports<0-8> [0]:
>  Are you sure you want to set the number of CATV UNI ports to auto-adaptive? (
y/n) [n]:
>  Number of CATV UNI ports<0-8> [0]:
>  Mapping mode<1-VLANID, 2-802_1pPRI, 3-VLANID_802_1pPRI, 4-PORTID,
   5-PORTID_VLANID, 6-PORTID_802_1pPRI, 7-PORTID_VLANID_802_1pPRI,
   9-IPTOS, 10-VLANID_IPTOS> [1]:
>  The type of flow control<1-PQ, 2-GEMPORT-CAR, 3-FLOW-CAR> [1]:
  Adding an ONT profile succeeded
  Profile ID  : 30
  Profile name: ont-profile_30
huawei(config)#display ont-profile profile-id 30
  ----------------------------------------------------------------------------
  Profile ID  : 30
  Profile name: ont-profile_30
  ----------------------------------------------------------------------------
  Number of POTS ports:               2
  Number of ETH ports:                4
  TDM port type:                      E1
  TDM service type:                   TDMoGem
  Number of TDM ports:                0
  Number of MOCA ports:               0
  Number of CATV UNI ports:           0
  Mapping mode:                       VLAN ID
  The type of flow control:           PQ
  ----------------------------------------------------------------------------
  Binding times:                      0
  ----------------------------------------------------------------------------
```

5.1.3 Configuring a GPON ONT Alarm Profile

This topic describes how to add an alarm profile, and configure most of the performance parameters for various ONT lines as a profile. After the alarm profile is configured and bound successfully, the ONT can directly use the profile when it is activated.

Context

An ONT alarm profile defines a series of alarm thresholds that are used to monitor the performance of an activated ONT line. When the statistics result of a parameter reaches the alarm threshold, the NE is notified and an alarm is sent to the log server and the NMS.

- The MA5600T/MA5603T supports up to 50 alarm profiles.
- The system contains a default alarm profile with the ID 1. This profile cannot be deleted but can be modified.

Procedure

Step 1 Run the **gpon alarm-profile add** command to add a GPON ONT alarm profile.

All parameters in the default profile are set to 0, which indicates that no alarm is reported. When an alarm profile is created, the default values of all alarm thresholds are 0, which indicates that no alarm is reported.

Step 2 Run the **display gpon alarm-profile** command to query the alarm profile.

----End

Example

To add GPON ONT alarm profile 5, set the alarm threshold for the packet loss of the GEM port to 10, set the alarm threshold for the number of mis-transmitted packets to 30, and use the default value 0 for all other thresholds, do as follows:

```
huawei(config)#gpon alarm-profile add profile-id 5
{ <cr>|profile-name<K> }:

  Command:
          gpon alarm-profile add profile-id 5
  Press 'Q' or 'q' to quit input
>  GEM port loss of packets threshold (0~100)[0]:                        10
>  GEM port misinserted packets threshold (0~100)[0]:                    30
>  GEM port impaired blocks threshold (0~100)[0]:
>  Ethernet FCS errors threshold (0~100)[0]:
>  Ethernet excessive collision count threshold (0~100)[0]:
>  Ethernet late collision count threshold (0~100)[0]:
>  Too long Ethernet frames threshold (0~100)[0]:
>  Ethernet buffer (Rx) overflows threshold (0~100)[0]:
>  Ethernet buffer (Tx) overflows threshold (0~100)[0]:
>  Ethernet single collision frame count threshold (0~100)[0]:
>  Ethernet multiple collisions frame count threshold (0~100)[0]:
>  Ethernet SQE count threshold (0~100)[0]:
>  Ethernet deferred transmission count threshold (0~100)[0]:
>  Ethernet internal MAC Tx errors threshold (0~100)[0]:
>  Ethernet carrier sense errors threshold (0~100)[0]:
>  Ethernet alignment errors threshold (0~100)[0]:
>  Ethernet internal MAC Rx errors threshold (0~100)[0]:
>  PPPOE filtered frames threshold (0~100)[0]:
>  MAC bridge port discarded frames due to delay threshold (0~100)[0]:
>  MAC bridge port MTU exceeded discard frames threshold (0~100)[0]:
>  MAC bridge port received incorrect frames threshold (0~100)[0]:
```

```
>  CES general error time threshold(0~100)[0]:
>  CES severely time threshold(0~100)[0]:
>  CES bursty time threshold(0~100)[0]:
>  CES controlled slip threshold(0~100)[0]:
>  CES unavailable time threshold(0~100)[0]:
>  Drop events threshold(0~100)[0]:
>  Undersize packets threshold(0~100)[0]:
>  Fragments threshold(0~100)[0]:
>  Jabbers threshold(0~100)[0]:
>  Failed signal of ONT threshold(Format:1e-x, x: 3~8)[3]:
>  Degraded signal of ONT threshold(Format:1e-x, x: 4~9)[4]:
>  FEC uncorrectable code words threshold(0~1101600000)[0]:
>  FEC correctable code words threshold(0~1101600000)[0]:
>  Upstream PQ discarded byte alarm threshold(0~65535)[0]:6
>  Downstream PQ discarded byte alarm threshold(0~65535)[0]:6
>  XGEM key errors threshold(0~100)[0]:
>  XGEM HEC error count threshold(0~100)[0]:

  Adding an alarm profile succeeded
  Profile ID  : 5
  Profile name: alarm-profile_5

huawei(config)#display gpon alarm-profile profile-id 5
  --------------------------------------------------------------
  Profile ID  : 5
  Profile name: alarm-profile_5
  --------------------------------------------------------------
  GEM port loss of packets threshold:                       10
  GEM port misinserted packets threshold:                   30
  GEM port impaired blocks threshold:                        0
  Ethernet FCS errors threshold:                             0
  Ethernet excessive collision count threshold:              0
  Ethernet late collision count threshold:                   0
  Too long Ethernet frames threshold:                        0
  Ethernet buffer (Rx) overflows threshold:                  0
  Ethernet buffer (Tx) overflows threshold:                  0
  Ethernet single collision frame count threshold:           0
  Ethernet multiple collisions frame count threshold:        0
  Ethernet SQE count threshold:                              0
  Ethernet deferred transmission count threshold:            0
  Ethernet internal MAC Tx errors threshold:                 0
  Ethernet carrier sense errors threshold:                   0
  Ethernet alignment errors threshold:                       0
  Ethernet internal MAC Rx errors threshold:                 0
  PPPOE filtered frames threshold:                           0
  MAC bridge port discarded frames due to delay threshold:   0
  MAC bridge port MTU exceeded discard frames threshold:     0
  MAC bridge port received incorrect frames threshold:       0
  CES general error time threshold:                          0
  CES severely time threshold:                               0
  CES bursty time threshold:                                 0
  CES controlled slip time threshold:                        0
  CES unavailable time threshold:                            0
  Drop events threshold:                                     0
  Undersize packets threshold:                               0
  Fragments threshold:                                       0
  Jabbers threshold:                                         0
  Failed signal of ONU threshold (Format:1e-x):              3
  Degraded signal of ONU threshold (Format:1e-x):            4
  FEC uncorrectable code words threshold:                    0
  FEC correctable code words threshold:                      0
  Upstream PQ discarded byte alarm threshold:                6
  Downstream PQ discarded byte alarm threshold:              6
  XGEM key errors threshold:                                 0
  XGEM HEC error count threshold:                            0
  --------------------------------------------------------------
  Binding Times:                                             0
  --------------------------------------------------------------
```

5.2 Creating a VLAN

Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see **Table 5-3**.

Table 5-3 VLAN planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN type: smart
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S+C.	
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	

Default Configuration

Table 5-4 lists the default parameter settings of VLAN.

Table 5-4 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart VLAN	You can run the **defaultvlan modify** command to modify the VLAN type but cannot delete the VLAN.
Reserved VLAN of the system	VLAN ID range: 4079-4093	You can run the **vlan reserve** command to modify the VLAN reserved by the system.

Prerequisite

- The VLAN to be added should not exist in the system.
- Service VLAN cannot be reserve VLAN.

Procedure

Step 1 Create a VLAN.

Run the **vlan** to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 5-5 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the **vlan** ***vlanid*** **standard** command.	Standard VLAN. Ethernet ports in a standard VLAN are interconnected with each other but Ethernet ports in different standard VLANs are isolated from each other.	Only available to Ethernet ports and specifically to network management and subtending.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Smart VLAN	To add a smart VLAN, run the **vlan** ***vlanid*** **smart** command.	One VLAN may contain multiple xDSL service ports or xPON service ports. The traffic streams of these ports, however, are isolated from each other. In addition, the traffic streams of different VLANs are also isolated. One smart VLAN provides access for multiple users and therefore saves VLAN resources.	Smart VLANs can be applied in residential communities to provide xDSL or xPON service access.
MUX VLAN	To add a MUX VLAN, run the **vlan** ***vlanid*** **mux** command.	One MUX VLAN contains only one xDSL service port or xPON service port. The traffic streams in different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. Hence, a MUX VLAN can identify an access user.	MUX VLANs are applicable to xDSL or xPON service access. For example, MUX VLANs can be used to distinguish users.
Super VLAN	To add a super VLAN, run the **vlan** ***vlanid*** **super** command.	The super VLAN is based on Layer 3. One super VLAN contains multiple sub-VLANs. Through an ARP proxy, the sub-VLANs in a super VLAN can be interconnected at Layer 3.	Super VLANs save IP addresses and improve the utilization of IP addresses. For a super VLAN, sub-VLANs must be configured. You can run the **supervlan** command to add a sub-VLAN to a specified super VLAN. A sub-VLAN must be a smart VLAN or MUX VLAN.

NOTE

- To add VLANs with consecutive IDs in batches, run the **vlan *vlanid* to *end-vlanid*** command.
- To add VLANs with inconsecutive IDs in batches, run the **vlan *vlan-list*** command.

----End

Example

Create VLAN 50 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 50 smart
```

Create VLAN 55-60 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 55 to 60 smart
```

Create VLAN 65, 73 and 52 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 65,73,52 smart
```

5.3 Configuring an Upstream Port

The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.

Prerequisites

The planned virtual local area network (VLAN) is already configured.

Procedure

Step 1 Configure an upstream port for the VLAN.

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

Step 2 Configure the attribute of the upstream port.

If the default attribute of the upstream port does not meet the requirement for interconnection of the upstream port with the upper-layer device, you need to configure the attribute. For configuration details, see **2.5 Configuring the Attributes of an Upstream Ethernet Port**.

Step 3 (Optional) Configure redundancy backup for the uplink.

To ensure reliability of the uplink, two upstream ports must be available. That is, redundancy backup of the upstream ports needs to be configured. For details, see **14.1 Configuring Ethernet Link Aggregation**.

----End

Example

Assume that the 0/19/0 and 0/19/1 upstream ports are to be added to VLAN 50. The 0/19/0 and 0/19/1 need to be configured into an aggregation group for double upstream accesses. For the two upstream ports, the working mode is full-duplex (full) and the port rate is 100 Mbit/s. To configure such upstream ports, do as follows:

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#duplex 0 full
huawei(config-if-giu-0/19)#duplex 1 full
huawei(config-if-giu-0/19)#speed 0 100
huawei(config-if-giu-0/19)#speed 1 100
huawei(config-if-giu-0/19)#quit
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

5.4 Configuring a GPON ONT

The MA5600T/MA5603T provides end users with services through the ONT. The MA5600T/MA5603T can manage the ONT and the ONT can work in the normal state only after the channel between the MA5600T/MA5603T and the ONT is available.

Prerequisites

The GPON ONT profile is already created. **Configuring a GPON ONT Capability Profile** and **Configuring a GPON ONT Alarm Profile** are already completed.

Context

The MA5600T/MA5603T uses the ONT Management and Control Interface (OMCI) protocol to manage and configure the GPON ONT, and supports the offline configuration of the ONT. The ONT does not need to save the configuration information locally. This helps to provision services.

Table 5-6 lists the default settings of the GPON ONT.

Table 5-6 Default settings of the GPON ONT

Parameter	Default Setting
ONT auto-find function of a GPON port	Disabled
ONT status after an ONT is added	Activated
Default VLAN of the ONT port	1

Procedure

Step 1 Run the **interface gpon** command to enter the GPON mode.

Step 2 Add a GPON ONT.

1. Run the **port *portid* ont-auto-find** command to enable the auto-find function of the ONT. After the function is enabled, you can add an ONT according to the information reported by the system. By default, the ONT auto-find function of a GPON port is disabled.

   NOTE

   An auto-find ONT is in the auto-find state. The auto-find ONT can work in the normal state only after it is confirmed or added.

2. Run the **ont add** command to add an ONT offline, or run the **ont confirm** command to confirm the auto-find ONT.

When ONTs are added or confirmed, the system provides four authentication modes: SN, password, SN+password, LOID+CHECKCODE.

- SN authentication: The OLT detects the serial number (SN) reported by an ONT. If the SN is consistent with the OLT configuration, authentication is passed and the ONT goes online. This mode requires recording all ONT SNs. Hence, it is used to confirm auto discovery ONTs and is not applicable to adding ONTs in batches.
- Password authentication: The OLT detects the password reported by an ONT. If the password is consistent with the OLT configuration, the ONT goes online normally. This mode requires planning ONT passwords and does not require manually recording ONT SNs. Hence, it is applicable to adding ONTs in batches. The password authentication provides two discovery modes: always-on and once-on.
  - always-on: After first password authentication is passed, no SN is allocated and password authentication is always used in subsequent authentications. This discovery mode is easy for future maintenance. In the always-on discovery mode, configuration is not required to be modified when an ONT is replaced and only the password is required. The always-on discovery mode has lower security. If other users know the password, the users will illegally have service permissions.
  - Once-on: After first password authentication is passed, an SN is automatically allocated and password+SN authentication is used in subsequent authentications. An ONT can go online only after the correct password and SN are entered. The once-on authentication mode has high security. After an ONT is replaced or the password is mistakenly changed, the ONT needs to be configured again, which requires more maintenance effort.
- SN+password authentication: The OLT detects the password and SN reported by an ONT. If the password and SN are consistent with the OLT configuration, the ONT goes online normally. This authentication mode has the highest security but it requires manually recording ONT SNs.
- LOID+CHECKCODE authentication: defined by a telecom operator. In this authentication mode, LOID has 24 bytes, and CHECKCODE has 12 bytes and is optional. Whether 24 bytes or 36 bytes are used for authentication depends on data planning, which is unified over the entire network. The OLT determines whether LOID+CHECKCODE reported by the ONT is the same as the configured one. If they are the same, the ONT authentication is passed. If they are different, the OLT obtains the ONT password and compares it with the last 10 bytes of the LOID. If they are the same, the ONT authentication is also passed. This operation is for compatibility with the ONTs using password authentication.

Adding ONTs in offline mode is applicable to the batch deployment scenario. All ONTs are added to the OLT to complete service provisioning beforehand. When a use subscribes to the service, an installation engineer takes an ONT to the user's house and completes configurations. After the ONT goes online and passes authentication (generally the password authentication mode or LOID authentication mode is used), the service is provisioned.

Adding ONTs in auto discovery mode is applicable to the scenario where a small number of ONTs are added. When users subscribe to the service, installation engineers take ONTs to the users' houses. After the ONTs go online, the OLT confirms the ONTs one by one. Generally, the MAC address authentication mode is used to confirm the ONTs.

NOTE

- If the ONU is an independent NE and is directly managed by the NMS through the SNMP management mode, select the SNMP management mode. For this mode, you only need to configure the parameters for the GPON line and the parameters for the management channel on the OLT.
- If the ONU is not an independent NE and all its configuration data is issued by the OLT through OMCI, select the OMCI management mode. For this mode, you need to configure all parameters (including line parameters, UNI port parameters, and service parameters) that are required for the ONU on the OLT.
- Generally, the ONT management mode is set to the OMCI mode.

3. (Optional) When the ONT management mode is the SNMP mode, you need to configure the SNMP management parameters for the ONT. The procedure is as follows:
   a. Run the **ont ipconfig** command to configure the management IP address of the ONT.

      The IP address should not be in the same subnet for the IP address of the VLAN port.
   b. Run the **ont snmp-profile** command to bind the ONT with an SNMP profile.

      Run the **snmp-profile add** command to add an SNMP profile before the configuration.
   c. Run the **ont snmp-route** command to configure a static route for the NMS server, that is, configure the IP address of the next hop.

Step 3 Configure the default VLAN (native VLAN) for the ONT port.

Run the **ont port native-vlan** command to configure the default VLAN for the ONT port. By default, the default VLAN ID of the ONT port is 1.

- If the packets reported from a user (such a PC) to the ONT are untagged, the packets are tagged with the default VLAN of the port on the ONT and then reported to the OLT.
- If the packets reported from a user to the ONT are tagged, you need to configure the port VLAN of the ONT to be the same as the VLAN in the user tag. The packets are not tagged with the default VLAN of the port on the ONT but are reported to the OLT with the user tag.

Step 4 Bind an alarm profile.

Run the **ont alarm-profile** command to bind an alarm profile. Ensure that **6.1.4 Configuring a GPON ONT Alarm Profile** is completed before the configuration.

Step 5 Bind a DBA profile.

Run the **tcont bind-profile** command to bind a DBA profile to a T-CONT.

A DBA profile can be bound to a T-CONT after an ONT is added.

Step 6 Configure a GEM port.

1. Run the **gemport add** command to add a GEM port. When adding a GEM port, select the correct attribute according to the service type.
2. Run the **ont gemport bind** command to bind the GEM port to an ONT T-CONT, that is, allocating the T-CONT resources to the GEM port.

   NOTE

   If traffic streams are configured on a GEM port and an ONT is the working ONT in a single-homing protection group, the GEM port cannot be bound to or unbound from the ONT.
3. Run the **ont gemport mapping** command to create the mapping between the GEM port and the ONT-side service.

Step 7 Activate the ONT.

Run the **ont activate** command to activate the ONT. The ONT can transmit services only when it is in the activated state.

After being added, the ONT is in the activated state by default. The step is required only when the ONT is in the deactivated state.

Step 8 Query the ONT status.

Run the **display ont info** command to query the ONT running status, configuration status, and matching status.

----End

Example

To add five ONTs in offline mode with password authentication mode (ONT passwords are 0100000001-0100000005), set the discovery mode of password authentication to always-on, and bind ONT capability profile 10, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000001 always-on profile-id
10 manage-mode omci
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000002 always-on profile-id
10 manage-mode omci
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000003 always-on profile-id
10 manage-mode omci
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000004 always-on profile-id
10 manage-mode omci
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000005 always-on profile-id
10 manage-mode omci
```

To add an ONT that is managed by the OLT through the OMCI protocol, confirm this ONT according to the SN 3230313185885B41 automatically reported by the system, and bind the ONT with capability profile 3 that match the ONT, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/2)#ont confirm 0 sn-auth 3230313185885B41 profile-id 3
manage-mode omci
```

To add an ONU that is managed as an independent NE and whose SN is known as 3230313185885641, bind the ONU with capability profile 4 that matches the ONU, configure the NMS parameters for the ONU, and set the management VLAN to 100, do as follows:

```
huawei(config)#snmp-profile add profile-id 1 v2c public private 10.10.5.53 161
huawei
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 2 sn-auth 3230313185885641 profile-id 4
manage-mode snmp
huawei(config-if-gpon-0/2)#ont ipconfig 0 2 static ip-address 10.20.20.20 mask
255.255.255.0 gateway 10.10.20.1 vlan 100
huawei(config-if-gpon-0/2)#ont snmp-profile 0 2 profile-id 1
huawei(config-if-gpon-0/2)#ont snmp-route 0 2 ip-address 10.10.20.190 mask
255.255.255.0 next-hop 10.10.20.100
```

5.5 Configuring a GPON Port

To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.

Default Configuration

Table 5-7 lists the default settings of the GPON port.

Table 5-7 Default settings of the GPON port

Parameter	Default Setting
GPON port	Enabled
Downstream FEC function of the GPON port	Disabled
Compensation distance range of the GPON port ranging	Minimum logical distance: 0 km; maximum logical distance: 20 km

Procedure

Step 1 Run the **interface gpon** command to enter the GPON mode.

Step 2 Configure the laser of the GPON port.

- Run the **undo shutdown** command to enable the laser of the GPON port. By default, the laser of the GPON port is enabled and the GPON port is available. In this case, skip this step.
- If the GPON port is not to be used, run the **shutdown** command to disable the laser of the GPON port.

⚠ **CAUTION**

Disabling a PON port that carries services will cause the interruption of such services.

Step 3 Configure the downstream FEC function of the GPON port.

Run the **port** ***portid*** **fec** command to configure the FEC function of the GPON port. By default, the FEC function is disabled.

NOTE

- FEC is to insert redundant data into normal packets so that the line has certain error tolerance. Some bandwidth, however, must be consumed. Enabling FEC enhances the error correction capability of the line but at the same time occupies certain bandwidth. Determine whether to enable FEC according to the actual line planning.
- If a large number of ONTs are already online, enabling FEC on the GPON port may cause certain ONTs to go offline. Therefore, it is suggested that FEC should not be enabled on a GPON port that connects to online ONTs.

Step 4 Configure the renewal time of the ONT key.

Run the **port** ***portid*** **ont-password-renew** command to configure the interval for renewing the ONT key. To ensure the system security, the ONT key renewal must be configured.

Step 5 Configure the compensation distance in the ranging.

Run the **port** ***portid*** **range** command to configure the compensation distance range of the GPON port ranging. By default, the minimum logical distance is 0 km, and the maximum logical distance is 20 km. The difference between the minimum logical distance and the maximum logical distance must not exceed 20 km.

Step 6 (Optional) Configure the DBA calculation period on a GPON port basis.

When different GPON ports provide different access services, the bandwidth delays on these ports are different. In this case, the DBA calculation period needs to be configured on a GPON port basis.

1. In GPON board mode, run the **port dba bandwidth-assignment-mode** command to configure the DBA mode on a GPON port.
2. In diagnose mode, run the **gpon port dba calculate-period** command to configure the DBA calculation period on the GPON port.

NOTE

- The DBA calculation period on a GPON port can be configured only when the DBA mode is set to **manual** on this GPON port.
- By default, the DBA mode on a GPON port is **default**, which means the global DBA mode is used as the bandwidth assignment mode for the GPON port. In this case, if the global DBA mode is modified by running the **gpon dba bandwidth-assignment-mode** command, the bandwidth assignment mode on the GPON port is also modified. If the DBA mode on a GPON port is not **default**, the bandwidth assignment mode on the GPON port is not affected by the global DBA mode.
- If ONTs are configured on a GPON port, modifying the DBA mode is not allowed on this GPON port.
- For the TDM service, the DBA mode must be set to **min-loop-delay**.

----End

Example

Assume that the key renew interval of the ONT under the port is 10 hours, the minimum compensation distance of ranging is 10 km, and the maximum compensation distance of ranging is 15 km. To enable the FEC function of GPON port 0/2/0, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 fec enable
huawei(config-if-gpon-0/2)#port 0 ont-password-renew 10
huawei(config-if-gpon-0/2)#port 0 range min-distance 10 max-distance 15
  This command will result in the ONT's re-register in the port.
  Are you sure to execute this command? (y/n)[n]: y
```

To set the global DBA mode to **min-loop-delay**, DBA mode on GPON port 0/2/0 to **manual**, and DBA calculation period to **4**, do as follows:

```
huawei(config)#gpon dba bandwidth-assignment-mode min-loop-delay
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port dba bandwidth-assignment-mode 0 manual
huawei(config-if-gpon-0/2)#quit
huawei(config)#diagnose
huawei(diagnose)%%gpon port dba calculate-period 0/2/0 4
```

5.6 Creating a GPON Service Port

A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

Context

A service port can carry a single service or multiple services. When a service port carries multiple services, the MA5600T/MA5603T supports the following modes of classifying traffic:

- By user-side VLAN
- By user-side service encapsulation mode
- By VLAN+user-side packet priority
- By VLAN+user-side service encapsulation mode

Table 5-8 lists the default settings of a service port.

Table 5-8 Default settings of a service port

Parameter	Default Setting
Traffic profile ID	0-6
Administrative status of the service port	Activated
Maximum number of MAC addresses that are learned	1023

Procedure

Step 1 Create a traffic profile.

Run the **traffic table ip** command to create a traffic profile. There are seven default traffic profiles in the system with the IDs of 0-6.

Before creating a service port, run the **display traffic table** command to check whether the traffic profiles in the system meet the requirement. If no traffic profile in the system meets the requirement, add a traffic profile that meets the requirement. For details about the traffic profile, see **Configuring Traffic Management Based on Service Port**.

Step 2 Create a service port.

You can choose to create a single service port or multiple service ports in batches according to requirements.

- Run the **service-port** command to create a single service port. Service ports are classified into single-service service ports and multi-service service ports. Multi-service service ports are generally used for the triple play service.
  - Single-service service port:

    By default, a service port is a single-service service port if you do not enter **multi-service**.
  - Multi-service service port based on the user-side VLAN:

    Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** | **other-all** }.
    - **untagged**: When **untagged** is selected, user-side packets do not carry a tag.
    - *user-vlanid*: When *user-vlanid* is selected, user-side packets carry a tag and the value of *user-vlanid* must be the same as the tag carried in user-side packets, that is, C-VLAN.
    - **priority-tagged**: When **priority-tagged** is selected, the VLAN tag is 0 and the priorities of user-side packets are 0-7.

  - **other-all**: When **other-all** is selected, service ports for the transparent LAN service (TLS) are created, which are mainly used in the QinQ transparent transmission service for enterprises. All the traffic except known traffic in the system is carried over this channel.
- Multi-service service port based on the user-side service encapsulation mode:

  Select **multi-service user-encap** *user-encap*.
- Multi-service service port based on VLAN+user-side packet priority (802.1p):

  Select **multi-service user-8021p** *user-8021p* [**user-vlan** *user-vlanid*].
- Multi-service service port based on VLAN + user-side service encapsulation mode (user-encap):

  Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** } **user-encap** *user-encap*.

NOTE

- The system supports creating service ports by index. One index maps one service port and the input of a large number of traffic parameters is not required. Therefore, the configuration of service ports is simplified. During the creation of a service port, *index* indicates the index of the service port and it is optional. If it is not input, the system automatically adopts the smallest value.
- **vlan** indicates the S-VLAN. An S-VLAN can only be a MUX VLAN or smart VLAN.
- **rx-cttr** is the same as **outbound** in terms of meanings and functions. Either of them indicates the index of the traffic from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meanings and functions. Either of them indicates the index of the traffic from the user side to the network side. The traffic profile bound to the service port is created in **Step 1**.

- Run the **multi-service-port** command to create service ports in batches.

Step 3 Configure the attributes of the service port. Configure the attributes of the service port according to requirements.

- Run the **service-port desc** command to configure the description of the service port. Configure the description for a service port to facilitate maintenance. In general, configure the purpose and related service information as the description of a service port.
- Run the **service-port *index* adminstatus** command to configure the administrative status of the service port. By default, a service port is in the activated state.

  A service port can be activated at two levels: port level and service port level. To provision services for a user, the access port and the corresponding service port of the user must be activated.
- Run the **mac-address max-mac-count service-port** command to configure the maximum number of MAC addresses learned by the service port to restrict the maximum number of PCs that can access the Internet by using a same account. By default, the maximum number of MAC addresses learned by the service port is 1023.

----End

Example

Connect ONT to GPON port 0/2/0 of the MA5600T/MA5603T. Plan an Internet access user. The ONT provides the Internet-access-only service with a rate of 4096 kbit/s for this user, the index of the GEM port that carries the service is 135, the service VLAN ID is 1000, and only three users are allowed to use a same account for Internet access at the same time. The query shows that there is no proper traffic profile in the system. Then, create traffic profile 10. This user is not registered yet. Therefore, the service is not provided for the user for the moment. To configure such a user, do as follows:

```
huawei(config)#traffic table ip index 10 cir 4096 priority 3 priority-policy loc
al-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index            : 10
  TD Name             : ip-traffic-table_10
  Priority            : 3
  Copy Priority       : -
  Mapping Index       : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy     : local-pri
  CIR                 : 4096 kbps
  CBS                 : 133072 bytes
  PIR                 : 8192 kbps
  PBS                 : 264144 bytes
  Color policy        : dei
  Referenced Status   : not used
  ------------------------------------------------
huawei(config)#service-port 5 vlan 1000 gpon 0/2/0 gemport 135 inbound
 traffic-table index 10 outbound traffic-table index 10
huawei(config)#mac-address max-mac-count service-port 5 3
huawei(config)#service-port 5 adminstatus disable
```

Connect ONT to GPON port 0/2/0 of the MA5600T/MA5603T. A commercial user requires the Internet access service with a rate of 8192 kbit/s to be provided. For subsequent service expansion, the ONT provides the Internet access service for this user in the multi-service mode. The user is differentiated based on the user-end VLAN, S-VLAN ID is 1023, C-VLAN ID is 100, and the index of the GEM port that carries the service is 130. The query shows that there is no proper traffic profile in the system. Then, create traffic profile 8. The Internet access service is required to be provided immediately. The description of the service port is added to facilitate maintenance. To configure such a user, do as follows:

```
huawei(config)#traffic table ip index 8 cir 8192 priority 4 priority-policy loca
l-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index            : 8
  TD Name             : ip-traffic-table_8
  Priority            : 4
  Copy Priority       : -
  Mapping Index       : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy     : local-pri
  CIR                 : 8192 kbps
  CBS                 : 264144 bytes
  PIR                 : 16384 kbps
  PBS                 : 526288 bytes
  Color policy        : dei
  Referenced Status   : not used
  ------------------------------------------------
huawei(config)#service-port 10 vlan 1023 gpon 0/2/0 gemport 130 multi-service
user-vlan 100 inbound traffic-table index 8 outbound traffic-table index 8
huawei(config)#service-port desc 10 description gpon/vlanid:1023/uservlan:100
```

6 Configuring the GPON Internet Access Service (Profile Mode)

About This Chapter

The GPON broadband Internet access service is applicable to the scenario that provides users with the Internet access service through optical fibers. The networking mode for the service can be FTTH, FTTB, FTTC, or FTTO. This topic describes how to configure the Internet access service provided by the MA5600T/MA5603T through GPON.

Application Context

GPON is mainly used in the FTTx solution. The FTTx technology is mainly used for adopting the optical network in the access network. Its coverage is from the CO device of the regional telecommunications room to the subscriber terminal. The optical line terminal (OLT) functions as the CO device. The optical network unit (ONU) or the optical network terminal (ONT) functions as the subscriber terminal.

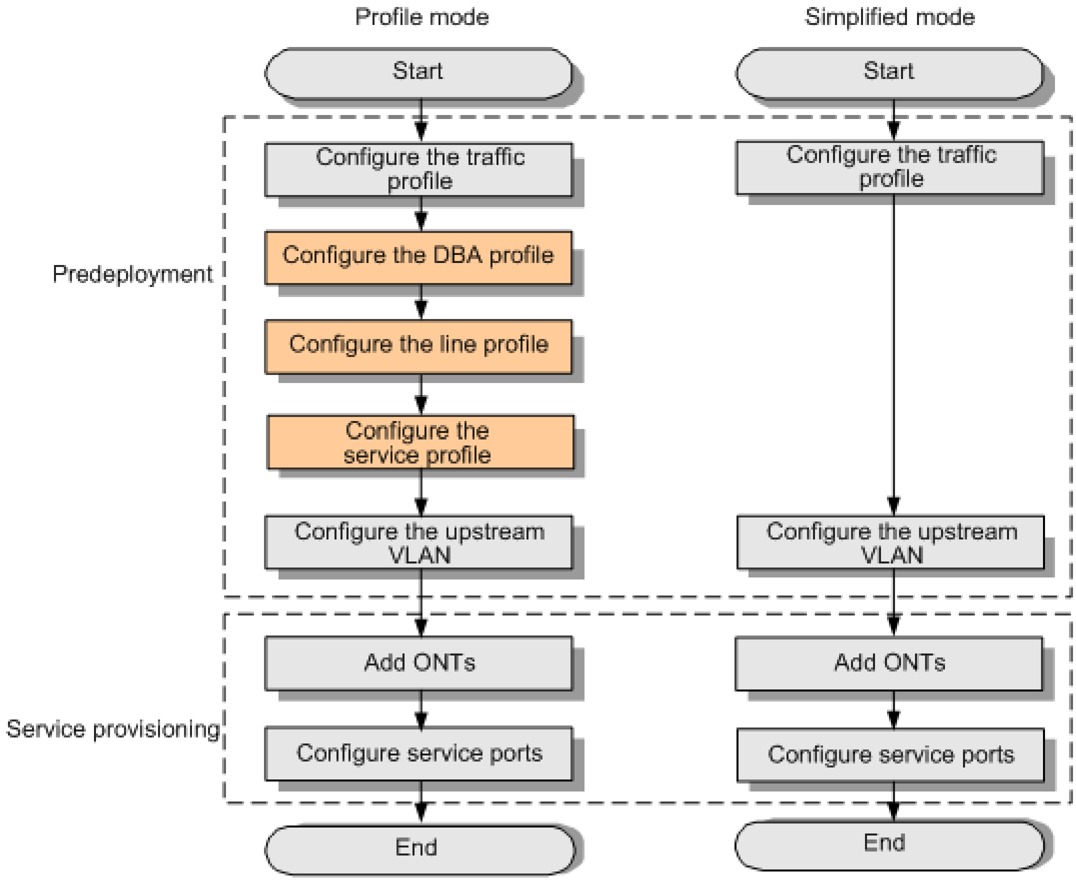
- FTTH refers to fiber to the home. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the ONT at lower layer through the ODN. The ONT is connected to subscribers to provide the voice, Internet access, and IPTV services.
- FTTB refers to fiber to the building. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the MDU or ONUs of other types at lower layer through the ODN. The ONU or MDU is connected to subscribers. FTTB can be further classified into FTTB+DSL and FTTB+LAN. These two modes respectively use the home gateway with an RJ-11 upstream port and the home gateway with a LAN upstream port to provide the voice, Internet access, and IPTV services.
- FTTC refers to fiber to the curb. FTTC is mainly used to provide services for residential subscribers. The ONU is placed in the cabinet at the curb. It uses coaxial cables to transmit CATV signals or uses twisted pairs to transmit the voice and Internet access services. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the MDU or outdoor cabinets for ONUs of other types at lower layer through the ODN. The ONU or MDU is connected to subscribers. FTTC and FTTB are the same in configuration and differ from each other only in the networking mode.
- FTTO refers to fiber to the office. The Ethernet port of the ONU is connected to the LAN of subscribers so that subscribers can be directly connected to the Internet, or connected to

the headquarters or branch offices through VPN. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the ONU at lower layer through the ODN. The ONU is connected to subscribers to provide the voice, Internet access, IPTV, and private line services.

Difference Between the Profile Mode and Simplified Mode

In FTTH scenarios, the simplified mode can be used for configuring the GPON service to simplify configurations and reduce costs. **Figure 6-1** shows configuration procedures in profile mode and simplified mode.

Figure 6-1 Configuration flowchart


Profile mode
Simplified mode
Start
Start
Predeployment
Configure the traffic profile
Configure the traffic profile
Configure the DBA profile
Configure the line profile
Configure the service profile
Configure the upstream VLAN
Configure the upstream VLAN
Service provisioning
Add ONTs
Add ONTs
Configure service ports
Configure service ports
End
End

The simplified mode is different from the profile mode in the following aspects:

- GEM ports are allocated automatically by the system.
- The DBA profile, line profile, and service profile do not need to be configured. When being added, an ONT is automatically bound to default line profile 0 and default service profile 0. The default line profile and service profile can be modified but cannot be deleted.
- By default, T-CONT 0 and T-CONT 1 are created in line profile 0. T-CONT 0 is bound to default DBA profile 2 (with 1 Mbit/s fixed bandwidth) and serves as an OMCI channel. T-CONT 1 is bound to default DBA profile 7 (with 8 Mbit/s fixed bandwidth and 20 Mbit/s maximum bandwidth) and serves as a service channel. By default, a GEM port does not

exist in T-CONT 1 but is automatically allocated by the system in traffic stream creation. The DBA profile bound to a T-CONT can be modified.

- The type and number of ONT ports in service profile 0 are not limited by the profile but are matched automatically when the ONT goes online. Before an ONT goes online for the first time, eight ETH ports and one IPHOST port are displayed by default.
- The simplified mode applies only to the scenario where multiple traffic streams use the same T-CONT. It is not applicable to the scenario whether different traffic streams use different T-CONTs. All traffic streams on an ONT share the same T-CONT for services; therefore, the traffic streams can be scheduled on the ONT only by GEM port CAR or PQ.
- The QinQ service cannot coexist with the simplified-mode configuration on an ONT. The simplified-mode configuration is not applicable to the open access scenario.

The following describes the restrictions of configuration in simplified mode:

- End-to-end (E2E) traffic streams and non-E2E traffic streams cannot coexist on an ONT.
- When the GEM port mapping mode is set to port, port+VLAN, or port+VLAN+priority on an ONT, E2E traffic streams cannot be created on the ONT.
- E2E GPON traffic streams need to be differentiated by VLAN, VLAN+Pbits, or VLAN +EtherType. If not differentiated by VLAN, traffic streams on the ONT ports cannot be forwarded to the OLT in QinQ mode.
- E2E GPON traffic streams can be differentiated by VLAN, VLAN+Pbits, or VLAN +EtherType. They cannot be differentiated by EtherType alone.
- GEM port encryption is not supported when E2E traffic streams are created.

Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.11 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.
- The GPON mode is already switched to the profile mode.

```
huawei(diagnose)%%display xpon mode
  --------------------------------------------------
        Current config mode: Profile-mode
  --------------------------------------------------
```

Data Plan

Before configuring the GPON Internet access service, plan the data items as listed in **Table 6-1**.

Table 6-1 Data plan for the GPON Internet access service

Parameter	Data	Remarks
MA5600T/MA5603T	Access rate	Configure the data according to the user requirements.

Parameter	Data	Remarks
	Access port	Configure the data according to the network planning.
	VLAN planning	The cooperation with the upper-layer device should be considered in the VLAN planning. The upstream VLAN must be the same as that of the upper-layer device.
	QoS policy	Configure the data according to the QoS policy of the entire network. Generally, the priority of the Internet access service is lower than the priorities of the voice and video services.
	T-CONT ID	It is recommended that you do not use T-CONT 0 to transmit services.
	GEM port index	-
ONT	ONT line profile, ONT service profile	The ONT service profile must be the same as the actual capacity.
	ONT index	GPON supports a split ratio of up to 1:128. You need to plan the ONTs connected to the MA5600T/MA5603T to facilitate management.
	Authentication mode	The password, SN, and LOID +CHECKCODE can be used for authentication.
Upper-layer LAN switch	The LAN switch transparently transmits the service packets of the MA5600T/MA5603T on Layer 2. The VLAN ID must be the same as the upstream VLAN ID of the MA5600T/MA5603T.	-

Parameter	Data	Remarks
BRAS	The BRAS performs the related configurations according to the authentication and accounting requirements for dialup users, for example, configures the access user domain (including the authentication scheme, accounting scheme, and authorization scheme bound to the domain) and specifies the RADIUS server. If the BRAS is used to authenticate users, you need to configure the user name and the password for each user on the BRAS. If the BRAS is used to allocate IP addresses, you need to configure the corresponding IP address pool on the BRAS.	-

Procedure

1. 6.1 Configuring a GPON ONT Profile
   Gigabit-capable passive optical network (GPON) optical network terminal (ONT) profiles are classified into dynamic bandwidth allocation (DBA) profiles, line profiles, service profiles, and alarm profiles. This topic describes how to configure these profiles.
2. 6.2 Creating a VLAN
   Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.
3. 6.3 Configuring an Upstream Port
   The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.
4. 6.4 Configuring a GPON ONT
   The MA5600T/MA5603T provides end users with services through the ONT. The MA5600T/MA5603T can manage the ONT and the ONT can work in the normal state only after the channel between the MA5600T/MA5603T and the ONT is available.
5. 6.5 Configuring a GPON Port
   To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.
6. 6.6 Creating a GPON Service Port
   A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

6.1 Configuring a GPON ONT Profile

Gigabit-capable passive optical network (GPON) optical network terminal (ONT) profiles are classified into dynamic bandwidth allocation (DBA) profiles, line profiles, service profiles, and alarm profiles. This topic describes how to configure these profiles.

Context

In the GPON profile mode, GPON ONT profiles are classified into line profiles and service profiles according to the GPON ONT parameters. The line profile is mainly used to configure the information related to DBA, transmission container (T-CONT), and GPON encapsulation mode (GEM) port. The service profile is used to configure the actual ONT capability and the parameters related to services.

The line profile is mandatory and the service profile is optional and dependent of service requirements. Set related attributes in line profile mode and service profile mode, and directly bind the ONT to the line profile and service profile.

GPON supports modifying the bound profile for ONT with service configuration unless in the following cases:

- GemIndex n is configured with services but the services do not exist in the specified new profile.
- GemIndex n is configured with services and the services exist in the specified new profile, but the service types (ETH/TDM) are different.
- GemIndex n is configured with services and the services exist in the specified new profile, but the subtending attributes (ON/OFF) are different.

Table 6-2 lists the default settings of the GPON ONT profile.

Table 6-2 Default settings of the GPON ONT profile

Parameter	Default Setting
GPON mode	Profile-mode

6.1.1 Configuring a DBA Profile

A DBA profile defines the traffic parameters of xPON and can be bound to a T-CONT dynamically allocate the bandwidth and improve the usage of the upstream bandwidth.

Default Configuration

Table 6-3 lists the default settings of the DBA profiles.

Table 6-3 Default settings of the DBA profiles

Parameter	Default Setting	Remarks
Default DBA profile ID in the system	0-9	You can run the **display dba-profile all** command to query the parameter values of each default DBA profile.

Procedure

Step 1 Add a DBA profile.

Run the **dba-profile add** command to add a DBA profile.

NOTE

- By default, T-CONT is not bound to any DBA profile. Hence, you need to bind a DBA to a T-CONT.
- When you add a DBA profile, the bandwidth value must be a multiple of 64. If you enter a bandwidth value not of a multiple of 64, the system adopts the closest multiple of 64 that is smaller than the value you enter.

Step 2 Query a DBA profile.

Run the **display dba-profile** command to query a DBA profile.

----End

Example

Assume that the name and type of a DBA profile are "DBA_bandwidth" and "type3" respectively, and that the bandwidth required by a user is 100 Mbit/s. To add such a DBA profile, do as follows:

```
huawei(config)#dba-profile add profile-name DBA_100M type3 assure 102400 max
102400
huawei(config)#display dba-profile profile-name DBA_100M
  -----------------------------------------------------------------
  Profile-name :             DBA_100M
  Profile-ID:                10
  type:                      3
  Bandwidth compensation:    No
  Fix(kbps):                 0
  Assure(kbps):              102400
  Max(kbps):                 102400
  bind-times:                0
  -----------------------------------------------------------------
```

6.1.2 Configuring a GPON ONT Line Profile

This topic describes how to configure a GPON ONT line profile and use it when adding an ONT. When an ONT is managed by OMCI or SNMP, the ONT must be bound to a GPON ONT line profile .

Default Configuration

Table 6-4 lists the default settings of a GPON ONT line profile.

Table 6-4 Default settings of a GPON ONT line profile

Parameter	Default Setting
QoS mode	Priority-queue (PQ) scheduling mode
Mapping mode supported by the ONT	VLAN mapping mode
Upstream FEC switch	Disabled

Procedure

Step 1 Run the **ont-lineprofile gpon** command to add a GPON ONT line profile and enter the GPON ONT line profile mode.

Regardless of whether the ONT is in the OMCI or SNMP management mode, the line profile must be configured for the ONT. After adding a GPON ONT line profile, directly enter the GPON ONT line profile mode to configure the related attributes of the ONT line.

Step 2 Bind a T-CONT to a DBA profile.

Use the following two methods to bind a DBA profile. Select either method as required. Both methods can coexist in the system.

- In line profile mode:

  This method is applicable to the scenario where the DBA profile is stable and the terminals are of a single type.

  Run the **tcont** command to bind the T-CONT to a DBA profile. Ensure that **6.1.1 Configuring a DBA Profile** is completed before the configuration.

- In GPON mode:

  This method is applicable to the scenario where the DBA profile changes frequently and the terminals are of different types.

  1. Run the **tcont** command to create a T-CONT, which is not bound to the DBA.
  2. After the configuration of a GPON ONT line profile is complete, enter the GPON mode. Run the **tcont bind-profile** command to bind the T-CONT to a DBA profile. Ensure that **6.1.1 Configuring a DBA Profile** is completed before the configuration.

By default, T-CONT 0 of an ONT is used by OMCI and is bound to DBA profile 1. The configuration suggestions for the OMCI T-CONT are as follows:

- Do not modify the DBA profile bound to the T-CONT. If you need to modify the profile, ensure that the fixed bandwidth of the modified profile is not lower than 5 Mbit/s.
- Do not bind a GEM port to the T-CONT. That is, ensure that the T-CONT does not carry any service.
- If the sum of the fixed bandwidth and assured bandwidth of the bound DBA profile is larger than the remaining bandwidth of the GPON port, the binding fails and the system displays a message "Failure: The bandwidth is not enough". In this case, you can run the **display port info** command to query the remaining bandwidth (Left guaranteed bandwidth (kbit/s)) of the GPON port, and then decrease the fixed bandwidth and assured bandwidth of the bound DBA profile accordingly.

Step 3 (Optional) Configure the QoS mode of the GPON ONT line profile.

Run the **qos-mode** command to configure the QoS mode of the GPON ONT line profile to be the same as the QoS mode of the GEM port. By default, the QoS mode of the ONT line profile is the PQ scheduling mode. The three QoS modes are as follows:

- flow-car: When this mode is selected, **flow-car** should be selected in the **gem mapping** command, and the maximum traffic depends on the traffic profile bound to the service port. Run the **traffic table ip** command to create a required traffic profile before the configuration.

  NOTE

  The service port here refers to the service channel from the ONT to the OLT, and is different from the service port created by running the **service-port** command.
- gem-car: When this mode is selected, **gem-car** should be selected in the **gem add** command, and the maximum traffic depends on the traffic profile bound to the GEM port.
- priority-queue: When this mode is selected, **priority-queue** should be selected in the **gem add** command. The system has eight default queues (0-7). Queue 7 has the highest priority and the traffic of this queue must be ensured first. The maximum traffic depends on the DBA profile bound to the corresponding T-CONT.

Step 4 Configure the binding relationship between the GEM port and the T-CONT.

Run the **gem add** command to configure the binding relation between the GEM index and the T-CONT in the GPON ONT line profile.

The ONT can carry services only after the mapping between the GEM port and the T-CONT, and the mapping between the GEM port and the service port are configured for the ONT. A correct attribute should be selected for **service-type** based on the service type. Select **eth** when the Ethernet service is carried. Select **tdm** when the TDM service is carried.

Step 5 Configure the mapping between the GEM port and the ONT-side service.

Run the **gem mapping** command to set up the mapping between the GEM port and the ONT-side service.

Before the configuration, run the **mapping-mode** command to configure the mapping mode supported by the ONT to be the same as the configured mapping mode between the GEM port and the ONT-side service. By default, the ONT supports the VLAN mapping mode.

- The mapping modes of the ETH port and the MOCA port are as follows:
  - If the port is specified and then the VLAN is further specified, the mapping mode should be configured to **port-vlan** in the **mapping-mode** command. That is, the port+VLAN mapping mode is used.
  - If the port is specified and then the priority is further specified, the mapping mode should be configured to **port-priority** in the **mapping-mode** command. That is, the port+priority mapping mode is used.
  - If the port and the VLAN are specified and then the priority is further specified, the mapping mode should be configured to **port-vlan-priority** in the **mapping-mode** command. That is, the port+VLAN+priority mapping mode is used.
- As a special port, the IPHOST or E1 port is not restricted by the ONT mapping mode.

When the mapping mode is **vlan-priority** or **port-vlan-priority**,

- If a GEM port is mapped to multiple VLANs, any of these VLANs cannot map to any other GEM port.
- If a VLAN is mapped to multiple GEM ports, any of these GEM ports cannot map to any other VLAN.

Step 6 Configure the upstream FEC switch.

Run the **fec-upstream** command to configure the upstream FEC switch of the GPON ONT line profile. By default, this switch is disabled.

In the FEC check, the system inserts redundancy data into normal packets. In this way, the line has certain error tolerant function, but certain bandwidth resources are wasted. Enabling the FEC function enhances the error tolerant capability of the line but occupies certain bandwidth. Therefore, determine whether to enable the FEC function based on the actual line planning.

Step 7 Run the **commit** command to make the parameters of the profile take effect. The configuration of a line profile takes effect only after you perform this operation.

NOTE

If this profile is not bound, all the parameters that are configured take effect when the profile is bound. If this profile is already bound, the configuration takes effect on all ONTs bound to this profile immediately.

Step 8 Run the **quit** command to return to the global configuration mode.

----End

Example

Assume that the GEM index is 1, the GEM port is bound to T-CONT 1 and mapped to ETH 1 of the ONT. To add GPON ONT line profile 5, create a channel for carrying the Ethernet service, with T-CONT 1 and bound to DBA profile 12, use the QoS policy of controlling the traffic based on GEM ports, and bind the GEM port to default traffic profile 6, do as follows:

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 12
huawei(config-gpon-lineprofile-5)#qos-mode gem-car
huawei(config-gpon-lineprofile-5)#gem add 1 eth tcont 1 gem-car 6
huawei(config-gpon-lineprofile-5)#mapping-mode port
huawei(config-gpon-lineprofile-5)#gem mapping 1 0 eth 1
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

To modify GPON ONT line profile 5, and change the DBA profile bound to T-CONT 1 from DBA profile 12 to DBA profile 10, do as follows:

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 10
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

To modify GPON ONT line profile 5, bind GEM index 1 to T-CONT 2, and map GEM index 1 to ONT ETH port 2, do as follows:

NOTE

If a GEM index is used by a traffic stream, delete this traffic stream first and then the GEM index.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#undo gem mapping 1 0
huawei(config-gpon-lineprofile-5)#gem delete 1
huawei(config-gpon-lineprofile-5)#gem add 1 eth tcont 2
huawei(config-gpon-lineprofile-5)#gem mapping 1 0 eth 2
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

6.1.3 Configuring a GPON ONT Service Profile

The GPON ONT service profile provides a channel for configuring the service of the ONT managed in the OMCI mode. To configure the service of the ONT (such as the MDU) managed in the SNMP mode, you need to log in to the ONT.

Default Configuration

Table 6-5 lists the default settings of the GPON ONT service profile.

Table 6-5 Default settings of the GPON ONT service profile

Parameter	Default Setting
Multicast mode of the ONT	Unconcern (the OLT does not perform any processing)
Mode for the ONT to process the VLAN tag of the multicast data packets	Unconcern
Coding mode for the E1 port of the ONT	HDB3
Source of the priority copied for the upstream packets on the ONT port	Unconcern
QinQ attribute for the Ethernet port of the ONT	Unconcern
Transparent transmission function of the ONT	Disabled
MAC address learning function of the ONT	Enabled

Procedure

Step 1 Run the **ont-srvprofile gpon** command to add a GPON ONT service profile, and then enter the GPON ONT service profile mode.

If the ONT management mode is the SNMP mode, you do not need to configure the service profile. After adding a GPON ONT service profile, directly enter the GPON ONT service profile mode to configure the related items. Select the configuration items according to the service requirements.

Step 2 Configure the Internet access service.

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The capability set plans various types of ports supported by the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

   If the port capability set of an ONT is set to **adaptive**, the OLT automatically adapts to the online ONT according to the OLT's actual capability. By default, eight ETH ports and one IPHOST are displayed.

2. Run the **port vlan** command to configure the port VLAN of the ONT.

Step 3 Configure the voice service.

NOTE

The voice service of the ONT is configured by issuing an XML file to the NMS and the OLT performs only transparent transmission. You only need to run the **service-port** command to create a service port carrying the voice service.

1. Run the **ont-port pots** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.
2. Run the **port vlan** command to configure the port VLAN of the ONT.

Step 4 Configure the multicast service.

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

   If the port capability set of an ONT is set to **adaptive**, the OLT automatically adapts to the online ONT according to the OLT's actual capability. By default, eight ETH ports and one IPHOST are displayed.
2. Run the **port vlan** command to configure the port VLAN of the ONT.
3. Run the **multicast mode** command to configure the multicast mode of the ONT. By default, the multicast mode of the ONT is **unconcern**.
   - Unconcern: indicates the unconcern mode. After this mode is selected, the OLT does not limit the multicast mode, and the multicast mode on the OLT automatically matches the multicast mode on the ONT.
   - Igmp-snooping: IGMP snooping obtains the related information and maintains the multicast forwarding entries by listening to the IGMP packets in the communication between the user and the multicast router.
   - Olt-control: indicates the dynamic controllable multicast mode. A multicast forwarding entry can be created for the multicast join packet of the user only after the packet passes the authentication. This mode is supported by the MDU, but is not supported by the ONT.
4. Run the **multicast-forward** command to configure the processing mode on the VLAN tag of the multicast data packets for the ONT. By default, the multicast forwarding mode of the ONT is **unconcern**.
   - Unconcern: indicates the unconcern forwarding mode. After this mode is selected, the OLT does not process the VLAN tag of the multicast data packets.
   - Tag: Set the multicast forwarding mode to contain the VLAN tag. To transparently transmit the VLAN tag of the multicast packets, select **transparent**. To switch the VLAN tag of the multicast packets, select **translation**, and then configure the VLAN ID that is switched to.
   - Untag: Set the multicast forwarding mode not to contain the VLAN tag.

Step 5 Configure the E1 service.

1. Run the **ont-port e1** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.
2. Run the **port vlan** command to configure the port VLAN of the ONT.
3. Run the **port e1** command to configure the coding mode supported by the E1 port of the ONT. By default, the E1 port supports the HDB3 coding mode. The coding mode must be the same as that on the interconnected device.

Step 6 Configure the transparent LAN service (TLS).

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

   If the port capability set of an ONT is set to **adaptive**, the OLT automatically adapts to the online ONT according to the OLT's actual capability. By default, eight ETH ports and one IPHOST are displayed.

2. Run the **port vlan** command to configure the port VLAN of the ONT.
3. Run the **port q-in-q eth *ont-portid* enable** command to enable the QinQ function of the Ethernet port on the ONT. By default, the QinQ function of the Ethernet port on the ONT is unconcerned.
4. Run the **port priority-policy** command to configure the source of the priority copied for the upstream packets on the ONT port. By default, the source of the priority copied for the upstream packets on the ONT Ethernet port is unconcerned.
   - Unconcern: The source of the priority copied for the upstream packets on the Ethernet port of the ONT is not concerned.
   - assigned: Specifies the priority. Run the **ont port native-vlan** command to specify the **priority** of the port.
   - Copy-cos: Copy the priority. Copy the priority from C-TAG.
5. Run the **transparent enable** command to enable the transparent transmission function of the ONT. By default, the transparent transmission function of the ONT is disabled. After the transparent transmission function of the ONT is enabled, all packets (including service packets and protocol packets) are transparently transmitted by the ONT.

NOTE

The service port for the TLS service must also be of the TLS type. Run the **service-port** command to create a service port of the TLS type. Select **other-all** for the multi-service type.

Step 7 Configure the 1:1 (that is, packets reported by the ONT must contain two VLAN tags) service.

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

   If the port capability set of an ONT is set to **adaptive**, the OLT automatically adapts to the online ONT according to the OLT's actual capability. By default, eight ETH ports and one IPHOST are displayed.

2. Run the **port vlan** command to configure the port VLAN of the ONT.
3. Run the **port q-in-q eth *ont-portid* enable** command to enable the QinQ function of the Ethernet port on the ONT. By default, the QinQ function of the Ethernet port on the ONT is unconcerned.
4. Run the **port priority-policy** command to configure the source of the priority copied for the upstream packets on the ONT port. By default, the source of the priority copied for the upstream packets on the ONT Ethernet port is unconcerned.
   - Unconcern: The source of the priority copied for the upstream packets on the Ethernet port of the ONT is not concerned.
   - assigned: Specifies the priority. Run the **ont port native-vlan** command to specify the **priority** of the port.
   - Copy-cos: Copy the priority. Copy the priority from C-TAG.
5. Run the **transparent disable** command to disable the transparent transmission function of the ONT.

Step 8 Run the **mac-learning** command to configure the MAC address learning function of the ONT. This function is enabled by default.

Step 9 Run the **commit** command to make the parameters of the profile take effect. The configuration of the service profile takes effect only after you perform this operation.

NOTE

If this profile is not bound, all the parameters that are configured take effect when the profile is bound. If this profile is already bound, the configuration takes effect on all ONTs bound to this profile immediately.

Step 10 Run the **quit** command to return to the global config mode.

----End

Example

Assume that the profile is used for the Internet access service, the ONT supports four ETH ports, and the VLAN ID of the ETH ports is 10. To add GPON ONT service profile 5, do as follows:

```
huawei(config)#ont-srvprofile gpon profile-id 5
huawei(config-gpon-srvprofile-5)#ont-port eth adaptive
huawei(config-gpon-srvprofile-5)#port vlan eth 1-4 10
huawei(config-gpon-srvprofile-5)#commit
huawei(config-gpon-srvprofile-5)#quit
```

Assume that the profile is used for the multicast service, the ONT supports four ETH ports, the VLAN ID of the ETH ports is 100, and the multicast mode of the ONT is the controllable multicast mode (you need to switch the multicast VLAN tag to 841 because the STB only supports carrying the VLAN tag of 841). To add GPON ONT service profile 6, do as follows:

```
huawei(config)#ont-srvprofile gpon profile-id 6
huawei(config-gpon-srvprofile-6)#ont-port eth adaptive
huawei(config-gpon-srvprofile-6)#port vlan eth 1-4 100
huawei(config-gpon-srvprofile-6)#multicast mode olt-control
huawei(config-gpon-srvprofile-6)#multicast-forward tag translation 841
huawei(config-gpon-srvprofile-6)#commit
huawei(config-gpon-srvprofile-6)#quit
```

6.1.4 Configuring a GPON ONT Alarm Profile

This topic describes how to add an alarm profile, and configure most of the performance parameters for various ONT lines as a profile. After the alarm profile is configured and bound successfully, the ONT can directly use the profile when it is activated.

Context

An ONT alarm profile defines a series of alarm thresholds that are used to monitor the performance of an activated ONT line. When the statistics result of a parameter reaches the alarm threshold, the NE is notified and an alarm is sent to the log server and the NMS.

- The MA5600T/MA5603T supports up to 50 alarm profiles.
- The system contains a default alarm profile with the ID 1. This profile cannot be deleted but can be modified.

Procedure

Step 1 Run the **gpon alarm-profile add** command to add a GPON ONT alarm profile.

All parameters in the default profile are set to 0, which indicates that no alarm is reported. When an alarm profile is created, the default values of all alarm thresholds are 0, which indicates that no alarm is reported.

Step 2 Run the **display gpon alarm-profile** command to query the alarm profile.

----End

Example

To add GPON ONT alarm profile 5, set the alarm threshold for the packet loss of the GEM port to 10, set the alarm threshold for the number of mis-transmitted packets to 30, and use the default value 0 for all other thresholds, do as follows:

```
huawei(config)#gpon alarm-profile add profile-id 5
{ <cr>|profile-name<K> }:

  Command:
          gpon alarm-profile add profile-id 5
  Press 'Q' or 'q' to quit input
>  GEM port loss of packets threshold (0~100)[0]:                     10
>  GEM port misinserted packets threshold (0~100)[0]:                 30
>  GEM port impaired blocks threshold (0~100)[0]:
>  Ethernet FCS errors threshold (0~100)[0]:
>  Ethernet excessive collision count threshold (0~100)[0]:
>  Ethernet late collision count threshold (0~100)[0]:
>  Too long Ethernet frames threshold (0~100)[0]:
>  Ethernet buffer (Rx) overflows threshold (0~100)[0]:
>  Ethernet buffer (Tx) overflows threshold (0~100)[0]:
>  Ethernet single collision frame count threshold (0~100)[0]:
>  Ethernet multiple collisions frame count threshold (0~100)[0]:
>  Ethernet SQE count threshold (0~100)[0]:
>  Ethernet deferred transmission count threshold (0~100)[0]:
>  Ethernet internal MAC Tx errors threshold (0~100)[0]:
>  Ethernet carrier sense errors threshold (0~100)[0]:
>  Ethernet alignment errors threshold (0~100)[0]:
>  Ethernet internal MAC Rx errors threshold (0~100)[0]:
>  PPPOE filtered frames threshold (0~100)[0]:
>  MAC bridge port discarded frames due to delay threshold (0~100)[0]:
>  MAC bridge port MTU exceeded discard frames threshold (0~100)[0]:
>  MAC bridge port received incorrect frames threshold (0~100)[0]:
>  CES general error time threshold(0~100)[0]:
>  CES severely time threshold(0~100)[0]:
>  CES bursty time threshold(0~100)[0]:
>  CES controlled slip threshold(0~100)[0]:
>  CES unavailable time threshold(0~100)[0]:
>  Drop events threshold(0~100)[0]:
>  Undersize packets threshold(0~100)[0]:
>  Fragments threshold(0~100)[0]:
>  Jabbers threshold(0~100)[0]:
>  Failed signal of ONT threshold(Format:1e-x, x: 3~8)[3]:
>  Degraded signal of ONT threshold(Format:1e-x, x: 4~9)[4]:
>  FEC uncorrectable code words threshold(0~1101600000)[0]:
>  FEC correctable code words threshold(0~1101600000)[0]:
>  Upstream PQ discarded byte alarm threshold(0~65535)[0]:6
>  Downstream PQ discarded byte alarm threshold(0~65535)[0]:6
>  XGEM key errors threshold(0~100)[0]:
>  XGEM HEC error count threshold(0~100)[0]:

  Adding an alarm profile succeeded
  Profile ID  : 5
  Profile name: alarm-profile_5

huawei(config)#display gpon alarm-profile profile-id 5
  ---------------------------------------------------------------
  Profile ID  : 5
  Profile name: alarm-profile_5
```

```
--------------------------------------------------------------
GEM port loss of packets threshold:                        10
GEM port misinserted packets threshold:                    30
GEM port impaired blocks threshold:                        0
Ethernet FCS errors threshold:                             0
Ethernet excessive collision count threshold:              0
Ethernet late collision count threshold:                   0
Too long Ethernet frames threshold:                        0
Ethernet buffer (Rx) overflows threshold:                  0
Ethernet buffer (Tx) overflows threshold:                  0
Ethernet single collision frame count threshold:           0
Ethernet multiple collisions frame count threshold:        0
Ethernet SQE count threshold:                              0
Ethernet deferred transmission count threshold:            0
Ethernet internal MAC Tx errors threshold:                 0
Ethernet carrier sense errors threshold:                   0
Ethernet alignment errors threshold:                       0
Ethernet internal MAC Rx errors threshold:                 0
PPPOE filtered frames threshold:                           0
MAC bridge port discarded frames due to delay threshold:   0
MAC bridge port MTU exceeded discard frames threshold:     0
MAC bridge port received incorrect frames threshold:       0
CES general error time threshold:                          0
CES severely time threshold:                               0
CES bursty time threshold:                                 0
CES controlled slip time threshold:                        0
CES unavailable time threshold:                            0
Drop events threshold:                                     0
Undersize packets threshold:                               0
Fragments threshold:                                       0
Jabbers threshold:                                         0
Failed signal of ONU threshold (Format:1e-x):              3
Degraded signal of ONU threshold (Format:1e-x):            4
FEC uncorrectable code words threshold:                    0
FEC correctable code words threshold:                      0
Upstream PQ discarded byte alarm threshold:                6
Downstream PQ discarded byte alarm threshold:              6
XGEM key errors threshold:                                 0
XGEM HEC error count threshold:                            0
--------------------------------------------------------------
Binding Times:                                             0
--------------------------------------------------------------
```

6.2 Creating a VLAN

Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see **Table 6-6**.

Table 6-6 VLAN planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN type: smart
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S +C.	
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	

Default Configuration

Table 6-7 lists the default parameter settings of VLAN.

Table 6-7 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart VLAN	You can run the **defaultvlan modify** command to modify the VLAN type but cannot delete the VLAN.
Reserved VLAN of the system	VLAN ID range: 4079-4093	You can run the **vlan reserve** command to modify the VLAN reserved by the system.

Prerequisite

- The VLAN to be added should not exist in the system.
- Service VLAN cannot be reserve VLAN.

Procedure

Step 1 Create a VLAN.

Run the **vlan** to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 6-8 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the **vlan** ***vlanid*** **standard** command.	Standard VLAN. Ethernet ports in a standard VLAN are interconnected with each other but Ethernet ports in different standard VLANs are isolated from each other.	Only available to Ethernet ports and specifically to network management and subtending.
Smart VLAN	To add a smart VLAN, run the **vlan** ***vlanid*** **smart** command.	One VLAN may contain multiple xDSL service ports or xPON service ports. The traffic streams of these ports, however, are isolated from each other. In addition, the traffic streams of different VLANs are also isolated. One smart VLAN provides access for multiple users and therefore saves VLAN resources.	Smart VLANs can be applied in residential communities to provide xDSL or xPON service access.
MUX VLAN	To add a MUX VLAN, run the **vlan** ***vlanid*** **mux** command.	One MUX VLAN contains only one xDSL service port or xPON service port. The traffic streams in different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. Hence, a MUX VLAN can identify an access user.	MUX VLANs are applicable to xDSL or xPON service access. For example, MUX VLANs can be used to distinguish users.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Super VLAN	To add a super VLAN, run the **vlan *vlanid* super** command.	The super VLAN is based on Layer 3. One super VLAN contains multiple sub-VLANs. Through an ARP proxy, the sub-VLANs in a super VLAN can be interconnected at Layer 3.	Super VLANs save IP addresses and improve the utilization of IP addresses. For a super VLAN, sub-VLANs must be configured. You can run the **supervlan** command to add a sub-VLAN to a specified super VLAN. A sub-VLAN must be a smart VLAN or MUX VLAN.

NOTE

- To add VLANs with consecutive IDs in batches, run the **vlan *vlanid* to *end-vlanid*** command.
- To add VLANs with inconsecutive IDs in batches, run the **vlan *vlan-list*** command.

----End

Example

Create VLAN 50 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 50 smart
```

Create VLAN 55-60 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 55 to 60 smart
```

Create VLAN 65, 73 and 52 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 65,73,52 smart
```

6.3 Configuring an Upstream Port

The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.

Prerequisites

The planned virtual local area network (VLAN) is already configured.

Procedure

Step 1 Configure an upstream port for the VLAN.

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

Step 2 Configure the attribute of the upstream port.

If the default attribute of the upstream port does not meet the requirement for interconnection of the upstream port with the upper-layer device, you need to configure the attribute. For configuration details, see **2.5 Configuring the Attributes of an Upstream Ethernet Port**.

Step 3 (Optional) Configure redundancy backup for the uplink.

To ensure reliability of the uplink, two upstream ports must be available. That is, redundancy backup of the upstream ports needs to be configured. For details, see **14.1 Configuring Ethernet Link Aggregation**.

----End

Example

Assume that the 0/19/0 and 0/19/1 upstream ports are to be added to VLAN 50. The 0/19/0 and 0/19/1 need to be configured into an aggregation group for double upstream accesses. For the two upstream ports, the working mode is full-duplex (full) and the port rate is 100 Mbit/s. To configure such upstream ports, do as follows:

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#duplex 0 full
huawei(config-if-giu-0/19)#duplex 1 full
huawei(config-if-giu-0/19)#speed 0 100
huawei(config-if-giu-0/19)#speed 1 100
huawei(config-if-giu-0/19)#quit
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

6.4 Configuring a GPON ONT

The MA5600T/MA5603T provides end users with services through the ONT. The MA5600T/MA5603T can manage the ONT and the ONT can work in the normal state only after the channel between the MA5600T/MA5603T and the ONT is available.

Prerequisites

The GPON ONT profile is already created.

- For an ONT, **6.1.2 Configuring a GPON ONT Line Profile**, **6.1.3 Configuring a GPON ONT Service Profile**, and **6.1.4 Configuring a GPON ONT Alarm Profile** are already completed.
- For an MDU or ONU, **6.1.2 Configuring a GPON ONT Line Profile** and **6.1.4 Configuring a GPON ONT Alarm Profile** are already completed.

Context

The MA5600T/MA5603T uses the ONT Management and Control Interface (OMCI) protocol to manage and configure the GPON ONT, and supports the offline configuration of the ONT.

In the profile mode, the related configuration of the GPON ONT is already integrated in the service profile and the line profile. When adding an ONT, you only need to bind the ONT with the corresponding service profile and line profile.

Table 6-9 lists the default settings of the GPON ONT.

Table 6-9 Default settings of the GPON ONT

Parameter	Default Setting
ONT auto-find function of a GPON port	Disabled
ONT status after an ONT is added	Activated
Default VLAN of the ONT port	1

Procedure

Step 1 Run the **interface gpon** command to enter the GPON mode.

Step 2 Add a GPON ONT.

1. Run the **port** ***portid*** **ont-auto-find** command to enable the auto discovery function of the ONT. After the function is enabled, you can add an ONT according to the information reported by the system. By default, the ONT auto discovery function of a GPON port is disabled.

   NOTE

   An auto discovery ONT is in the auto discovery state. The auto discovery ONT can work in the normal state only after it is confirmed or added.

2. Run the **ont add** command to add an ONT offline, or run the **ont confirm** command to confirm the auto discovery ONT.

   When ONTs are added or confirmed, the system provides four authentication modes: SN, password, SN+password, LOID+CHECKCODE.

   - SN authentication: The OLT detects the serial number (SN) reported by an ONT. If the SN is consistent with the OLT configuration, authentication is passed and the ONT goes online. This mode requires recording all ONT SNs. Hence, it is used to confirm auto discovery ONTs and is not applicable to adding ONTs in batches.
   - Password authentication: The OLT detects the password reported by an ONT. If the password is consistent with the OLT configuration, the ONT goes online normally. This mode requires planning ONT passwords and does not require manually recording ONT SNs. Hence, it is applicable to adding ONTs in batches. The password authentication provides two discovery modes: always-on and once-on.
     - always-on: After first password authentication is passed, no SN is allocated and password authentication is always used in subsequent authentications. This discovery mode is easy for future maintenance. In the always-on discovery mode, configuration is not required to be modified when an ONT is replaced and only the password is required. The always-on discovery mode has lower security. If other users know the password, the users will illegally have service permissions.
     - Once-on: After first password authentication is passed, an SN is automatically allocated and password+SN authentication is used in subsequent authentications. An ONT can go online only after the correct password and SN are entered. The once-on authentication mode has high security. After an ONT is replaced or the password is mistakenly changed, the ONT needs to be configured again, which requires more maintenance effort.
   - SN+password authentication: The OLT detects the password and SN reported by an ONT. If the password and SN are consistent with the OLT configuration, the ONT goes

online normally. This authentication mode has the highest security but it requires manually recording ONT SNs.

- LOID+CHECKCODE authentication: defined by a telecom operator. In this authentication mode, LOID has 24 bytes, and CHECKCODE has 12 bytes and is optional. Whether 24 bytes or 36 bytes are used for authentication depends on data planning, which is unified over the entire network. The OLT determines whether LOID +CHECKCODE reported by the ONT is the same as the configured one. If they are the same, the ONT authentication is passed. If they are different, the OLT obtains the ONT password and compares it with the last 10 bytes of the LOID. If they are the same, the ONT authentication is also passed. This operation is for compatibility with the ONTs using password authentication.

Adding ONTs in offline mode is applicable to the batch deployment scenario. All ONTs are added to the OLT to complete service provisioning beforehand. When a use subscribes to the service, an installation engineer takes an ONT to the user's house and completes configurations. After the ONT goes online and passes authentication (generally the password authentication mode or LOID authentication mode is used), the service is provisioned.

Adding ONTs in auto discovery mode is applicable to the scenario where a small number of ONTs are added. When users subscribe to the service, installation engineers take ONTs to the users' houses. After the ONTs go online, the OLT confirms the ONTs one by one. Generally, the MAC address authentication mode is used to confirm the ONTs.

NOTE

- If the ONU is an independent NE and is directly managed by the NMS through the SNMP management mode, select the SNMP management mode. For this mode, you only need to configure the parameters for the GPON line and the parameters for the management channel on the OLT. You only need to bind the ONU with a line profile.
- If the ONU is not an independent NE and all its configuration data is issued by the OLT through OMCI, select the OMCI management mode. For this mode, you need to configure all parameters (including line parameters, UNI port parameters, and service parameters) that are required for the ONU on the OLT. Configuring management channel parameters is not supported. You need to bind the ONT with a line profile and a service profile.
- Generally, the ONT management mode is set to the OMCI mode. You need to bind the ONT with a line profile and a service profile.

3. (Optional) When the ONT management mode is the SNMP mode, you need to configure the SNMP management parameters for the ONT. The procedure is as follows:

   a. Run the **ont ipconfig** command to configure the management IP address of the ONT.

      The IP address should not be in the same subnet for the IP address of the VLAN port.

   b. Run the **ont snmp-profile** command to bind the ONT with an SNMP profile.

      Run the **snmp-profile add** command to add an SNMP profile before the configuration.

   c. Run the **ont snmp-route** command to configure a static route for the NMS server, that is, configure the IP address of the next hop.

Step 3 Configure the default VLAN (native VLAN) for the ONT port.

Run the **ont port native-vlan** command to configure the default VLAN for the ONT port. By default, the default VLAN ID of the ONT port is 1.

- If the packets reported from a user (such a PC) to the ONT are untagged, the packets are tagged with the default VLAN of the port on the ONT and then reported to the OLT.

- If the packets reported from a user to the ONT are tagged, you need to configure the port VLAN of the ONT to be the same as the VLAN in the user tag. The packets are not tagged with the default VLAN of the port on the ONT but are reported to the OLT with the user tag.

Step 4 Bind an alarm profile.

Run the **ont alarm-profile** command bind an alarm profile. Ensure that **6.1.4 Configuring a GPON ONT Alarm Profile** is completed before the configuration.

Step 5 Activate the ONT.

Run the **ont activate** command to activate the ONT. The ONT can transmit services only when it is in the activated state.

After being added, the ONT is in the activated state by default. The step is required only when the ONT is in the deactivated state.

Step 6 Query the ONT status.

Run the **display ont info** command to query the ONT running status, configuration status, and matching status.

----End

Example

To add five ONTs in offline mode with password authentication mode (ONT passwords are 0100000001-0100000005), set the discovery mode of password authentication to always-on, and bind line profile 10 and service profile 10, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000001 always-on omci ont-
lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 password-auth 0100000002 always-on omci ont-
lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#ont add 2 password-auth 0100000003 always-on omci ont-
lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#ont add 3 password-auth 0100000004 always-on omci ont-
lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#ont add 4 password-auth 0100000005 always-on omci ont-
lineprofile-id 10 ont-srvprofile-id 10
```

To add an ONT that is managed by the OLT through the OMCI protocol, confirm this ONT according to the SN 3230313185885B41 automatically reported by the system, and bind the ONT with line profile 3 and service profile 3 that match the ONT, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/2)#ont confirm 0 sn-auth 3230313185885B41 omci ont-
lineprofile-id 3 ont-srvprofile-id 3
```

To add an ONU that is managed as an independent NE and whose SN is known as 3230313185885641, bind the ONU with line profile 4 that matches the ONU, configure the NMS parameters for the ONU, and set the management VLAN to 100, do as follows:

```
huawei(config)#snmp-profile add profile-id 1 v2c public private 10.10.5.53 161
huawei
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 2 sn-auth 3230313185885641 snmp ont-
lineprofile-id 4
huawei(config-if-gpon-0/2)#ont ipconfig 0 2 static ip-address 10.20.20.20 mask
255.255.255.0 gateway 10.10.20.1 vlan 100
huawei(config-if-gpon-0/2)#ont snmp-profile 0 2 profile-id 1
huawei(config-if-gpon-0/2)#ont snmp-route 0 2 ip-address 10.10.20.190 mask
255.255.255.0 next-hop 10.10.20.100
```

6.5 Configuring a GPON Port

To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.

Default Configuration

Table 6-10 lists the default settings of the GPON port.

Table 6-10 Default settings of the GPON port

Parameter	Default Setting
GPON port	Enabled
Downstream FEC function of the GPON port	Disabled
Compensation distance range of the GPON port ranging	Minimum logical distance: 0 km; maximum logical distance: 20 km

Procedure

Step 1 Run the **interface gpon** command to enter the GPON mode.

Step 2 Configure the laser of the GPON port.

- Run the **undo shutdown** command to enable the laser of the GPON port. By default, the laser of the GPON port is enabled and the GPON port is available. In this case, skip this step.
- If the GPON port is not to be used, run the **shutdown** command to disable the laser of the GPON port.

⚠ **CAUTION**

Disabling a PON port that carries services will cause the interruption of such services.

Step 3 Configure the downstream FEC function of the GPON port.

Run the **port** ***portid*** **fec** command to configure the FEC function of the GPON port. By default, the FEC function is disabled.

NOTE

- FEC is to insert redundant data into normal packets so that the line has certain error tolerance. Some bandwidth, however, must be consumed. Enabling FEC enhances the error correction capability of the line but at the same time occupies certain bandwidth. Determine whether to enable FEC according to the actual line planning.
- If a large number of ONTs are already online, enabling FEC on the GPON port may cause certain ONTs to go offline. Therefore, it is suggested that FEC should not be enabled on a GPON port that connects to online ONTs.

Step 4 Configure the renewal time of the ONT key.

Run the **port** ***portid*** **ont-password-renew** command to configure the interval for renewing the ONT key. To ensure the system security, the ONT key renewal must be configured.

Step 5 Configure the compensation distance in the ranging.

Run the **port** ***portid*** **range** command to configure the compensation distance range of the GPON port ranging. By default, the minimum logical distance is 0 km, and the maximum logical distance is 20 km. The difference between the minimum logical distance and the maximum logical distance must not exceed 20 km.

Step 6 (Optional) Configure the DBA calculation period on a GPON port basis.

When different GPON ports provide different access services, the bandwidth delays on these ports are different. In this case, the DBA calculation period needs to be configured on a GPON port basis.

1. In GPON board mode, run the **port dba bandwidth-assignment-mode** command to configure the DBA mode on a GPON port.
2. In diagnose mode, run the **gpon port dba calculate-period** command to configure the DBA calculation period on the GPON port.

NOTE

- The DBA calculation period on a GPON port can be configured only when the DBA mode is set to **manual** on this GPON port.
- By default, the DBA mode on a GPON port is **default**, which means the global DBA mode is used as the bandwidth assignment mode for the GPON port. In this case, if the global DBA mode is modified by running the **gpon dba bandwidth-assignment-mode** command, the bandwidth assignment mode on the GPON port is also modified. If the DBA mode on a GPON port is not **default**, the bandwidth assignment mode on the GPON port is not affected by the global DBA mode.
- If ONTs are configured on a GPON port, modifying the DBA mode is not allowed on this GPON port.
- For the TDM service, the DBA mode must be set to **min-loop-delay**.

----End

Example

Assume that the key renew interval of the ONT under the port is 10 hours, the minimum compensation distance of ranging is 10 km, and the maximum compensation distance of ranging is 15 km. To enable the FEC function of GPON port 0/2/0, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 fec enable
huawei(config-if-gpon-0/2)#port 0 ont-password-renew 10
huawei(config-if-gpon-0/2)#port 0 range min-distance 10 max-distance 15
  This command will result in the ONT's re-register in the port.
  Are you sure to execute this command? (y/n)[n]: y
```

To set the global DBA mode to **min-loop-delay**, DBA mode on GPON port 0/2/0 to **manual**, and DBA calculation period to **4**, do as follows:

```
huawei(config)#gpon dba bandwidth-assignment-mode min-loop-delay
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port dba bandwidth-assignment-mode 0 manual
huawei(config-if-gpon-0/2)#quit
huawei(config)#diagnose
huawei(diagnose)%%gpon port dba calculate-period 0/2/0 4
```

6.6 Creating a GPON Service Port

A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

Context

A service port can carry a single service or multiple services. When a service port carries multiple services, the MA5600T/MA5603T supports the following modes of classifying traffic:

- By user-side VLAN
- By user-side service encapsulation mode
- By VLAN+user-side packet priority
- By VLAN+user-side service encapsulation mode

Table 6-11 lists the default settings of a service port.

Table 6-11 Default settings of a service port

Parameter	Default Setting
Traffic profile ID	0-6
Administrative status of the service port	Activated
Maximum number of MAC addresses that are learned	1023

Procedure

Step 1 Create a traffic profile.

Run the **traffic table ip** command to create a traffic profile. There are seven default traffic profiles in the system with the IDs of 0-6.

Before creating a service port, run the **display traffic table** command to check whether the traffic profiles in the system meet the requirement. If no traffic profile in the system meets the requirement, add a traffic profile that meets the requirement. For details about the traffic profile, see **Configuring Traffic Management Based on Service Port**.

Step 2 Create a service port.

You can choose to create a single service port or multiple service ports in batches according to requirements.

- Run the **service-port** command to create a single service port. Service ports are classified into single-service service ports and multi-service service ports. Multi-service service ports are generally used for the triple play service.
  - Single-service service port:

    By default, a service port is a single-service service port if you do not enter **multi-service**.
  - Multi-service service port based on the user-side VLAN:

    Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** | **other-all** }.
    - **untagged**: When **untagged** is selected, user-side packets do not carry a tag.
    - *user-vlanid*: When *user-vlanid* is selected, user-side packets carry a tag and the value of *user-vlanid* must be the same as the tag carried in user-side packets, that is, C-VLAN.
    - **priority-tagged**: When **priority-tagged** is selected, the VLAN tag is 0 and the priorities of user-side packets are 0-7.
    - **other-all**: When **other-all** is selected, service ports for the transparent LAN service (TLS) are created, which are mainly used in the QinQ transparent transmission service for enterprises. All the traffic except known traffic in the system is carried over this channel.
  - Multi-service service port based on the user-side service encapsulation mode:

    Select **multi-service user-encap** *user-encap*.
  - Multi-service service port based on VLAN+user-side packet priority (802.1p):

    Select **multi-service user-8021p** *user-8021p* [**user-vlan** *user-vlanid*].
  - Multi-service service port based on VLAN + user-side service encapsulation mode (user-encap):

    Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** } **user-encap** *user-encap*.

  📖 NOTE

  - The system supports creating service ports by index. One index maps one service port and the input of a large number of traffic parameters is not required. Therefore, the configuration of service ports is simplified. During the creation of a service port, *index* indicates the index of the service port and it is optional. If it is not input, the system automatically adopts the smallest value.
  - **vlan** indicates the S-VLAN. An S-VLAN can only be a MUX VLAN or smart VLAN.
  - **rx-cttr** is the same as **outbound** in terms of meanings and functions. Either of them indicates the index of the traffic from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meanings and functions. Either of them indicates the index of the traffic from the user side to the network side. The traffic profile bound to the service port is created in **Step 1**.
- Run the **multi-service-port** command to create service ports in batches.

Step 3 Configure the attributes of the service port. Configure the attributes of the service port according to requirements.

- Run the **service-port desc** command to configure the description of the service port. Configure the description for a service port to facilitate maintenance. In general, configure the purpose and related service information as the description of a service port.
- Run the **service-port** ***index*** **adminstatus** command to configure the administrative status of the service port. By default, a service port is in the activated state.

A service port can be activated at two levels: port level and service port level. To provision services for a user, the access port and the corresponding service port of the user must be activated.

- Run the **mac-address max-mac-count service-port** command to configure the maximum number of MAC addresses learned by the service port to restrict the maximum number of PCs that can access the Internet by using a same account. By default, the maximum number of MAC addresses learned by the service port is 1023.

----End

Example

Connect ONT 1 to GPON port 0/2/0 of the MA5600T/MA5603T. Plan an Internet access user. The ONT provides the Internet-access-only service with a rate of 4096 kbit/s for this user, the index of the GEM port that carries the service is 126, the service VLAN ID is 1000, and only three users are allowed to use a same account for Internet access at the same time. The query shows that there is no proper traffic profile in the system. Then, create traffic profile 10. This user is not registered yet. Therefore, the service is not provided for the user for the moment. To configure such a user, do as follows:

```
huawei(config)#traffic table ip index 10 cir 4096 priority 3 priority-policy loc
al-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 10
  TD Name              : ip-traffic-table_10
  Priority             : 3
  Mapping Priority     : -
  Mapping Index        : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                  : 4096 kbps
  CBS                  : 133072 bytes
  PIR                  : 8192 kbps
  PBS                  : 264144 bytes
  Color policy         : dei
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 5 vlan 1000 gpon 0/2/0 ont 1 gemport 126 inbound
traffic-table index 10 outbound traffic-table index 10
huawei(config)#mac-address max-mac-count service-port 5 3
huawei(config)#service-port 5 adminstatus disable
```

Connect ONT 2 to GPON port 0/2/0 of the MA5600T/MA5603T. A commercial user requires the Internet access service with a rate of 8192 kbit/s to be provided. For subsequent service expansion, the ONT provides the Internet access service for this user in the multi-service mode. The user is differentiated based on the user-end VLAN, S-VLAN ID is 1023, C-VLAN ID is 100, and the index of the GEM port that carries the service is 126. The query shows that there is no proper traffic profile in the system. Then, create traffic profile 8. The Internet access service is required to be provided immediately. The description of the service port is added to facilitate maintenance. To configure such a user, do as follows:

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ----------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ----------------------------------------------------------------------------
  Total Num : 7
huawei(config)#traffic table ip index 8 cir 8192 priority 4 priority-policy
 local-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index            : 8
  TD Name             : ip-traffic-table_8
  Priority            : 4
  Copy Priority       : -
  Mapping Index       : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                 : 8192 kbps
  CBS                 : 264144 bytes
  PIR                 : 16384 kbps
  PBS                 : 526288 bytes
  Color policy        : dei
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 10 vlan 1023 gpon 0/2/0 ont 2 gemport 126 multi-
service
 user-vlan 100 inbound traffic-table index 8 outbound traffic-table index 8
huawei(config)#service-port desc 10 description gpon/Vlanid:1023/uservlan:100
```

7 Configuring the GPON Internet Access Service (Simplified Mode)

About This Chapter

The simplified mode of the GPON Internet access service reduces configuration workloads and OM costs. Currently, this mode supports only GPON FTTH scenarios. The simplified mode is recommended for service configuration in newly-built GPON FTTH networks and scenarios with low QoS requirements.

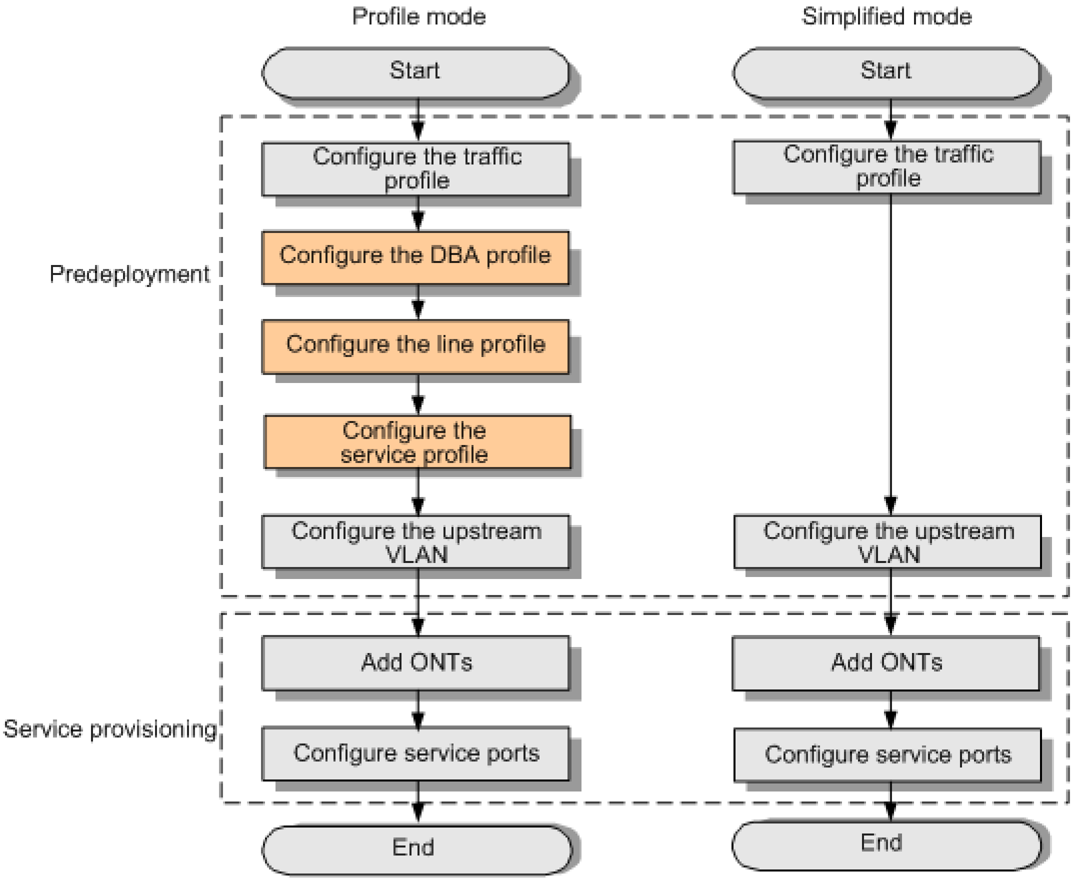
Application Context

FTTH refers to fiber to the home. In this networking scenario, the MA5600T/MA5603T functions as an OLT and is connected to the ONT at lower layer through the ODN. The ONT is connected to subscribers to provide the voice, Internet access, and IPTV services.

Difference Between the Profile Mode and Simplified Mode

In FTTH scenarios, the simplified mode can be used for configuring the GPON service to simplify configurations and reduce costs. **Figure 7-1** shows configuration procedures in profile mode and simplified mode.

Figure 7-1 Configuration flowchart


Profile mode
Simplified mode
Start
Start
Predeployment
Configure the traffic profile
Configure the DBA profile
Configure the line profile
Configure the service profile
Configure the upstream VLAN
Configure the traffic profile
Configure the upstream VLAN
Service provisioning
Add ONTs
Configure service ports
Add ONTs
Configure service ports
End
End

The simplified mode is different from the profile mode in the following aspects:

- GEM ports are allocated automatically by the system.
- The DBA profile, line profile, and service profile do not need to be configured. When being added, an ONT is automatically bound to default line profile 0 and default service profile 0. The default line profile and service profile can be modified but cannot be deleted.
- By default, T-CONT 0 and T-CONT 1 are created in line profile 0. T-CONT 0 is bound to default DBA profile 2 (with 1 Mbit/s fixed bandwidth) and serves as an OMCI channel. T-CONT 1 is bound to default DBA profile 7 (with 8 Mbit/s fixed bandwidth and 20 Mbit/s maximum bandwidth) and serves as a service channel. By default, a GEM port does not exist in T-CONT 1 but is automatically allocated by the system in traffic stream creation. The DBA profile bound to a T-CONT can be modified.
- The type and number of ONT ports in service profile 0 are not limited by the profile but are matched automatically when the ONT goes online. Before an ONT goes online for the first time, eight ETH ports and one IPHOST port are displayed by default.
- The simplified mode applies only to the scenario where multiple traffic streams use the same T-CONT. It is not applicable to the scenario whether different traffic streams use different T-CONTs. All traffic streams on an ONT share the same T-CONT for services; therefore, the traffic streams can be scheduled on the ONT only by GEM port CAR or PQ.
- The QinQ service cannot coexist with the simplified-mode configuration on an ONT. The simplified-mode configuration is not applicable to the open access scenario.

Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.11 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.
- The alarm profile for the Internet access service is created. For details about how to configure an alarm profile, see **6.1.4 Configuring a GPON ONT Alarm Profile**.
- The GPON mode is already switched to the profile mode.

Data Plan

Before configuring the GPON Internet access service, plan the data items as listed in **Table 7-1**.

Table 7-1 Data plan for the GPON Internet access service

Parameter	Data	Remarks
MA5600T/MA5603T	Access rate	Configure the data according to the user requirements.
	Access port	Configure the data according to the network planning.
	VLAN planning	The cooperation with the upper-layer device should be considered in the VLAN planning. The upstream VLAN must be the same as that of the upper-layer device.
	QoS policy	Configure the data according to the QoS policy of the entire network. Generally, the priority of the Internet access service is lower than the priorities of the voice and video services.
ONT	ONT index	GPON supports a split ratio of up to 1:128. You need to plan the ONTs connected to the MA5600T/MA5603T to facilitate management.
	Authentication mode	The password, SN, and LOID +CHECKCODE can be used for authentication.

Parameter	Data	Remarks
Upper-layer LAN switch	The LAN switch transparently transmits the service packets of the MA5600T/MA5603T on L2. The VLAN ID must be the same as the upstream VLAN ID of the MA5600T/MA5603T.	-
BRAS	The BRAS performs the related configurations according to the authentication and accounting requirements for dialup users, for example, configures the access user domain (including the authentication scheme, accounting scheme, and authorization scheme bound to the domain) and specifies the RADIUS server. If the BRAS is used to authenticate users, you need to configure the user name and the password for each user on the BRAS. If the BRAS is used to allocate IP addresses, you need to configure the corresponding IP address pool on the BRAS.	-

Procedure

1. 7.1 Creating a VLAN
   Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.
2. 7.2 Configuring an Upstream Port
   The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.
3. 7.3 Configuring a GPON ONT
   The MA5600T/MA5603T provides end users with services through the ONT. The MA5600T/MA5603T can manage the ONT and the ONT can work in the normal state only after the channel between the MA5600T/MA5603T and the ONT is available.
4. 7.4 Configuring a GPON Port
   To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.
5. 7.5 Creating a GPON Service Port
   A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

7.1 Creating a VLAN

Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see **Table 7-2**.

Table 7-2 VLAN planning

User Type	Application Scenario	VLAN Planning
● Household user ● Commercial user of the Internet access service	N:1 scenario, that is, the scenario of upstream transmission through a single VLAN, where the services of multiple users are converged to the same VLAN.	VLAN type: smart
	1:1 scenario, that is, the scenario of upstream transmission through double VLANs, where the outer VLAN tag identifies a service and the inner VLAN tag identifies a user. The service of each user is indicated by a unique S+C.	
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	

Default Configuration

Table 7-3 lists the default parameter settings of VLAN.

Table 7-3 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart VLAN	You can run the **defaultvlan modify** command to modify the VLAN type but cannot delete the VLAN.
Reserved VLAN of the system	VLAN ID range: 4079-4093	You can run the **vlan reserve** command to modify the VLAN reserved by the system.

Prerequisite

- The VLAN to be added should not exist in the system.
- Service VLAN cannot be reserve VLAN.

Procedure

Step 1 Create a VLAN.

Run the **vlan** to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 7-4 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the **vlan** ***vlanid*** **standard** command.	Standard VLAN. Ethernet ports in a standard VLAN are interconnected with each other but Ethernet ports in different standard VLANs are isolated from each other.	Only available to Ethernet ports and specifically to network management and subtending.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Smart VLAN	To add a smart VLAN, run the **vlan** ***vlanid*** **smart** command.	One VLAN may contain multiple xDSL service ports or xPON service ports. The traffic streams of these ports, however, are isolated from each other. In addition, the traffic streams of different VLANs are also isolated. One smart VLAN provides access for multiple users and therefore saves VLAN resources.	Smart VLANs can be applied in residential communities to provide xDSL or xPON service access.
MUX VLAN	To add a MUX VLAN, run the **vlan** ***vlanid*** **mux** command.	One MUX VLAN contains only one xDSL service port or xPON service port. The traffic streams in different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. Hence, a MUX VLAN can identify an access user.	MUX VLANs are applicable to xDSL or xPON service access. For example, MUX VLANs can be used to distinguish users.
Super VLAN	To add a super VLAN, run the **vlan** ***vlanid*** **super** command.	The super VLAN is based on Layer 3. One super VLAN contains multiple sub-VLANs. Through an ARP proxy, the sub-VLANs in a super VLAN can be interconnected at Layer 3.	Super VLANs save IP addresses and improve the utilization of IP addresses. For a super VLAN, sub-VLANs must be configured. You can run the **supervlan** command to add a sub-VLAN to a specified super VLAN. A sub-VLAN must be a smart VLAN or MUX VLAN.

NOTE

- To add VLANs with consecutive IDs in batches, run the **vlan *vlanid* to *end-vlanid*** command.
- To add VLANs with inconsecutive IDs in batches, run the **vlan *vlan-list*** command.

----End

Example

Create VLAN 50 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 50 smart
```

Create VLAN 55-60 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 55 to 60 smart
```

Create VLAN 65, 73 and 52 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 65,73,52 smart
```

7.2 Configuring an Upstream Port

The uplink port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.

Prerequisites

The planned virtual local area network (VLAN) is already configured.

Procedure

Step 1 Configure an upstream port for the VLAN.

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

Step 2 Configure the attribute of the upstream port.

If the default attribute of the upstream port does not meet the requirement for interconnection of the upstream port with the upper-layer device, you need to configure the attribute. For configuration details, see **2.5 Configuring the Attributes of an Upstream Ethernet Port**.

Step 3 (Optional) Configure redundancy backup for the uplink.

To ensure reliability of the uplink, two upstream ports must be available. That is, redundancy backup of the upstream ports needs to be configured. For details, see **14.1 Configuring Ethernet Link Aggregation**.

----End

Example

Assume that the 0/19/0 and 0/19/1 upstream ports are to be added to VLAN 50. The 0/19/0 and 0/19/1 need to be configured into an aggregation group for double upstream accesses. For the two upstream ports, the working mode is full-duplex (full) and the port rate is 100 Mbit/s. To configure such upstream ports, do as follows:

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#duplex 0 full
huawei(config-if-giu-0/19)#duplex 1 full
huawei(config-if-giu-0/19)#speed 0 100
huawei(config-if-giu-0/19)#speed 1 100
huawei(config-if-giu-0/19)#quit
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

7.3 Configuring a GPON ONT

The MA5600T/MA5603T provides end users with services through the ONT. The MA5600T/MA5603T can manage the ONT and the ONT can work in the normal state only after the channel between the MA5600T/MA5603T and the ONT is available.

Context

The MA5600T/MA5603T uses the ONT Management and Control Interface (OMCI) protocol to manage and configure the GPON ONT, and supports the offline configuration of the ONT. The ONT need not save the configuration information locally. This helps to provision services.

Table 7-5 lists the default settings of the GPON ONT.

Table 7-5 Default settings of the GPON ONT

Parameter	Default Setting
ONT auto-find function of a GPON port	Disabled
ONT status after an ONT is added	Activated

Procedure

Step 1 Run the **interface gpon** command to enter the GPON mode.

Step 2 Add a GPON ONT.

1. Run the **port *portid* ont-auto-find** command to enable the auto-find function of the ONT. After the function is enabled, you can add an ONT according to the information reported by the system. By default, the ONT auto-find function of a GPON port is disabled.

   NOTE

   An auto-find ONT is in the auto-find state. The auto-find ONT can work in the normal state only after it is confirmed or added.

2. Run the **ont add** command to add the ONT offline, or run the **ont confirm** command to confirm the auto-find ONT.

   NOTE

   In the simplified mode, the line profile and service profile do not need to be bound to an ONT when the ONT is added. The ONT is automatically bound to default line profile 0 and default service profile 0.

   When ONTs are added or confirmed, the system provides four authentication modes: SN, password, SN+password, LOID+CHECKCODE.

   - SN authentication: The OLT detects the serial number (SN) reported by an ONT. If the SN is consistent with the OLT configuration, authentication is passed and the ONT goes online. This mode requires recording all ONT SNs. Hence, it is used to confirm auto discovery ONTs and is not applicable to adding ONTs in batches.

- Password authentication: The OLT detects the password reported by an ONT. If the password is consistent with the OLT configuration, the ONT goes online normally. This mode requires planning ONT passwords and does not require manually recording ONT SNs. Hence, it is applicable to adding ONTs in batches. The password authentication provides two discovery modes: always-on and once-on.
  - always-on: After first password authentication is passed, no SN is allocated and password authentication is always used in subsequent authentications. This discovery mode is easy for future maintenance. In the always-on discovery mode, configuration is not required to be modified when an ONT is replaced and only the password is required. The always-on discovery mode has lower security. If other users know the password, the users will illegally have service permissions.
  - Once-on: After first password authentication is passed, an SN is automatically allocated and password+SN authentication is used in subsequent authentications. An ONT can go online only after the correct password and SN are entered. The once-on authentication mode has high security. After an ONT is replaced or the password is mistakenly changed, the ONT needs to be configured again, which requires more maintenance effort.
- SN+password authentication: The OLT detects the password and SN reported by an ONT. If the password and SN are consistent with the OLT configuration, the ONT goes online normally. This authentication mode has the highest security but it requires manually recording ONT SNs.
- LOID+CHECKCODE authentication: defined by a telecom operator. In this authentication mode, LOID has 24 bytes, and CHECKCODE has 12 bytes and is optional. Whether 24 bytes or 36 bytes are used for authentication depends on data planning, which is unified over the entire network. The OLT determines whether LOID +CHECKCODE reported by the ONT is the same as the configured one. If they are the same, the ONT authentication is passed. If they are different, the OLT obtains the ONT password and compares it with the last 10 bytes of the LOID. If they are the same, the ONT authentication is also passed. This operation is for compatibility with the ONTs using password authentication.

Adding ONTs in offline mode is applicable to the batch deployment scenario. All ONTs are added to the OLT to complete service provisioning beforehand. When a use subscribes to the service, an installation engineer takes an ONT to the user's house and completes configurations. After the ONT goes online and passes authentication (generally the password authentication mode or LOID authentication mode is used), the service is provisioned.

Adding ONTs in auto discovery mode is applicable to the scenario where a small number of ONTs are added. When users subscribe to the service, installation engineers take ONTs to the users' houses. After the ONTs go online, the OLT confirms the ONTs one by one. Generally, the MAC address authentication mode is used to confirm the ONTs.

Step 3 Bind an alarm profile.

Run the **ont alarm-profile** command bind an alarm profile. Ensure that **6.1.4 Configuring a GPON ONT Alarm Profile** is completed before the configuration.

Step 4 Activate the ONT.

Run the **ont activate** command to activate the ONT. The ONT can transmit services only when it is in the activated state.

After being added, the ONT is in the activated state by default. The step is required only when the ONT is in the deactivated state.

----End

Example

Assume that five ONTs are authenticated by passwords 0100000001-0100000005 respectively and the discovery mode of these passwords is always-on. To add these ONTs, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000001 always-on omci
huawei(config-if-gpon-0/2)#ont add 1 password-auth 0100000002 always-on omci
huawei(config-if-gpon-0/2)#ont add 2 password-auth 0100000003 always-on omci
huawei(config-if-gpon-0/2)#ont add 3 password-auth 0100000004 always-on omci
huawei(config-if-gpon-0/2)#ont add 4 password-auth 0100000005 always-on omci
```

To add an ONT that is managed by the OLT through the OMCI protocol, confirm this ONT according to the SN 3230313185885B41 automatically reported by the system, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/2)#ont confirm 0 sn-auth 3230313185885B41 omci
```

7.4 Configuring a GPON Port

To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.

Default Configuration

Table 7-6 lists the default settings of the GPON port.

Table 7-6 Default settings of the GPON port

Parameter	Default Setting
GPON port	Enabled
Downstream FEC function of the GPON port	Disabled
Compensation distance range of the GPON port ranging	Minimum logical distance: 0 km; maximum logical distance: 20 km

Procedure

Step 1 Run the **interface gpon** command to enter the GPON mode.

Step 2 Configure the laser of the GPON port.

- Run the **undo shutdown** command to enable the laser of the GPON port. By default, the laser of the GPON port is enabled and the GPON port is available. In this case, skip this step.
- If the GPON port is not to be used, run the **shutdown** command to disable the laser of the GPON port.

⚠ **CAUTION**

Disabling a PON port that carries services will cause the interruption of such services.

Step 3 Configure the downstream FEC function of the GPON port.

Run the **port** ***portid*** **fec** command to configure the FEC function of the GPON port. By default, the FEC function is disabled.

NOTE

- FEC is to insert redundant data into normal packets so that the line has certain error tolerance. Some bandwidth, however, must be consumed. Enabling FEC enhances the error correction capability of the line but at the same time occupies certain bandwidth. Determine whether to enable FEC according to the actual line planning.
- If a large number of ONTs are already online, enabling FEC on the GPON port may cause certain ONTs to go offline. Therefore, it is suggested that FEC should not be enabled on a GPON port that connects to online ONTs.

Step 4 Configure the renewal time of the ONT key.

Run the **port** ***portid*** **ont-password-renew** command to configure the interval for renewing the ONT key. To ensure the system security, the ONT key renewal must be configured.

Step 5 Configure the compensation distance in the ranging.

Run the **port** ***portid*** **range** command to configure the compensation distance range of the GPON port ranging. By default, the minimum logical distance is 0 km, and the maximum logical distance is 20 km. The difference between the minimum logical distance and the maximum logical distance must not exceed 20 km.

Step 6 (Optional) Configure the DBA calculation period on a GPON port basis.

When different GPON ports provide different access services, the bandwidth delays on these ports are different. In this case, the DBA calculation period needs to be configured on a GPON port basis.

1. In GPON board mode, run the **port dba bandwidth-assignment-mode** command to configure the DBA mode on a GPON port.
2. In diagnose mode, run the **gpon port dba calculate-period** command to configure the DBA calculation period on the GPON port.

NOTE

- The DBA calculation period on a GPON port can be configured only when the DBA mode is set to **manual** on this GPON port.
- By default, the DBA mode on a GPON port is **default**, which means the global DBA mode is used as the bandwidth assignment mode for the GPON port. In this case, if the global DBA mode is modified by running the **gpon dba bandwidth-assignment-mode** command, the bandwidth assignment mode on the GPON port is also modified. If the DBA mode on a GPON port is not **default**, the bandwidth assignment mode on the GPON port is not affected by the global DBA mode.
- If ONTs are configured on a GPON port, modifying the DBA mode is not allowed on this GPON port.
- For the TDM service, the DBA mode must be set to **min-loop-delay**.

----End

Example

Assume that the key renew interval of the ONT under the port is 10 hours, the minimum compensation distance of ranging is 10 km, and the maximum compensation distance of ranging is 15 km. To enable the FEC function of GPON port 0/2/0, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 fec enable
huawei(config-if-gpon-0/2)#port 0 ont-password-renew 10
huawei(config-if-gpon-0/2)#port 0 range min-distance 10 max-distance 15
  This command will result in the ONT's re-register in the port.
  Are you sure to execute this command? (y/n)[n]: y
```

To set the global DBA mode to **min-loop-delay**, DBA mode on GPON port 0/2/0 to **manual**, and DBA calculation period to **4**, do as follows:

```
huawei(config)#gpon dba bandwidth-assignment-mode min-loop-delay
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port dba bandwidth-assignment-mode 0 manual
huawei(config-if-gpon-0/2)#quit
huawei(config)#diagnose
huawei(diagnose)%%gpon port dba calculate-period 0/2/0 4
```

7.5 Creating a GPON Service Port

A service port is a service channel connecting the user side to the network side. To provision services, a service port must be created.

Context

A service port can carry a single service or multiple services. When a service port carries multiple services, the MA5600T/MA5603T supports traffic classification. In the simplified configuration mode, the MA5600T/MA5603T supports only CVLAN-based traffic classification.

Table 7-7 lists the default settings of a service port.

Table 7-7 Default settings of a service port

Parameter	Default Setting
Traffic profile ID	0-6
Administrative status	Activated
Maximum number of learnable MAC addresses	1023

Procedure

Step 1 Create a traffic profile.

Run the **traffic table ip** command to create a traffic profile. There are seven default traffic profiles in the system with IDs 0-6.

Before creating a service port, run the **display traffic table** command to check whether the existing traffic profiles in the system meet the application requirement. If no traffic profile in the system meets the application requirement, create a traffic profile accordingly. For details about traffic profiles, see **Configuring Traffic Management Based on Service Port**.

Step 2 Create a service port.

Run the **service-port vlan *vlanid* port** command to create a service port. In the simplified configuration mode, a service port can be considered as a whole from the MA5600T/MA5603T to a specific port on the ONT, that is, as an end-to-end configuration. The user needs to care about only the translation between the SVLAN and the CVLAN and need not care about the GEM port mapping.

1. Specify an ONT port by selecting a port type from **ont** *ontid* { **eth** | **iphost** }.
   - **eth**: Specifies an Ethernet port, which is generally used for the Internet access service or multicast service.
   - **iphost**: Specifies a POTS port, which is generally used for the voice service.
2. Specify the CVLAN tag by selecting **multi-service user-vlan** { **untagged** | *user-vlanid* }.
   - **untagged**: Indicates that the user-side packets are untagged.
   - *user-vlanid*: Indicates that the user-side packets are tagged. The tag value must be the same as the tag carried in the user-side packets, that is, the CVLAN tag.

The parameter configurations are related to the ONT type. Therefore, the ONT type must be specified before a service port is created.

- For a bridge ONT (SFU), the ONT port providing the POTS service is set to **iphost** and ONT ports providing other services are set to **eth**.
- For a gateway ONT (HGU), the ONT port providing the Internet access service with untagged packets is set to **iphost**; other services cannot be configured on the specific physical ports but on the ONT.

Table 7-8 lists the specific commands.

Table 7-8 Parameter configuration

Service Type	Bridge ONT	Gateway ONT
Tagged HSI service	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **eth** *port-index-list* **multi-service**...	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **multi-service**...
Untagged HSI service	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **eth** *port-index-list* **multi-service**...	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **iphost multi-service**... NOTE Services can be distinguished only when native VLAN is configured on the ONT port.
Voice service	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **iphost multi-service**...	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **multi-service**...
IPTV service	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **eth** *port-index-list* **multi-service**...	**service-port** [*index*] **vlan** *vlanid* **port** *frameid/slotid/portid* **ont** *ontid* **multi-service**...

"..." in the preceding table indicates the omitted command format.

NOTE

- The system supports creation of service ports by index. One index maps one service port. In this way, you need not input a large number of traffic parameters and hence the configuration of service ports is simplified. During the creation of a service port, *index* indicates the index of the service port and it is optional. If you do not specify a value, the system allocates an idle index starting from the currently configured maximum index (regardless of whether the index is deleted). After the maximum value range is exceeded, the system searches for new idle indexes starting from 0.
- **vlan** indicates the SVLAN. An SVLAN can only be a MUX VLAN or smart VLAN.
- **rx-cttr** is the same as **outbound** in terms of meaning and function. Either parameter indicates the index of the traffic from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meaning and function. Either parameter indicates the index of the traffic from the user side to the network side. The traffic profile bound to the service port is created in **Step 1**.

Step 3 (Optional) Modify the ETH port list of service ports.

Run the **service-port *index* modify** command to modify the ETH port list of the E2E service ports.

You must plan services of each port in advance for E2E service ports. If the planned services change, you need to run the **service-port *index* modify** command to modify **Port-list** but cannot run the **service-port** command in **Step 2** to reconfigure service ports.

Step 4 Configure the attributes of the service port. Configure the attributes of the service port according to the application requirement.

- Run the **service-port desc** command to configure the description of the service port. Configuring description for a service port facilitates maintenance. In general, configure the purpose and related service information as the description of a service port.
- Run the **service-port *index* adminstatus** command to set the administrative status of the service port. By default, a service port is in the activated state.

  Services can be provisioned at two levels: port level and service port level. To provision services for a user, the access port and the corresponding service port of the user must be activated.
- Run the **mac-address max-mac-count service-port** command to set the maximum number of MAC addresses learned by the service port. This configuration restricts the maximum number of PCs that can access the Internet by using the same user account. By default, the maximum number of learnable MAC addresses of a service port is 1023.

----End

Example

Assume that GPON port 0/2/0 of the MA5600T/MA5603T is connected to an ONT with the ID of 1. The data plan of an Internet access user is as follows: The ONT provides the 4096 kbit/s Internet access service (through the single-service service port). The user is connected to ETH port 1 of the ONT, the SVLAN ID is 1000, and a maximum of three users can use the same user account for concurrently accessing the Internet.

The query result shows that the system does not have a suitable traffic profile. Hence, create traffic profile hsi. This user account is not opened yet and no service is provisioned for the user account temporarily.

To perform these configurations, do as follows:

```
huawei(config)#traffic table ip name hsi cir 4096 priority 3 priority-policy loc
al-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index            : 10
  TD Name             : hsi
  Priority            : 3
  Copy Priority       : -
  Mapping Index       : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy     : local-pri
  CIR                 : 4096 kbps
  CBS                 : 133072 bytes
  PIR                 : 8192 kbps
  PBS                 : 264144 bytes
  Color policy        : dei
  Referenced Status   : not used
  ------------------------------------------------
huawei(config)#service-port 5 vlan 1000 port 0/2/0 ont 1 eth 1 multi-service
 user-vlan untagged inbound traffic-table name hsi outbound traffic-table name hsi
huawei(config)#mac-address max-mac-count service-port 5 3
huawei(config)#service-port 5 adminstatus disable
```

Assume that GPON port 0/2/0 of the MA5600T/MA5603T is connected to an ONT with the ID of 2. The data plan of a commercial user is as follows: The user requests the 8192 kbit/s Internet access service. To facilitate future service extension, the ONT provisions the service to the user through the multi-service service port and differentiates users by CVLAN. The SVLAN ID is 1023 and the CVLAN ID is 100. Port 2 on the ONT carries traffic streams.

The query result shows that the system does not have a suitable traffic profile. Hence, create traffic profile huawei. The system needs to provision the Internet access service to the user immediately. To facilitate maintenance, the description of the service port needs to be configured.

To perform these configurations, do as follows:

```
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      1024      34768      2048      69536   6 -              tag-pri
     1      2496      81872      4992     163744   6 -              tag-pri
     2       512      18384      1024      36768   0 -              tag-pri
     3       576      20432      1152      40864   2 -              tag-pri
     4        64       4048       128       8096   4 -              tag-pri
     5      2048      67536      4096     135072   0 -              tag-pri
     6       off        off       off        off   0 -              tag-pri
  ----------------------------------------------------------------------------
  Total Num : 7
huawei(config)#traffic table ip name huawei cir 8192 priority 4 priority-policy
 local-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index            : 8
  TD Name             : huawei
  Priority            : 4
  Copy Priority       : -
  Mapping Index       : -
  CTAG Mapping Priority: -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                  : 8192 kbps
  CBS                  : 264144 bytes
  PIR                  : 16384 kbps
  PBS                  : 526288 bytes
  Color policy         : dei
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 10 vlan 1023 port 0/2/0 ont 2 eth 2 multi-service
 user-vlan 100 inbound traffic-table name huawei outbound traffic-table name
huawei
huawei(config)#service-port desc 10 description gpon/Vlanid:1023/uservlan:100
```

Assume that only ONT port 1 is originally used to provide the Internet access service for a home user and now ONT ports 2 and 3 are also required to provide the Internet access service; the service port ID is 10. To achieve the Internet access services on ONT port 1-3, do as follows:

```
huawei(config)#service-port 10 modify ont eth 1-3
```

8 Configuring the Multicast Service

About This Chapter

The MA5600T/MA5603T supports multicast cascading for reducing the number of ports used on the convergence device, and also supports MSTP network protection. With these two functions, the network structure is optimized and the multicast service reliability is improved.

Context

For details about multicast features, see Multicast.

To ensure service quality, physical layer retransmission is recommended. This retransmission technology is put forward to more reliably transmit services over lines. Compared with traditional data and voice services, video services such as IPTV and video on demand (VoD) impose far higher requirements on bit error ratio and packet loss ratio but lower requirements on delay.

- Run the **adsl extline-profile add** or **adsl extline-profile modify** command to configure physical layer retransmission for asymmetric digital subscriber line (ADSL) lines.
- Run the **vdsl channel-profile add**, **vdsl channel-profile modify**, **vdsl channel-profile quickadd**, or **vdsl channel-profile quickmodify** command to configure physical layer retransmission for very high speed digital subscriber line (VDSL) lines

This topic provides the default settings of the multicast service in the system, including the configuration of multicast protocol, IGMP version, program configuration mode, bandwidth management, program preview, and log function.

When the network structure is simple, the configuration of a single NE can meet multicast service requirements. Compared with cascading networking, single-NE networking is more secure and stable, and provides more bandwidth resources, but requires more line resources. The method of configuring multicast services for an NE in the cascading or MSTP networking scenario is the same as that in single-NE networking scenario.

This topic describes how to configure the multicast service for an xDSL user of the MA5600T/MA5603T in a subtending network.

8.4 Configuring the Multicast Service in an MSTP Network

This topic describes how to configure the multicast service for an xDSL user of the MA5600T/MA5603T in an MSTP network.

8.1 Default Settings of the Multicast Service

This topic provides the default settings of the multicast service in the system, including the configuration of multicast protocol, IGMP version, program configuration mode, bandwidth management, program preview, and log function.

Table 8-1 lists the default settings of the multicast service of the MA5600T/MA5603T.

Table 8-1 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	Disabled
IGMP version	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	Enabled
Multicast preview	Enabled
Multicast log function	Enabled

8.2 Configuring the Multicast Service on a Single NE

When the network structure is simple, the configuration of a single NE can meet multicast service requirements. Compared with cascading networking, single-NE networking is more secure and stable, and provides more bandwidth resources, but requires more line resources. The method of configuring multicast services for an NE in the cascading or MSTP networking scenario is the same as that in single-NE networking scenario.

Application Context

The multicast feature of the MA5600T/MA5603T is mainly applied to the live TV and near-video on demand (NVOD) multicast video services. The MA5600T/MA5603T runs the IGMP proxy or IGMP snooping protocol, and the interconnected device can run the IGMP proxy, IGMP snooping, or multicast router protocol.

Currently, the multicast application of the MA5600T/MA5603T is oriented to Layer 2, and the MA5600T/MA5603T forwards data based on VLAN ID+multicast MAC address. A multicast program in the network is identified by VLAN ID + multicast IP address uniquely. The MA5600T/MA5603T differentiates multicast sources by VLAN ID. It allocates a unique VLAN ID to each multicast source, controls the multicast domain and the user right based on the multicast VLAN ID, and provides a platform for different ISPs to implement different multicast video services.

Data Plan

Before configuring the multicast video service, plan the data items as listed in **Table 8-2**.

Table 8-2 Data plan for configuring the multicast service on a single MA5600T/MA5603T

Device	Data Item
MA5600T/MA5603T	Multicast VLAN
	Layer 2 multicast protocol
	IGMP version of the multicast VLAN
	IGMP version of the multicast user
	Multicast program configuration mode
	Multicast general query and group-specific query parameters **NOTE** The default values are adopted.
	Program list
	User authentication policy
	Program bandwidth, upstream port bandwidth, and user bandwidth
	Multicast ONT
	Multicast logging policy
Upper-layer multicast router	IGMP version **NOTE** The IGMP version of the upper-layer multicast router must not be earlier than the IGMP version of the multicast VLAN used by the MA5600T/MA5603T.
Home gateway or modem	IGMP version **NOTE** The IGMP version of the CPE must not be earlier than the IGMP version of the multicast user on the MA5600T/MA5603T.

Table 8-3 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	Disabled
IGMP version	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	Enabled
Multicast preview	Enabled
Multicast log function	Enabled

Configuration Flowchart

8.2.1 Configuring Multicast Global Parameters

The general parameters of Layer 2 multicast protocols (including IGMP proxy and IGMP snooping) configured for a device are applicable to all the multicast VLANs on the device.

Context

The multicast global parameters include general query, group-specific query, the policy of processing multicast packets and the multicast forwarding mode.

The description of a general query is as follows:

- Purpose: A general query packet is periodically sent by the MA5600T/MA5603T to check whether there is any multicast user who leaves the multicast group without sending the leave packet. Based on the query result, the MA5600T/MA5603T periodically updates the multicast forwarding table and releases the bandwidth of the multicast user that has left the multicast group.
- Principle: The MA5600T/MA5603T periodically sends the general query packet to all online IGMP users. If the MA5600T/MA5603T does not receive the response packet from a multicast user within a specified time (Robustness variable x General query interval + Maximum response time of a general query), it regards the user as having left the multicast group and deletes the user from the multicast group.

The description of a group-specific query is as follows:

- Purpose: A group-specific query packet is sent by the MA5600T/MA5603T after a multicast user that is not configured with the quick leave attribute sends the leave packet. The group-specific query packet is used to check whether the multicast user has left the multicast group.
- Principle: When a multicast user leaves a multicast group, for example, switches to another channel, the user unsolicitedly sends a leave packet to the MA5600T/MA5603T. If the multicast user is not configured with the quick leave attribute, the MA5600T/MA5603T sends a group-specific query packet to the multicast group. If the MA5600T/MA5603T does not receive the response packet from the multicast user within a specified duration (Robustness variable x Group-specific query interval + Maximum response time of a group-specific query), it deletes the multicast user from the multicast group.

Table 8-4 lists the default settings of the multicast global parameters. In the actual application, you can modify the values according to the data plan.

Table 8-4 Default settings of the multicast global parameters

Parameter	Default Value
General query parameter	Query interval: 125s Maximum response time: 10s Robustness variable (query times): 2
Group-specific query parameter	Query interval: 1s Maximum response time: 0.8s. Robustness variable (query times): 2

Parameter	Default Value
Policy of processing multicast packets	IGMP packet: normal (IGMP packets are processed as controllable multicast) Unknown multicast packet: discard
Policy of processing multicast packets	IGMP packet: normal (IGMP packets are processed as controllable multicast) Unknown multicast packet: discard
Policy of processing multicast packets	IGMP packet: normal (IGMP packets are processed as controllable multicast) Unknown multicast packet: ● For switch-oriented traffic streams: discard ● For connection-oriented traffic streams: transparent transmission
Multicast forwarding mode	disable(VLAN+GMAC mode)

Procedure

Step 1 Configure the general query parameters.

1. Run the **igmp proxy router gen-query-interval** command to set the general query interval. By default, the general query interval is 125s.
2. Run the **igmp proxy router gen-response-time** command to set the maximum response time of the general query. By default, the maximum response time of the general query is 10s.
3. Run the **igmp proxy router robustness** command to set the robustness variable (query times) of the general query. By default, the robustness variable (query times) is 2.

Step 2 Set the group-specific query parameters.

1. Run the **igmp proxy router sp-response-time** command to set the group-specific query interval. By default, the group-specific query interval is 1s.
2. Run the **igmp proxy router sp-query-interval** command to set the maximum response time of the group-specific query. By default, the maximum response time of the group-specific query is 0.8s.
3. Run the **igmp proxy router sp-query-number** command to set the robustness variable (query times) of the group-specific query. By default, the robustness variable (query times) is 2.

Step 3 Configure the policy of processing multicast packets.

By default, the normal mode for processing IGMP packets is adopted. In this mode, IGMP packets are processed as controllable multicast. The discard mode is adopted for unknown multicast packets. In this mode, unknown multicast packets are discarded.

The default values are adopted for multicast service and do not need to be modified. To control the forwarding of multicast packets when configuring other services, run the following commands to configure the policy.

1. Run the **igmp policy** command to set the policy of processing IGMP packets.
2. Run the **multicast-unknown policy** command to set the policy of processing unknown multicast packets(downstream UDP packets).

Step 4 (Optional) Configure the multicast forwarding mode.

The multicast forwarding mode including these following two types. Run the **igmp sip-gip-forward** { **disable** | **enable** } command to set the multicast forwarding mode.

- disable: Sets the forwarding mode to VLAN+GMAC. That is, packets are forwarded based on the MAC address mapped from the IP address of the multicast program and the multicast VLAN ID.
- enable: Sets the forwarding mode to SIP+GIP. That is, IGMP packets are forwarded in the mode of multicast source multicst VLAN ID+IP address+multicast program IP address. When multiple multicast sources have the programs with the same IP address, to differentiate programs and their corresponding multicast sources, you need to set the forwarding mode of IGMP packets to SIP+GIP.

Step 5 Run the **display igmp config global** command to check whether the values of the multicast parameters are correct.

----End

Example

(IPv4) To configure the multicast general query parameters by setting the query interval to 150s, maximum response time to 20s, and number of queries to 3 on the multicast VLAN 100, do as follows:

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp proxy router gen-query-interval 150
huawei(config-mvlan100)#igmp proxy router gen-response-time v3 20
huawei(config-mvlan100)#igmp proxy router robustness 3
```

(IPv4) To configure the multicast group-specific query parameters by setting the query interval to 200s, maximum response time to 100s, and number of queries to 3 on the multicast VLAN 100, do as follows:

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp proxy router sp-query-interval 200
huawei(config-mvlan100)#igmp proxy router sp-response-time v3 100
huawei(config-mvlan100)#igmp proxy router sp-query-number 3
```

(IPv6) To configure the multicast general query parameters by setting the query interval to 150s, maximum response time to 20s, and number of queries to 3 on the multicast VLAN 200, do as follows:

```
huawei(config)#multicast-vlan 200
huawei(config-mvlan200)#igmp ipv6 router gen-query-interval 150
huawei(config-mvlan200)#igmp ipv6 router gen-response-time v2 20
huawei(config-mvlan200)#igmp ipv6 router robustness 3
```

(IPv6) To configure the multicast group-specific query parameters by setting the query interval to 200s, maximum response time to 100s, and number of queries to 3 on the multicast VLAN 200, do as follows:

```
huawei(config)#multicast-vlan 200
huawei(config-mvlan200)#igmp ipv6 router sp-query-interval 200
huawei(config-mvlan200)#igmp ipv6 router sp-response-time v2 100
huawei(config-mvlan200)#igmp ipv6 router sp-query-number 3
```

8.2.2 Configuring the Multicast VLAN and the Multicast Program

In the application of multicast service, multicast VLANs (MVLANs) are used to distinguish multicast ISPs. Generally, an MVLAN is allocated to each multicast ISP for the VLAN-based management of multicast programs, multicast protocols, IGMP versions, and the VLAN-based control of multicast domain and user right.

Context

To create a multicast VLAN, a common VLAN must be created first. The multicast VLAN can be the same as the unicast VLAN. In this case, the two VLANs can share the same service stream channel. The multicast VLAN can be different from the unicast VLAN. In this case, the two VLANs use different service stream channels.

One user port can be added to multiple multicast VLANs under the following restrictions:

- Among all the multicast VLANs of a user port, only one multicast VLAN is allowed to have dynamically generated programs.
- One user port is not allowed to belong to multiple MVLANs that are in the IGMP v3 snooping mode.

The source IP address in the multicast packets that are sent to the upper device by the OLT may be as follows:

- If the IP address of the program VLAN interface is configured, the source IP address is the IP address of VLAN interface.
- If the IP address of the program VLAN interface is not configured, the source IP address is the host IP address of the program.
- If the host IP address is not configured, the default address 0.0.0.0 is used.

Table 8-5 lists the default settings of the MVLAN attributes, including the Layer 2 multicast protocol, IGMP version, multicast program, and multicast upstream port.

Table 8-5 Default settings of the MVLAN attributes

Parameter	Default Value
Program matching mode	enable (static configuration mode)
Multicast upstream port mode	default
Layer 2 multicast protocol	off (multicast function disabled)
IGMP version	v3
Priority of forwarding IGMP packets by the upstream port	6
Group filter mode	asm-ssm

Procedure

Step 1 Create a multicast VLAN.

1. Run the **vlan** command to create a VLAN, and set the VLAN type according to the actual application. For details on the VLAN configuration, see **Configuring VLAN**.
2. Run the **multicast-vlan** command to set the created VLAN to a multicast VLAN. The VLAN with S+C forwarding mode cannot be set as a multicast VLAN.

Step 2 Configure multicast programs.

The multicast VLAN can be configured statically or generated dynamically. The program configuration of the MVLAN has three modes: static configuration, dynamic generation, and static and dynamic mixed configuration.

- Static configuration mode: Configure the program list before users watch the video programs. In this mode, the right profile can be used to implement controllable multicast. The program list and the right profile, however, need to be maintained according to the change of the video service. The program host, program prejoin, and multicast bandwidth management functions are supported.

1. Run the **igmp match mode enable** command to set the static configuration mode. By default, the system adopts the static configuration mode.
2. Run the **igmp program add** [**name** *name*] **ip** *ip-addr* [**sourceip** *ip-addr*] [**hostip** *ip-addr*] command to add a multicast program.

   NOTE

   If the IGMP version of a multicast VLAN is v3, the program must be configured with a source IP address. If the IGMP version of a multicast VLAN is v2, the program must not be configured with a source IP address.
3. Add a right profile.

   In the BTV mode, run the **igmp profile add** command to add a right profile.
4. Bind the program to the right profile.

   In the BTV mode, run the **igmp profile** command to bind the program to the right profile, and set the right to watch.

   NOTE

   When a user is bound to multiple right profiles, and the right profiles have different rights to a program, the right with the highest priority prevails. You can run the **igmp right-priority** command to adjust the priorities of the four rights: watch, preview, forbidden, and idle. By default, the priorities of the four rights are forbidden > preview > watch > idle.

- Dynamic generation mode: A program list is dynamically generated 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.

1. Run the **igmp match mode disable** command to set the dynamic generation mode.

   CAUTION

   The **igmp match mode** command can be executed only when the IGMP mode is disabled.
2. Run the **igmp match group** command to configure the IP address range of the program group that can be dynamically generated. Users can order only the programs whose IP addresses are within the specified range.

- Static and dynamic mixed configuration: Configure the program list before users watch the video programs. In this mode, the right profile can be used to implement controllable multicast. The program list and the right profile, however, need to be maintained according to the change of the video service. The program host, program prejoin, and multicast bandwidth management functions are supported.

1. Run the **igmp match mode disable** command to set the mode to the dynamic generation mode.
2. Run the **igmp match group** command to configure the IP address range of the program group that can be dynamically generated. Users can order only the programs whose IP addresses are within the specified range.
3. Run the **igmp program add** [**name** *name*] **ip** *ip-addr* [**sourceip** *ip-addr*] [**hostip** *ip-addr*] command to add a multicast static program.

   NOTE

   When the range of static program IP addresses and the range of dynamic program IP addresses overlap each other, static programs can go online with priority.

4. Run the **igmp group-filter-mode** command to set the group filter mode based on multicast VLAN (MVLAN).

   NOTE

   - When the group filter mode of an MVLAN is configured to **asm-only** or **asm-ssm**, only one program with the unique multicast IP address is generated in the MVLAN. The [*, G] multicast forwarding table is used for this MVLAN instance on the forwarding plane.
   - When the group filter mode of an MLVAN is configured to **ssm-only**, multiple programs with the same multicast IP addresses but different source IP addresses can be generated in the MVLAN. The [s, g] multicast forwarding table is used for this VLAN instance on the forwarding plane.

     NOTE

     The source IP addresses are regarded as different ones when they have different least significant 20 bits from each other.
   - The maximum number of programs is calculated according to the number of actually-generated programs. For example:
     - When a multicast user joins an MVLAN with the multicast filter mode **asm-ssm** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates only one multicast program with the multicast IP address G1 for the multicast user;
     - When a multicast user joins an MVLAN with the multicast filter mode **ssm-only** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates two multicast programs with IP addresses [S1, G1] and [S2, G1].

Step 3 Configure the multicast upstream port.

1. Run the **igmp uplink-port** command to configure the multicast upstream port. The packets of the MVLAN corresponding to the upstream port are forwarded and received by this upstream port.
2. In the BTV mode, run the **igmp uplink-port-mode** command to change the mode of the multicast upstream port. By default, the port is in the default mode. In the MSTP network, the port adopts the MSTP mode.
   - Default mode: If the MVLAN contains only one upstream port, the multicast packets that go upstream can be sent only by this port. If the MVLAN contains multiple upstream ports, the multicast packets that go upstream are sent by all the upstream ports.
   - MSTP mode: This mode is adopted in the MSTP network.

Step 4 Select the multicast mode.

Run the **igmp mode** { **proxy** | **snooping** } command to select the Layer 2 multicast mode. By default, the multicast mode is disabled.

In terms of multicast processing mode, the MA5600T/MA5603T supports the Internet Group Management Protocol (IGMP) Proxy and IGMP Snooping Layer 2 multicast protocols. IGMP proxy and IGMP snooping both support multicast video data forwarding; however, the two modes have different processing mechanisms.

- In IGMP snooping, the related information for maintaining multicast forwarding entries is obtained by listening to the IGMP packets between the user and the multicast router.
- IGMP proxy intercepts the IGMP packets between the user and the multicast router, processes the IGMP packets, and then forwards the IGMP packets to the upper-layer multicast router. For the multicast user, the MA5600T/MA5603T is a multicast router that implements the router functions in the IGMP protocol; for the multicast router, the MA5600T/MA5603T is a multicast user.

In the IGMP snooping mode, proxy can be enabled for the report packet and the leave packet. When a multicast user joins or leaves a multicast program, the MA5600T/MA5603T can implement IGMP proxy. IGMP snooping and IGMP proxy are controlled separately.

- Run the **igmp report-proxy enable** command to enable the proxy of the snooping report packet. When the first user requests to join a program, after authenticating the user, the MA5600T/MA5603T sends the user report packet to the network side and receives a corresponding multicast stream from the multicast router. The report packets of the users that follow the first user are not sent by the MA5600T/MA5603T to the network side.
- Run the **igmp leave-proxy enable** command to enable the proxy of the snooping leave packet. When the last user requests to leave the program, the MA5600T/MA5603T sends the user leave packet to the network side to request the upper-layer device to stop sending multicast streams. The leave packets of the users that precede the last user are not sent by the MA5600T/MA5603T to the network side.

Step 5 Set the IGMP version.

Run the **igmp version**{ **v2** | **v3** } command to set the IGMP version. By default, IGMP v3 is enabled in the system. If the upper-layer and lower-layer devices in the network are IGMP v2 devices and cannot recognize the IGMP v3 packets, run this command to change the IGMP version.

IGMP v3 is compatible with IGMP v2 in packet processing. If IGMP v3 is enabled on the MA5600T/MA5603T and the upper-layer multicast router switches to IGMP v2, the MA5600T/MA5603T automatically switches to IGMP v2 when receiving the IGMP v2 packets. If the MA5600T/MA5603T does not receive any more IGMP v2 packets within the preset IGMP v2 timeout time, it automatically switches back to IGMP v3. In the BTV mode, run the **igmp proxy router timeout** command to set the IGMP v2 timeout time. By default, the timeout time is 400s.

Step 6 Change the priority for forwarding IGMP packets.

Run the **igmp priority** command to change the priority for forwarding the IGMP packets by the upstream port. By default, the priority is 6 and does not need to be changed.

- In the IGMP proxy mode, the IGMP packets sent from the upstream port to the network side adopt the priority set through the preceding command in the MVLAN.
- In the IGMP snooping mode, the IGMP packets forwarded to the network side adopt the priority of the user service stream. The priority of the service stream is set through the traffic profile.

Step 7 Check whether the configuration is correct.

- Run the **display igmp config vlan** command to query the attributes of the multicast VLAN.

- Run the **display igmp program vlan** command to query the information about the program of the MVLAN.

----End

Example

Assume that:

- MVLAN ID: 101
- Program configuration mode: static configuration; program IP address: 224.1.1.1
- Source IP address: 10.10.10.10; host IP address: 10.0.0.254
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/19/0
- Protocol: IGMP proxy; IGMP version: v3
- Group filter mode: ssm-only

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode enable
huawei(config-mvlan101)#igmp program add name movie ip 224.1.1.1 sourceip
10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#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
huawei(config-mvlan101)#igmp version v3
huawei(config-mvlan101)#igmp group-filter-mode ssm-only
```

Assume that:

- MVLAN ID: 101
- Program configuration mode: dynamic generation
- Address range of the dynamic program group: 224.1.1.10 to 224.1.1.50
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/19/0
- Protocol: IGMP proxy; IGMP version: v3

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#iigmp match mode disable
  This operation will delete all the programs in current multicast vlan
  Are you sure to change current match mode? (y/n)[n]: y
  Command is being executed, please wait...
  Command has been executed successfully
huawei(config-mvlan101)#igmp match group ip 224.1.1.10 to-ip 224.1.1.50
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#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
huawei(config-mvlan101)#igmp version v3
```

Assume that:

- MVLAN ID: 101
- Program configuration mode: static and dynamic mixed configuration
- MVLAN upstream port: 0/19/0
- IP address of the static program: 224.1.1.1; source IP address: 10.10.10.10; host IP address: 10.0.0.254; program bandwidth: 5000 kbit/s
- Address range of the dynamic program group: 224.1.1.10 to 224.1.1.50
- Protocol: IGMP proxy; IGMP version: v3

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode disable
  This operation will delete all the programs in current multicast vlan
  Are you sure to change current match mode? (y/n)[n]: y
  Command is being executed, please wait...
  Command has been executed successfully
huawei(config-mvlan101)#igmp match group ip 224.1.1.10 to-ip 224.1.1.50
huawei(config-mvlan101)#igmp program add name movie ip 224.1.1.1 sourceip
10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#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
huawei(config-mvlan101)#igmp version v3
```

Assume that:

- MVLAN ID: 101
- Program configuration mode: static configuration; program IP address:ffff::1
- Source IPv6 address: 2000::1
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/19/0
- Protocol: IGMP proxy; IGMP version: v2

To configure the MVLAN and multicast program for the IPv6 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode enable
huawei(config-mvlan101)#igmp program add name movie ipv6 ffff::1 source-ipv6
2000::1
 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#igmp ipv6 mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
huawei(config-mvlan101)#igmp ipv6 version v2
```

8.2.3 Configuring a Multicast User

This topic describes how to configure a multicast user and the related user right for provisioning the multicast service.

Prerequisites

Before configuring a multicast user, create a service channel. The procedure is as follows:

1. **Add a VLAN.**
2. **Configure the upstream port.**
3. **Configure the xDSL port.**
4. **Create an xDSL service port.**

NOTE

The multicast service supports the IPoE and PPPoE user access modes, but does not support the IPoEoA or PPPoEoA user access mode.

- Configure a GPON multicast user
  1. **Configure the VLAN**
  2. **Configure the upstream port**
  3. **Configure the multicast GPON ONT**
  4. **Configure the GPON user port**
  5. **Configure the GPON traffic stream**

Context

Add a multicast user, and bind the multicast user to the multicast VLAN to create a multicast member. Bind the multicast user to a right profile to implement multicast user authentication.

Table 8-6 lists the default settings of the attributes related to the multicast user.

Table 8-6 Default settings of the attributes related to the multicast user

Parameter	Default Value
Maximum number of programs that can be watched by the multicast user	8
Maximum number of programs of different priorities that can be watched by the multicast user	no-limit
Quick leave mode of the multicast user	MAC-based
Global switch of multicast user authentication	enable
IGMP version of the multicast user	v3

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Configure a multicast user and the multicast user attributes.

1. Add a multicast user.

   Run the **igmp user add service-port** command to add a multicast user.

2. Configure the maximum number of programs that can be watched by the multicast user.

   - Run the **igmp user add service-port** *index* **max-program** { **max-program-num** | **no-limit** } command to configure the maximum number of programs that can be watched by the multicast user concurrently. Up to 32 programs can be watched by the multicast user concurrently. By default, it is 8.
   - Run the **igmp user watch-limit service-port** { **hdtv** | **sdtv** | **streaming-video** } command to configure the maximum number of programs of different priorities that can be watched by the multicast user.

3. Set the quick leave mode of the multicast user.

   Run the **igmp user add service-port** *index* **quickleave** { **immediate** | **disable** | **mac-based** } command to configure the quick leave mode of the multicast user. By default, the quick leave mode is the MAC-based mode.

   - **Immediate**: After receiving the leave packet of the multicast user, the system immediately deletes the multicast user from the multicast group.
   - **Disable**: After receiving the leave packet of the multicast user, the system sends an ACK packet to confirm that the multicast user leaves, and then deletes the multicast user from the multicast group.
   - **MAC-based**: It is the quick leave mode based on the MAC address. The system checks the MAC address in the leave packet of the user. If it is the same as the MAC address in the report packet of the user and it is the last MAC addres of multicast user, the system immediately deletes the multicast user from the multicast group. Otherwise, the system does not delete the multicast user. This mode is applied to the scenario with multiple terminals.

4. Set the IGMP version for the multicast user.

   Run **igmp user add service-port** *index* **igmp-version** { **v2** | **v3** | **v3-forced** } command to set the IGMP version for the multicast user. Each multicast users has an independent querier instance. This command specifies the IGMP version (default: v3) for the multicast user querier.

   - v2: specifies the IGMP version to v2 for the multicast user querier. When this setting applies, the system processes only IGMP v2 packets and directly drops IGMP v1 packets and IGMP v3 packets.
   - v3: specifies the v3–compatible mode (default setting for the system). When this setting applies, the system automatically specifies the IGMP version according to the version of the IGMP packets sent by users, but it directly drops IGMP v1 packets.
   - v3-forced: forcibly specifies the IGMP version to V3 for the multicast user querier. When this setting applies, the system processes only IGMP v3 packets but directly drops IGMP v1 packets and IGMP v2 packets.

Step 3 Configure multicast user authentication.

To control the right of a multicast user, you can enable the multicast user authentication function.

1. Configure the multicast user authentication function.

   Run the **igmp user add service-port** *index* { **auth** | **no-auth** } command to configure whether to authenticate a multicast user.

NOTE

After configuring multicast user authentication, you need to enable the global authentication function to make the configuration take effect. By default, the global authentication function is enabled. You can run the **igmp proxy authorization** command to change the configuration.

2. Bind the multicast user to the right profile. This operation is to implement user authentication.

   Run the **igmp user bind-profile** command to bind the user to a right profile. After the binding, the multicast user has the rights to the programs as configured in the profile.

Step 4 Bind the multicast user to a multicast VLAN.

In the multicast VLAN mode, run the **igmp multicast-vlan member** command to bind the user to the multicast VLAN. Then, the multicast user becomes a multicast member of the multicast VLAN and can request the programs configured in the multicast VLAN.

Step 5 Run the **display igmp user** command to check whether the related multicast user information is correctly configured.

----End

Example

To add multicast user (port) 0/2/1 to multicast VLAN 101, enable user authentication, enable log report, set the maximum bandwidth to 10 Mbit/s, set IGMP version of the multicast user to v3-forced, and bind the user to right profile **music**, do as follows:

```
huawei(config)#service-port 100 vlan 101 adsl 0/2/1 vpi 0 vci 35 rx-cttr 2 tx-cttr
2
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 100 auth log enable max-bandwidth
10240 igmp-version v3-forced
huawei(config-btv)#igmp user bind-profile service-port 100 profile-name music
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
```

8.2.4 (Optional) Configuring the Multicast Bandwidth

To limit the multicast bandwidth of a user, you can enable multicast bandwidth management, that is, connection admission control (CAC), and then control the bandwidth of a multicast user by setting the program bandwidth and the user bandwidth.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

If the CAC function is enabled and a user requests a multicast program, the system compares the remaining bandwidth of the user (bandwidth configured for the user - total bandwidth of the online programs of the user) with the bandwidth of the multicast program. If the remaining bandwidth of the user is sufficient, the system adds the user to the multicast group. If the bandwidth is insufficient, the system does not respond to the request of the user.

The MA5600T/MA5603T also supports dynamic application of unicast bandwidth for xDSL multicast users. This function is implemented through the ANCP protocol between the MA5600T/MA5603T and the BRAS. If CAC and ANCP are enabled on the device, when the user requests a multicast program, the resource admission control subsystem (RACS) compares the remaining bandwidth of the user with the bandwidth of the requested program. If the remaining bandwidth of the user is sufficient, the RACS adds the user to the multicast group. If the remaining bandwidth of the user is insufficient, the MA5600T/MA5603T applies to the RACS for the multicast video resource. Then, the RACS determines whether the available unicast video bandwidth of the user port can be allocated for the multicast video service of the user. In this way, the video bandwidth of the port is adjusted dynamically. For details on the ANCP configuration, see **Configuring ANCP**.

If the CAC function is disabled, the system does not guarantee the bandwidth of the multicast program. When the bandwidth is not guaranteed, problems such as mosaic and delay occur in the multicast program.

Table 8-7 lists the default settings of the CAC parameters.

Table 8-7 Default settings of the CAC parameters

Parameter	Default Value
Global CAC function	enable
Bandwidth of the multicast program	5000 kbit/s
Bandwidth of the multicast user	no-limit

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Enable the global CAC function.

By default, the global CAC function is already enabled. You can run the **igmp bandwidthCAC** { **enable** | **disable** } command to change the setting.

Step 3 Configure the bandwidth of the multicast user.

Run the **igmp user add service-port** *index* **max-bandwidth** command to allocate the maximum bandwidth of the multicast user.

Step 4 Configure the bandwidth of the multicast program.

- Run the **igmp program add ip** *ip-addr* **bandwidth** command to configure the bandwidth of a single multicast program. The program bandwidth is an attribute of a multicast program, specifying the bandwidth requirement of the program being played.
- Run the **igmp bandwidth port** *frameid/slotid/portid* **max-bandwidth** { *bandwidth* | **no-limit** } command to configure the program bandwidth of a physical port on a board. This command is available for only the GPON port. The default bandwidth of a port is 716800 kbit/s. Configuring the total program bandwidth for a single port is a way of traffic management, which helps avoid network congestion caused by the excessively-large total program bandwidth on a port. When the total program bandwidth of a port exceeds the value configured using the **igmp bandwidth port** *frameid/slotid/portid* **max-bandwidth** { *bandwidth* | **no-limit** } command, subsequent programs ordered by users on this port cannot be played.

Step 5 Check whether the multicast bandwidth configuration is correct.

- Run the **display igmp config global** command to check the status of the global CAC function.
- Run the **display igmp program** command to query the bandwidth allocated to the multicast program.
- Run the **display igmp user** command to query the maximum bandwidth and the occupied bandwidth of the multicast user.

----End

Example

To enable bandwidth management for multicast users, set the user bandwidth to 10 Mbit/s when adding multicast user 0/2/1, and configure the program bandwidth to 1 Mbit/s when adding multicast program 224.1.1.1.

```
huawei(config)#btv
huawei(config-btv)#igmp bandwidthcAC enable
huawei(config-btv)#igmp user add port 0/2/1 max-bandwidth 10240
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 bandwidth 1024
```

8.2.5 (Optional) Configuring Multicast Preview

Multicast preview is an advertizing method provided by carriers for ISPs. The purpose is to allow users to have an overview of a program in a controlled way. In other words, the duration, interval, and count of the user previews are controlled.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

The difference between program preview and normal program watching is that, after the user goes online, the duration of the preview is restricted. When the duration expires, the user goes offline. The user can request the program again only after the preview interval expires. The count by which the user can request the program within a day (the start time can be configured) is restricted by the preview count of the user.

Multicast preview parameters are managed through the preview profile. One program can be bound to only one preview profile, but one preview profile can be referenced by multiple programs.

Table 8-8 lists the default settings of the multicast preview parameters.

Table 8-8 Default settings of the multicast preview parameters

Parameter	Default Value
Global multicast preview function	enable
Preview profile	Preview profile with index 0

Parameter	Default Value
Preview profile parameters	Maximum preview duration: 120s Maximum preview count: 8 Minimum interval between two previews: 120s
Time for resetting the preview record	4:00:00 am
Valid duration of multicast preview	30s

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Enable the global multicast preview function.

By default, the global multicast preview function is enabled. You can run the **igmp preview**{ **enable** | **disable** } command to change the setting.

Step 3 Configure the preview profile.

Run the **igmp preview-profile add** command to configure the preview profile, and set the parameters: maximum preview duration, maximum preview count, and minimum interval between two previews. The system has a default preview profile with index 0.

Step 4 Bind the program to the preview profile.

In the multicast VLAN mode, run the **igmp program add ip** *ip-addr* **preview-profile** *index* command to bind the program to be previewed to the preview profile so that the program has the preview attributes as defined in the preview profile. By default, the program is bound to the preview profile with index 0.

Step 5 Change the time for resetting the preview record.

Run the **igmp preview auto-reset-time** command to change the time for resetting the preview record. The preview record of the user remains valid within one day. On the second day, the preview record is reset. By default, the system resets the preview record at 4:00:00 a.m.

Step 6 Modify the valid duration of multicast preview.

Run the **igmp proxy recognition-time** or **igmp preview recognition-time** command to modify the valid duration of multicast preview. If the actual preview duration of the user is shorter than the valid duration, the preview is not regarded as a valid one and is not added to the preview count. By default, the valid duration of multicast preview is 30s.

NOTE

If you use **igmp proxy recognition-time** and **igmp preview recognition-time** commands to set the valid duration of multicast preview concurrently, the one set by the **igmp preview recognition-time** command takes effect.

Step 7 Run the **display igmp config global** command to check whether the values of the multicast preview parameters are correct.

----End

Example

To enable preview of multicast programs by using the system default preview profile, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp preview enable
```

To enable preview of multicast programs, create preview profile 1, set the maximum preview time to 150s, the maximum preview count to 10, and apply this preview profile when adding program 224.1.1.1, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp preview enable
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 10
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 preview-profile 1
```

8.2.6 (Optional) Configuring Program Prejoin

In program prejoin, the MA5600T/MA5603T receives in advance the multicast stream of a program from the upper-layer multicast router to the upstream port before a user sends a request to join a program, shortening the waiting time of the user for requesting the program.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

Multicast program prejoin is the same as program request. The MA5600T/MA5603T plays the role of a user and sends the report packet for receiving in advance the multicast stream from the upper-layer multicast router to the upstream port.

After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, the unsolicited report function needs to be enabled so that the user can request the program quickly. Generally, the upper-layer multicast router processes the user request by responding to the group-specific query and the general query.

Table 8-9 lists the default settings of the prejoin parameters.

Table 8-9 Default settings of the prejoin parameters

Parameter	Default Value
Prejoin function	disable
Unsolicited report of IGMP packets	disable

Procedure

Step 1 Enable the prejoin function.

Run the **igmp program add ip** *ip-addr* **prejoin enable** command to enable the prejoin function of a program. By default, the prejoin function is disabled.

Step 2 After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, the unsolicited report function needs to be enabled for IGMP packets.

- Run the **igmp program add ip** *ip-addr* **unsolicited enable** command to enable the unsolicited report function for IGMP packets. By default, the unsolicited report function is disabled.
- Run the **igmp unsolicited-report interval** command to modify the interval for unsolicitedly reporting IGMP packets. By default, the interval is 10s.

Step 3 Check whether the prejoin function is configured correctly.

- Run the **display igmp program** command to query the status of the prejoin function and the unsolicited report function.
- Run the **display igmp config vlan** command to query the interval for unsolicitedly reporting IGMP packets.

----End

Example

To enable the prejoin function when adding program 224.1.1.1, do as follows:

```
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 prejoin enable
```

8.2.7 (Optional) Configuring the Multicast Logging Function

Multicast log serves as a criterion for carriers to evaluate the viewership of multicast programs.

Prerequisites

If the syslog is used for reporting multicast logs, the syslog server must be properly configured.

If the syslog server is not configured, you can run the **igmp syslog disable** command to disable the multicast syslog reporting function to save system resources.

Context

Multicast logs have three control levels: multicast VLAN level, multicast user level, and multicast program level. The system generates logs only when the logging functions at the three levels are enabled.

When the user stays online for longer than the valid time for generating logs, the system generates logs in any of the following conditions:

- The user goes offline naturally, by force, or abnormally.
- The user is blocked or deleted.
- The program is deleted.
- The program priority is changed.
- The upstream port to which the program is bound changes.
- The VLAN of the upstream port to which the program is bound changes.
- The right mode is switched.
- The user preview times out.
- The IGMP mode is switched.

- The bandwidth CAC is not passed.

The system supports up to 10K logs. When the user goes online, the system records only the online date and time. The system generates a complete log only when the user goes offline.

The MA5600T/MA5603T can report the multicast log to the log server in the syslog mode and the call detailed record (CDR) mode. By default, the MA5600T/MA5603T reports the log in the syslog mode.

- Syslog mode: Logs are reported to the syslog server in the form of a single log.
- CDR mode: Logs are reported to the log server in the form of a log file (.cvs). One log file contains multiple logs.

Table 8-10 lists the default settings of the multicast logging parameters.

Table 8-10 Default settings of the multicast logging parameters

Parameter	Default Value
Report mode of the multicast log	Syslog mode
Logging function at the multicast VLAN level	enable
Logging function at the multicast user level	enable
Logging function at the multicast program level	enable
Action report function of the multicast user	disable
Interval for automatically logging	2 hours
Minimum online duration for generating a valid log	30s
Parameters of the log report in the CDR mode	Report interval: 600s Maximum number of logs that can be reported each time: 200

Procedure

- Configure the parameters of the logging function of the multicast host.
  1. Enable the multicast logging functions.

     Multicast logs have three control levels: multicast VLAN level, multicast user level, and multicast program level. The system generates logs only when the logging functions at the three levels are enabled. By default, the three functions are enabled.

     - In the BTV mode, run the **igmp log** { **enable** | **disable** } command to configure the logging function at the multicast VLAN level.

- In the BTV mode, run the **igmp user add service-port** *index* **log** { **enable** | **disable** } command to configure the logging function at the multicast user level.

  In the BTV mode, run the **igmp log record** { **user** | **mac** } command to configure the log record object. After the configuration, the device can record ordering action of users or multicast terminals identified by MAC addresses.
- In the Multicast VLAN mode, run the **igmp program add ip** *ip-addr* **log** { **enable** | **disable** } command to configure the logging function at the multicast program level.

2. Modify the interval for automatically logging.

   In the BTV mode, run the **igmp proxy log-interval** command to modify the interval for automatically logging. When the user stays online for a long time, the system generates logs at the preset interval. This is to prevent the problem that a log is not generated when the user leaves the multicast group without sending a leave packet, which can affect the accounting. By default, the interval is two hours.
3. Modify the minimum online duration for generating a valid log.

   In the BTV mode, run the **igmp proxy recognition-time** or **igmp log recognition-time** command to modify the minimum online duration for generating a valid log. If the user is in a multicast group (such as to preview a program) for shorter than the preset duration, the user operation is not regarded as a valid one and a log is not generated. A log is generated only when a user stays online for longer than the specified duration. By default, the minimum online duration is 30s.

   NOTE

   If you use **igmp proxy recognition-time** and **igmp log recognition-time** commands to set the minimum online duration for generating a valid log concurrently, the one set by the **igmp log recognition-time** command takes effect.

- (Optional) Configure the action report function of the multicast user.

  By default, the system uses the syslog mode to report multicast logs. You can run the **igmp user-action-report** command to configure the action report function of the multicast user. By default, the action report function of the multicast user is disabled.
  - **enable**: Enables the action report function of the multicast user. Logs are reported to the syslog server when a multicast user goes online and offline.
  - **disable**: Disables the action report function of the multicast user. Logs are reported to the syslog server only when a multicast user goes offline.
- Configure the function of CDR-mode log report.
  1. Configure the multicast log server and the data transmission mode for the CDR-mode log report.

     Run the **file-server auto-backup cdr** command to configure the active and standby multicast log servers.
  2. Enable the function of CDR-mode log report.

     In the BTV mode, run the **igmp cdr** { **enable** | **disable** } command to configure the function of CDR-mode log report. After the function is enabled, the MA5600T/MA5603T reports the local multicast logs to the multicast log server in the form of a file. After the function is disabled, the MA5600T/MA5603T reports each single log to the syslog server in the default syslog mode.
  3. Configure the parameters of the log report in the CDR mode.

   - In the BTV mode, run the **igmp cdr-interval** command to set the report interval. By default, the interval is 600s.
   - In the BTV mode, run the **igmp cdr-number** command to set the maximum number of logs that can be reported each time. When the number of the multicast logs in the CDR file reaches the preset value, the MA5600T/MA5603T reports the logs. By default, the maximum number is 200.
4. Check whether the configuration is correct.
   - Run the **display file-server** command to query the configuration of the CDR multicast log server.
   - Run the **display igmp config global** command to query the status and other parameters of the function of CDR-mode log report.

----End

Example

To configure the multicast log to be reported to log server 10.10.10.1 in the CDR mode, and use the TFTP transmission mode, do as follows:

```
huawei(config)#file-server auto-backup cdr primary 10.10.10.1 tftp
huawei(config)#btv
huawei(config-btv)#igmp cdr enable
```

8.2.8 (Optional) Configuring the Maximum Number of Programs That Can Be Watched by the Multicast User

This topic describes how to configure the maximum number of programs that can be ordered by the multicast user at the same time. You can configure the maximum number of all programs that can be watched by the multicast user at the same time, or configure the maximum number of the different-level programs that can be watched by the multicast user.

Prerequisites

When you configure the maximum number of programs based on the program level, the program level must be configured at the same time and the programs must be configured statically.

Context

During automatic program generation, the number of the programs generated based on the same IGMP join request varies with the group filter mode. When the group filter mode of an MVLAN is configured to **asm-only** or **asm-ssm**, only one program with the unique multicast IP address is generated in the MVLAN. The [*, G] multicast forwarding table is used for this MVLAN instance on the forwarding plane. When the group filter mode of an MLVAN is configured to **ssm-only**, multiple programs with the same multicast IP addresses but different source IP addresses can be generated in the MVLAN. The [S, G] multicast forwarding table is used for this VLAN instance on the forwarding plane. The maximum number of programs is calculated according to the number of actually-generated programs. For example, when a multicast user joins an MVLAN with the multicast filter mode **asm-ssm** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates only one multicast program with the multicast IP address G1 for the multicast user; when a multicast user joins an MVLAN with the multicast filter mode **ssm-only** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates two multicast programs with IP addresses [S1, G1] and [S2, G1].

ASM Message

IGMP v2 message type:

- Join
- Leave

IGMP v3 message type:

- TO_IN({})
- IS_IN({})
- TO_EX({})
- IS_EX({})

Table 8-11 lists the actions of the ASM messages in different group filter modes.

Table 8-11 Actions of the ASM messages in different group filter modes

asm-only	ssm-only	asm-ssm
The system processes the [*, G] messages. The multicast packets are forwarded only according to the multicast IP addresses.	The system does not process the [*, G] messages.	The system processes the [*, G] messages. If there is no program with its multicast IP address identical to that carried in the message, the system generates a program without a source IP address according to the MVLAN and multicast IP address. If there is a program with the MVLAN, multicast IP address (identical to the multicast IP address of the message), and source IP address, the system does not generate a new program and users directly join this program. The multicast packets are forwarded only according to the multicast IP addresses.

SSM message

IGMP v2 message type:NA

IGMP v3 message type:

- ALLOW(S,G)
- BLOCK(S,G)
- TO_IN(S,G)
- IS_IN(S,G)

Table 8-12 lists the actions of the ASM and SSM messages in different group filter modes.

Table 8-12 Actions of the SSM messages in different group filter modes

asm-only	ssm-only	asm-ssm
The system does not process the [S, G] messages.	If messages with [S1, G1] and [S2, G2] are received, two programs with [S1, G1] and [S2, G2] are generated. The multicast packets are forwarded according to the multicast IP address and source IP address.	The system processes the [S, G] messages. If there is no program with its multicast IP address identical to that carried in the message in an MVLAN, the system generates the program with source IP address according to the VLAN, and multicast IP address and source IP address. If there is a program with the VLAN, multicast IP address (identical to the multicast IP address of the message), and source IP address (different from the source IP address of the message), the system does not process user's ordering requests. If there is a program without a source IP address but with the VLAN, and multicast IP address (identical to the multicast IP address of the message), the system does not generate a new program and users directly join this program. The multicast packets are forwarded only according to the multicast IP addresses.

Table 8-13 lists the default settings of the max-program parameters.

Table 8-13 Default settings of the multicast max-program parameters

Parameter	Default Value
Maximum number of programs that can be watched by the multicast user	8
Grade of the multicast program	no-grade

Parameter	Default Value
Maximum number of programs of different priorities that can be watched by the multicast user	no-limit

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Configure the max-program of the multicast user.

Run the **igmp user add service-port** ***index*** **max-program** ***max-program-num*** command to set the maximum number of programs that can be watched by the multicast user.

Step 3 Configure the maximum number of programs of different priorities that can be watched by the multicast user.

Run the **igmp user watch-limit service-port** ***index*** command to set the maximum number of programs of different priorities that can be watched by the multicast user.

Step 4 Configure the grade of the multicast program.

In the multicast VLAN mode, run the **igmp program add ip** ***ip-addr*** **grade**command to configure the grade of a multicast program.

Step 5 Check whether the multicast max-program configuration is correct.

- Run the **display igmp user** command to query the maximum number of programs that can be watched and watching by the multicast user.
- Run the **display igmp program** command to query the grade of the multicast program.
- Run the **display igmp user extended-attributes** command to query the maximum number of programs that can be watched and watching by the multicast user.

----End

Example

To set the user max-program to 10 when adding multicast service-port 0, set the user can watch 2 HDTV program, and configure the program grade to hdtv when adding multicast program 224.1.1.1, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 0 max-program 10
huawei(config-btv)#igmp user watch-limit service-port 0 hdtv 2
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-multicast-vlan 101)#igmp program add ip 224.1.1.1 grade hdtv
```

8.2.9 (Optional) Configuring the Maximum Rate for Sending IGMP Packets

When the multicast and anti-DoS attack functions are enabled, the system reports DoS attack alarms and drops IGMP packets over the rate limit, if a user port sends such IGMP packets to the CPU. When the anti-DoS attack function is disabled, the system always sends IGMP packets to the CPU. If they are sent to the CPU at a rate higher than the limit, the system drops the IGMP packets that exceed the rate limit but does not report DoS attack alarms.

Prerequisites

The multicast function is enabled.

Context

When the multicast function is enabled, the system will always send the received IGMP packets to the CPU if no control is implemented over the process. Then if a user port receives a large number of IGMP packets, the IGMP packets for other users will not be processed and directly dropped instead.

Table 8-14 lists the default system settings.

Table 8-14 Default system settings

Parameter	Default Value
Anti-DoS attack function	disable
Maximum rate for sending IGMP packets to the CPU	63 pps

Procedure

Step 1 Enable the anti-DoS attack function.

Run the **security anti-dos** { **enable** | **disable** } command to enable the anti-DoS attack function, which is disabled by default.

Step 2 Specify the maximum rate for sending IGMP packets to the CPU.

Run the **security anti-dos control-packet igmp rate** *frameid/slotid/portid* { **value** | **no-limit** } command to specify the maximum rate for sending IGMP packets to the CPU, which is 63 by default.

----End

Example

Example: Specify the maximum rate for sending IGMP packets to the CPU to 63 pps for user port 0/1/1, and enable the system to report the port to the blacklist if it sends IGMP packets over the rate limit to the CPU.

```
huawei(config)#security anti-dos enable
huawei(config)#security anti-dos control-packet igmp rate 0/1/1 20
```

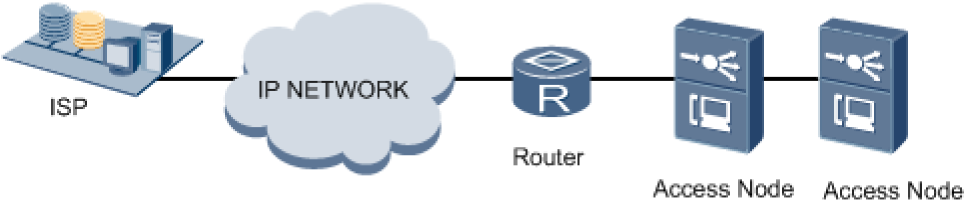
8.3 Configuring the Multicast Service in a Subtending Network

This topic describes how to configure the multicast service for an xDSL user of the MA5600T/MA5603T in a subtending network.

Application Context

Figure 8-1 shows the application context of the multicast service in a subtending network. When a subtended device needs to provision the multicast service, the subtending port on the subtending device needs to be configured as a multicast subtending port. In this way, the subtending device regards the subtended device as an IGMP user.

Figure 8-1 Application context of multicast service in a subtending network



Context

Default Configuration

Table 8-15 lists the default settings of the multicast service of the MA5600T/MA5603T.

Table 8-15 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	Disabled
IGMP version, includes multicast user version and multicast VLAN version.	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	Enabled
Multicast preview	Enabled
Multicast log function	Enabled

Precautions

- The multicast program list of the subtending device must cover the multicast program list of the subtended device.

- In this network, the MA5600T/MA5603T functions as a DSLAM, and the multicast VLANs of the subtending device and subtended device must be the same.

Procedure

The procedure for configuring the subtended device is the same as described in **Configuring the Multicast Service in a Single-NE Network**.

The procedure of configuring the subtending device is as follows:

1. For details on configuring the multicast service, see **Configuring the Multicast Service in a Single-NE Network**.
2. Configure the multicast subtending port.

   Run the **igmp cascade-port** *frameid/slotid/portid* command to configure the subtending port as the multicast subtending port. The multicast upstream port cannot be configured as a multicast subtending port.
3. Configure the mode for processing unknown multicast packets by the multicast subtending port.

   By default, the multicast subtending port transparently transmits the unknown multicast packets sent by lower-layer devices. This applies to the situation that the lower-layer devices may require the transparent transmission of unknown multicast packets. When multicast service is a priority, it is suggested to run the **igmp cascade-port** *frameid/slotid/portid* **mismatch** { **transparent** | **discard** } command to discard unknown multicast packets.
4. When the subtended device requires the quick leave function of the multicast user, run the **igmp cascade-port** *frameid/slotid/portid* **quickleave enable** command to enable the quick leave attribute on the multicast subtending port.

CAUTION

If the lower-layer device does not support the proxy of the IGMP leave packet, all the users requesting the program may go offline when a user requesting the same program goes offline. Therefore, when the quick leave attribute is enabled on the multicast subtending port, it is recommended that the lower-layer device use the IGMP proxy function, or switch to the IGMP snooping mode with the IGMP leave packet proxy function enabled.

8.4 Configuring the Multicast Service in an MSTP Network

This topic describes how to configure the multicast service for an xDSL user of the MA5600T/MA5603T in an MSTP network.

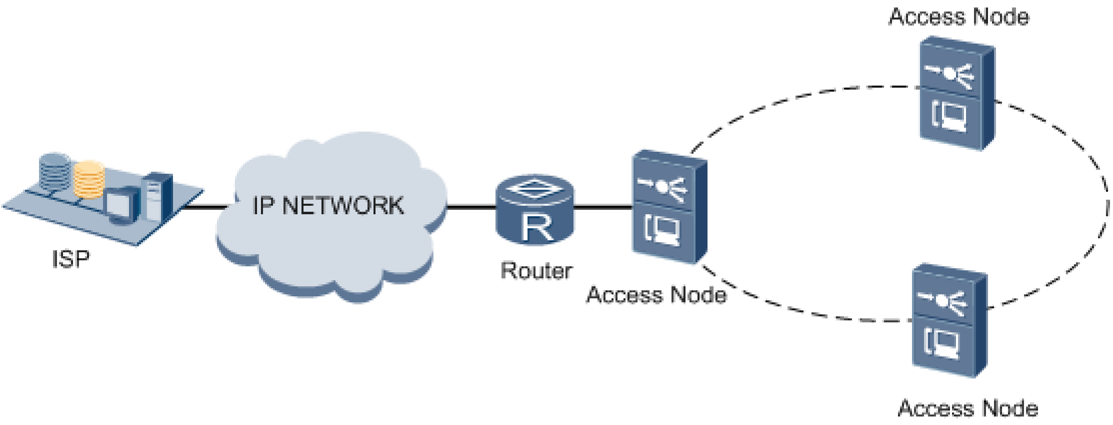
Prerequisites

Basic configurations for the MSTP network are complete. For details about configuring the MSTP network, see **Configuring the MSTP**.

Application Context

Figure 8-2 shows the application context of the multicast service in an MSTP network. When the multicast service is provisioned in an MSTP ring network, the multicast upstream port and the subtending port need to be added to the multicast VLAN. According to the running result of the MSTP protocol, the multicast request packets are sent from the root port or the default port (when the device is a root bridge), and the other ports in the VLAN serve as subtending ports.

Figure 8-2 Application context of the multicast service in an MSTP network



Context

Default Configuration

Table 8-16 lists the default settings of the multicast service of the MA5600T/MA5603T.

Table 8-16 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	Disabled
IGMP version, includes multicast user version and multicast VLAN version.	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	Enabled
Multicast preview	Enabled
Multicast log function	Enabled

Procedure

1. For details on configuring the MSTP ring network, see **Configuring the MSTP**.
2. For details on configuring the multicast service, see **Configuring the Multicast Service in a Single-NE Network**.
3. Configure the MSTP multicast upstream port.

   When multicast service is provisioned in an MSTP network, the multicast upstream port needs to be set to the MSTP mode, and the default upstream port of the multicast VLAN can be specified. After the configuration is completed, multicast packets are forwarded by the root port or default port of the multicast VLAN.

- Run the **igmp uplink-port-mode mstp** command to set the upstream port to the MSTP mode.
- Run the **igmp default uplink-port** command to specify the default upstream port of the multicast VLAN. When the upstream port is set to the MSTP mode and an MSTP root port is not available in the multicast VLAN, the multicast VLAN by default adopts the upstream port as the multicast upstream port.

4. Configure the multicast subtending port.

   Run the **igmp cascade-port** command to configure the subtending port as the multicast subtending port.

5. Configure multicast quick convergence in the case of an MSTP network topology change.

   Multicast quick convergence means that the device can quickly join the multicast group through a new upstream port when the MSTP network topology changes. The device can unsolicitedly send the new upstream port the IGMP join packet for an online program so that the device joins all the multicast groups. Or, the device can send the IGMP global leave packet to the upstream port. Then, the upper-layer querier sends a query packet for generating a new multicast forwarding tree.

   Run the **igmp send global-leave** command to enable the function of sending the IGMP global leave packet. When this function is enabled, the device sends the IGMP global leave packet to the upper-layer multicast router. When this function is disabled, the device sends the IGMP join packet to the upper-layer multicast router. By default, the function of sending the IGMP global leave packet is enabled.

9 Configuring the Multicast Service (PON)

About This Chapter

This topic describes how to configure the GPON multicast service on the MA5600T/MA5603T in a single-NE network.

For details about multicast features, see Multicast.

Data Plan

Before configuring the multicast video service, plan the data items as listed in **Table 9-1**.

Table 9-1 Data items planned for the multicast service

Device	Data Item	Remarks
MA5600T/ MA5603T	Layer 2 multicast protocol	-
	IGMP version	-
	Multicast program configuration mode	-
	Parameter values of the multicast protocol	-
	Program list	-
	User authentication policy	-
	Program bandwidth, upstream port bandwidth, and user bandwidth	-
	Multicast ONT	-
	Multicast log policy	-

Device	Data Item	Remarks
Upper-layer multicast router	IGMP version	The IGMP version of the upper-layer multicast router cannot be earlier than the IGMP version used by the MA5600T/ MA5603T.

Configuration Flowchart

1. 9.1 Differences Between the IPv4 Multicast Configuration and IPv6 Multicast Configuration
   IPv6 multicast refers to the multicast service of the IPv6 protocol. Differences between the IPv4 multicast configuration and IPv6 multicast configuration mainly rest on commands and functions. It is recommended that you know well about how to configure the IPv4 service and then configure the IPv6 service based on their differences.
2. 9.2 Configuring Multicast Global Parameters
   The general parameters of Layer 2 multicast protocols (including IGMP proxy and IGMP snooping) configured for a device are applicable to all the multicast VLANs on the device.
3. 9.3 Configuring the Multicast VLAN and the Multicast Program
   In the application of multicast service, multicast VLANs (MVLANs) are used to distinguish multicast ISPs. Generally, an MVLAN is allocated to each multicast ISP for the VLAN-based management of multicast programs, multicast protocols, IGMP versions, and the VLAN-based control of multicast domain and user right.
4. 9.4 Configuring the Multicast GPON ONT
   When the MA5600T/MA5603T is connected with an ONT or an MDU, you need to configure the multicast interconnection data to forward the multicast traffic streams.
5. 9.5 Configuring a Multicast User
   This topic describes how to configure a multicast user and the related authority to provision the multicast service.
6. 9.6 (Optional) Configuring the Multicast Bandwidth
   To limit the multicast bandwidth of a user, you can enable multicast bandwidth management, that is, connection admission control (CAC), and then control the bandwidth of a multicast user by setting the program bandwidth and the user bandwidth.
7. 9.7 (Optional) Configuring Multicast Preview
   Multicast preview is an advertising method provided by carriers for ISPs. The purpose is to allow users to have an overview of a program in a controlled way. In other words, the duration, interval, and count of the user previews are controlled.
8. 9.8 (Optional) Configuring Program Prejoin
   The channel change request sent by a user needs to be processed by different intermediate devices on the network, which brings a channel change delay. Program prejoin is able to shorten the channel change delay, improving user experience.
9. 9.9 (Optional) Configuring the Multicast Logging Function
   Multicast log serves as a criterion for carriers to evaluate the viewership of multicast programs.
10. 9.10 (Optional) Configuring the Maximum Number of Programs That Can Be Watched by the Multicast User

This topic describes how to configure the maximum number of programs that can be ordered by the multicast user at the same time. You can configure the maximum number of all programs that can be watched by the multicast user at the same time, or configure the maximum number of the different-level programs that can be watched by the multicast user.

11. 9.11 (Optional) Configuring the Maximum Rate for Sending IGMP Packets
    When the multicast and anti-DoS attack functions are enabled, the system reports DoS attack alarms and drops IGMP packets over the rate limit, if a user port sends such IGMP packets to the CPU. When the anti-DoS attack function is disabled, the system always sends IGMP packets to the CPU. If they are sent to the CPU at a rate higher than the limit, the system drops the IGMP packets that exceed the rate limit but does not report DoS attack alarms.

9.1 Differences Between the IPv4 Multicast Configuration and IPv6 Multicast Configuration

IPv6 multicast refers to the multicast service of the IPv6 protocol. Differences between the IPv4 multicast configuration and IPv6 multicast configuration mainly rest on commands and functions. It is recommended that you know well about how to configure the IPv4 service and then configure the IPv6 service based on their differences.

Command Differences

Table 9-2 Differences between IPv4 multicast commands and IPv6 multicast commands

NOTE
"-" indicates that there is no command in IPv6 corresponding to the one in IPv4. That is, the corresponding multicast feature is not supported in IPv6.

IPv4	IPv6
Multicast additional function	
igmp leave-proxy	igmp ipv6 leave-proxy
igmp priority	igmp ipv6 priority
imgp report-proxy	igmp ipv6 report-proxy
igmp accelerator	-
igmp echo	-
igmp encapsulation	-
igmp multicast-tag	igmp multicast-tag
igmp policy	-
igmp query-offline-user	-
igmp user-action-report	-
igmp mismatch	-
display igmp policy	-
igmp sip-gip-forward	-
Protocol parameter	
igmp proxy router gen-query-interval	igmp ipv6 proxy router gen-query-interval
igmp proxy router gen-response-time	igmp ipv6 proxy router gen-response-time
igmp proxy router robustness	igmp ipv6 proxy router robustness
igmp proxy router sp-query-interval	igmp ipv6 proxy router sp-query-interval
igmp proxy router sp-query-number	igmp ipv6 proxy router sp-query-number

IPv4	IPv6
igmp proxy router sp-response-time	igmp ipv6 proxy router sp-response-time
igmp initial-unsolicited-report interval	igmp ipv6 initial-unsolicited-report interval
igmp unsolicited-report interval	igmp ipv6 unsolicited-report interval
display igmp config vlan	display igmp ipv6 config vlan
igmp proxy router timeout	-
Multicast VLAN (MVLAN)	
igmp mode	igmp ipv6 mode
igmp match mode	igmp ipv6 match mode
igmp version	igmp ipv6 version
igmp match group	igmp ipv6 match group
display igmp config vlan	display igmp ipv6 config vlan
igmp inner-vlan	igmp inner-vlan
igmp send global-leave	-
Multicast user and right	
debugging igmp	debugging igmp ipv6
Preview	
igmp preview	-
igmp preview auto-reset-time	-
igmp preview reset count	-
igmp preview reset record	-
igmp preview-profile add	-
igmp preview-profile delete	-
igmp preview-profile modify	-
display igmp preview user	-
display igmp preview-profile	-
Statistics	
igmp statistic reset	igmp ipv6 statistic reset
display igmp statistic	display igmp ipv6 statistic
display multicast flow-statistic	-
Log	

IPv4	IPv6
display igmp log statistic	-

NOTE

The multicast commands that are not listed in this table are the commands shared by the IPv4 multicast and IPv6 multicast.

Function Differences

Compared with the IPv4 multicast feature, the IPv6 feature does not support the following sub features currently:

- SIP+GIP forwarding mode
- Layer 3 IPv6 multicast routing protocol
- Transparent transmission of unknown IGMP packets
- Spanish multicast log mode
- Dynamic generation of multiple program segments
- Multicast preview
- Video stream statistics
- Global leave
- Load sharing between active and standby control boards
- Transparent transmission policy and VLAN-based forwarding policy for mismatched IGMP packets
- Recognition of MLD PPPoE packet (only transparent transmission of MLD PPPoE packets is supported)
- Reporting of IPv6 multicast log

Differences in the Multicast Basic Service Configuration

IPv4 multicast can share VLANs with IPv6 multicast; therefore, you can deploy IPv6 multicast in existing IPv4 MVLANs only by adding IPv6 multicast programs in the IPv4 MVLANs and in rights profiles. The configured parameters such as the bound right profiles and MVLANs can remain unchanged.

9.2 Configuring Multicast Global Parameters

The general parameters of Layer 2 multicast protocols (including IGMP proxy and IGMP snooping) configured for a device are applicable to all the multicast VLANs on the device.

Context

The multicast global parameters include general query, group-specific query, and the policy of processing multicast packets.

The description of a general query is as follows:

- Purpose: A general query packet is periodically sent by the MA5600T/MA5603T to check whether there is any multicast user who leaves the multicast group without sending the leave packet. Based on the query result, the MA5600T/MA5603T periodically updates the multicast forwarding table and releases the bandwidth of the multicast user that has left the multicast group.
- Principle: The MA5600T/MA5603T periodically sends the general query packet to all online IGMP users. If the MA5600T/MA5603T does not receive the response packet from a multicast user within a specified time (Robustness variable x General query interval + Maximum response time of a general query), it regards the user as having left the multicast group and deletes the user from the multicast group.

The description of a group-specific query is as follows:

- Purpose: A group-specific query packet is sent by the MA5600T/MA5603T after a multicast user that is not configured with the quick leave attribute sends the leave packet. The group-specific query packet is used to check whether the multicast user has left the multicast group.
- Principle: When a multicast user leaves a multicast group, for example, switches to another channel, the user unsolicitedly sends a leave packet to the MA5600T/MA5603T. If the multicast user is not configured with the quick leave attribute, the MA5600T/MA5603T sends a group-specific query packet to the multicast group. If the MA5600T/MA5603T does not receive the response packet from the multicast user within a specified duration (Robustness variable x Group-specific query interval + Maximum response time of a group-specific query), it deletes the multicast user from the multicast group.

Table 9-3 lists the default settings of the multicast global parameters. In the actual application, you can modify the values according to the data plan.

Table 9-3 Default settings of the multicast global parameters

Parameter	Default Value
General query parameter	Query interval: 125s Maximum response time: 10s Robustness variable (query times): 2
Group-specific query parameter	Query interval: 1s Maximum response time: 0.8s. Robustness variable (query times): 2
Policy of processing multicast packets	IGMP packet: normal (IGMP packets are processed as controllable multicast) Unknown multicast packet: ● For switch-oriented traffic streams: discard ● For connection-oriented traffic streams: transparent transmission

Procedure

Step 1 Configure the general query parameters.

1. Run the **igmp proxy router gen-query-interval** command to set the general query interval..
2. Run the **igmp proxy router gen-response-time** command to set the maximum response time of the general query..
3. Run the **igmp proxy router robustness** command to set the robustness variable (query times) of the general query.

Step 2 Set the group-specific query parameters.

1. Run the **igmp proxy router sp-response-time** command to set the group-specific query interval.
2. Run the **igmp proxy router sp-query-interval** command to set the maximum response time of the group-specific query.
3. Run the **igmp proxy router sp-query-number** command to set the robustness variable (query times) of the group-specific query.

Step 3 Configure the policy of processing multicast packets.

By default, the normal mode for processing IGMP packets is adopted. In this mode, IGMP packets are processed as controllable multicast. The discard mode is adopted for unknown multicast packets. In this mode, unknown multicast packets are discarded.

The default values are adopted for multicast service and do not need to be modified. To control the forwarding of multicast packets when configuring other services, run the following commands to configure the policy.

1. Run the **igmp policy** command to set the policy of processing IGMP packets.
2. Run the **multicast-unknown policy** command to set the policy of processing unknown multicast packets.

Step 4 Run the **display igmp config global** command to check whether the values of the multicast parameters are correct.

----End

Example

To configure the IGMP v3 general query parameters of IPv4 MVLAN 100 by setting the query interval to 150s, maximum response time to 20s, and number of queries to 3, do as follows:

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp proxy router gen-query-interval 150
huawei(config-mvlan100)#igmp proxy router gen-response-time v3 20
huawei(config-mvlan100)#igmp proxy router robustness 3
```

To configure the IGMP v3 group-specific query parameters of IPv4 MVLAN 100 by setting the query interval to 200s, maximum response time to 100s, and number of queries to 3, do as follows:

```
huawei(config)#btv
huawei(config-mvlan100)#igmp proxy router sp-query-interval 200
huawei(config-mvlan100)#igmp proxy router sp-response-time v3 100
huawei(config-mvlan100)#igmp proxy router sp-query-number 3
```

To configure the MLD v2 general query parameters of IPv6 MVLAN 200 by setting the query interval to 150s, maximum response time to 20s, and number of queries to 3, do as follows:

```
huawei(config)#multicast-vlan 200
huawei(config-mvlan200)#igmp ipv6 router gen-query-interval 150
huawei(config-mvlan200)#igmp ipv6 router gen-response-time v2 20
huawei(config-mvlan200)#igmp ipv6 router robustness 3
```

To configure the MLD v2 group-specific query parameters of IPv6 MVLAN 200 by setting the query interval to 200s, maximum response time to 100s, and number of queries to 3, do as follows:

```
huawei(config)#multicast-vlan 200
huawei(config-mvlan200)#igmp ipv6 router sp-query-interval 200
huawei(config-mvlan200)#igmp ipv6 router sp-response-time v2 100
huawei(config-mvlan200)#igmp ipv6 router sp-query-number 3
```

9.3 Configuring the Multicast VLAN and the Multicast Program

In the application of multicast service, multicast VLANs (MVLANs) are used to distinguish multicast ISPs. Generally, an MVLAN is allocated to each multicast ISP for the VLAN-based management of multicast programs, multicast protocols, IGMP versions, and the VLAN-based control of multicast domain and user right.

Context

To create an MVLAN, a common VLAN must be created first. The MVLAN can be the same as the unicast VLAN. In this case, the two VLANs can share the same service stream channel. The MVLAN can be different from the unicast VLAN. In this case, the two VLANs use different service stream channels.

One user port can be added to multiple MVLANs under the following restrictions:

- Among all the MVLANs of a user port, only one MVLAN is allowed to have dynamically generated programs.
- One user port is not allowed to belong to multiple MVLANs that are in the IGMP v3 snooping mode.

Table 9-4 lists the default settings of the MVLAN attributes, including the Layer 2 multicast protocol, IGMP version, multicast program, and multicast upstream port.

Table 9-4 Default settings of the MVLAN attributes

Parameter	Default Value
Program matching mode	Enable (static configuration mode)
Multicast upstream port mode	Default
Layer 2 multicast protocol	Off (multicast function disabled)
IGMP version (IPv4 multicast)	V3
MLD version (IPv6 multicast)	V2
Priority of forwarding IGMP packets by the upstream port	6
Group filter mode	asm-ssm

NOTE

The device supports both the IPv4 multicast and IPv6 multicast. The configuration differences between the IPv4 multicast and IPv6 multicast rest on only the commands for configuring the multicast program but not the configuration of the multicast program. The configuration procedure in this topic is based on the IPv4 multicast and the related configuration of the IPv6 multicast will be mentioned in the example.

Procedure

Step 1 Create an MVLAN.

1. Run the **vlan** command to create a VLAN, and set the VLAN type according to the actual application. For details on the VLAN configuration, see **Configuring VLAN**.
2. Run the **multicast-vlan** command to set the created VLAN to an MVLAN. The VLAN with S+C forwarding mode cannot be set as an MVLAN.

Step 2 Configure multicast programs.

The program configuration of the MVLAN has three modes: static configuration, dynamic generation, and static and dynamic mixed configuration.

- Static configuration mode: Configure the program list before the users watch the video programs. In this mode, the right profile can be used to implement controllable multicast. The program list and the right profile, however, need to be maintained according to the change of the video service. The program host, program prejoin, and multicast bandwidth management functions are supported.

1. Run the **igmp match mode enable** command to set the static configuration mode. By default, the system adopts the static configuration mode.
2. Run the **igmp program add** [**name** *name*] **ip** *ip-addr* [**sourceip** *ip-addr*] [**hostip** *ip-addr*] command to add a multicast program.

   NOTE

   If the IGMP version of an MVLAN is v3, the program must be configured with a source IP address. If the IGMP version of an MVLAN is v2, the program must not be configured with a source IP address.
3. Add a right profile.

   In the BTV mode, run the **igmp profile add** command to add a right profile.
4. Bind the program to the right profile.

   In the BTV mode, run the **igmp profile** command to bind the program to the right profile, and set the right to watch.

   NOTE

   When a user is bound to multiple right profiles, and the right profiles have different rights to a program, the right with the highest priority prevails. You can run the **igmp right-priority** command to adjust the priorities of the four rights: watch, preview, forbidden, and idle. By default, the priorities of the four rights are forbidden > preview > watch > idle.

- Dynamic generation mode: A program list is dynamically generated 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.

1. Run the **igmp match mode disable** command to set the dynamic generation mode.

⚠ **CAUTION**

The **igmp match mode** command can be executed only when the IGMP mode is disabled.

2. Run the **igmp match group** command to configure the IP address range of the program group that can be dynamically generated. Users can order only the programs whose IP addresses are within the specified range.

- Static and dynamic mixed configuration: Add some programs (generally popular programs) as static programs and dynamically generate other programs based on user requests. In this mode, users can quickly order popular programs and reduce the channel switch time.

1. Run the **igmp match mode disable** command to set the mode to the dynamic generation mode.
2. Run the **igmp match group** command to configure the IP address range of the program group that can be dynamically generated. Users can order only the programs whose IP addresses are within the specified range.
3. Run the **igmp program add** [**name** *name*] **ip** *ip-addr* [**sourceip** *ip-addr*] [**hostip** *ip-addr*] command to add a multicast static program.

   📖 **NOTE**

   When the range of static program IP addresses and the range of dynamic program IP addresses overlap each other, static programs can go online with priority.

4. Run the **igmp group-filter-mode** command to set the group filter mode based on multicast VLAN (MVLAN).

   📖 **NOTE**

   - When the group filter mode of an MVLAN is configured to **asm-only** or **asm-ssm**, only one program with the unique multicast IP address is generated in the MVLAN. The [*, G] multicast forwarding table is used for this MVLAN instance on the forwarding plane.
   - When the group filter mode of an MLVAN is configured to **ssm-only**, multiple programs with the same multicast IP addresses but different source IP addresses can be generated in the MVLAN. The [s, g] multicast forwarding table is used for this VLAN instance on the forwarding plane.

     📖 **NOTE**

     The source IP addresses are regarded as different ones when they have different least significant 20 bits from each other.

   - The maximum number of programs is calculated according to the number of actually-generated programs. For example:
     - When a multicast user joins an MVLAN with the multicast filter mode **asm-ssm** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates only one multicast program with the multicast IP address G1 for the multicast user;
     - When a multicast user joins an MVLAN with the multicast filter mode **ssm-only** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates two multicast programs with IP addresses [S1, G1] and [S2, G1].

Step 3 Configure the multicast upstream port.

1. Run the **igmp uplink-port** command to configure the multicast upstream port. The packets of the MVLAN corresponding to the upstream port are forwarded and received by this upstream port.
2. In the BTV mode, run the **igmp uplink-port-mode** command to change the mode of the multicast upstream port. By default, the port is in the default mode. In the MSTP network, the port adopts the MSTP mode.

- Default mode: If the MVLAN contains only one upstream port, the multicast packets that go upstream can be sent only by this port. If the MVLAN contains multiple upstream ports, the multicast packets that go upstream are sent by all the upstream ports.
- MSTP mode: This mode is adopted in the MSTP network.

Step 4 Select the multicast mode.

Run the **igmp mode** { **proxy** | **snooping** } command to select the Layer 2 multicast mode. By default, the multicast mode is disabled.

In terms of multicast processing mode, the MA5600T/MA5603T supports the Internet Group Management Protocol (IGMP) Proxy and IGMP Snooping Layer 2 multicast protocols. IGMP proxy and IGMP snooping both support multicast video data forwarding; however, the two modes have different processing mechanisms.

- In IGMP snooping, the related information for maintaining multicast forwarding entries is obtained by listening to the IGMP packets between the user and the multicast router.
- IGMP proxy intercepts the IGMP packets between the user and the multicast router, processes the IGMP packets, and then forwards the IGMP packets to the upper-layer multicast router. For the multicast user, the MA5600T/MA5603T is a multicast router that implements the router functions in the IGMP protocol; for the multicast router, the MA5600T/MA5603T is a multicast user.

In the IGMP snooping mode, proxy can be enabled for the report packet and the leave packet. When a multicast user joins or leaves a multicast program, the MA5600T/MA5603T can implement IGMP proxy. IGMP snooping and IGMP proxy are controlled separately.

- Run the **igmp report-proxy enable** command to enable the proxy of the snooping report packet. When the first user requests to join a program, after authenticating the user, the MA5600T/MA5603T sends the user report packet to the network side and receives a corresponding multicast stream from the multicast router. The report packets of the users that follow the first user are not sent by the MA5600T/MA5603T to the network side.
- Run the **igmp leave-proxy enable** command to enable the proxy of the snooping leave packet. When the last user requests to leave the program, the MA5600T/MA5603T sends the user leave packet to the network side to request the upper-layer device to stop sending multicast streams. The leave packets of the users that precede the last user are not sent by the MA5600T/MA5603T to the network side.

Step 5 Set the IGMP version.

Run the **igmp version**{ **v2** | **v3** } command to set the IGMP version. By default, IGMP v3 is enabled in the system. If the upper-layer and lower-layer devices in the network are IGMP v2 devices and cannot recognize the IGMP v3 packets, run this command to change the IGMP version.

IGMP v3 is compatible with IGMP v2 in packet processing. If IGMP v3 is enabled on the MA5600T/MA5603T and the upper-layer multicast router switches to IGMP v2, the MA5600T/MA5603T automatically switches to IGMP v2 when receiving the IGMP v2 packets. If the MA5600T/MA5603T does not receive any more IGMP v2 packets within the preset IGMP v2 timeout time, it automatically switches back to IGMP v3. In the BTV mode, run the **igmp proxy router timeout** command to set the IGMP v2 timeout time. By default, the timeout time is 400s.

Step 6 Change the priority for forwarding IGMP packets.

Run the **igmp priority** command to change the priority for forwarding the IGMP packets by the upstream port. By default, the priority is 6 and does not need to be changed.

- In the IGMP proxy mode, the IGMP packets sent from the upstream port to the network side adopt the priority set through the preceding command in the MVLAN.
- In the IGMP snooping mode, the IGMP packets forwarded to the network side adopt the priority of the user service stream. The priority of the service stream is set through the traffic profile.

Step 7 Check whether the configuration is correct.

- Run the **display igmp config vlan** command to query the attributes of the MVLAN.
- Run the **display igmp program vlan** command to query the information about the program of the MVLAN.

----End

Example

Assume that:

- MVLAN ID: 101
- Program configuration mode: static configuration; program IP address: 224.1.1.1
- Source IP address: 10.10.10.10; host IP address: 10.0.0.254
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/19/0
- Protocol: IGMP proxy; IGMP version: v3
- Group filter mode: ssm-only

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode enable
huawei(config-mvlan101)#igmp program add name movie ip 224.1.1.1 sourceip
10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#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
huawei(config-mvlan101)#igmp version v3
huawei(config-mvlan101)#igmp group-filter-mode ssm-only
```

Assume that:

- MVLAN ID: 101
- Program configuration mode: dynamic generation
- Address range of the dynamic program group: 224.1.1.10 to 224.1.1.50
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/19/0
- Protocol: IGMP proxy; IGMP version: v3

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#iigmp match mode disable
  This operation will delete all the programs in current multicast vlan
  Are you sure to change current match mode? (y/n)[n]: y
  Command is being executed, please wait...
  Command has been executed successfully
huawei(config-mvlan101)#igmp match group ip 224.1.1.10 to-ip 224.1.1.50
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#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
huawei(config-mvlan101)#igmp version v3
```

Assume that:

- MVLAN ID: 101
- Program configuration mode: static and dynamic mixed configuration
- MVLAN upstream port: 0/19/0
- IP address of the static program: 224.1.1.1; source IP address: 10.10.10.10; host IP address: 10.0.0.254; program bandwidth: 5000 kbit/s
- Address range of the dynamic program group: 224.1.1.10 to 224.1.1.50
- Protocol: IGMP proxy; IGMP version: v3

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode disable
  This operation will delete all the programs in current multicast vlan
  Are you sure to change current match mode? (y/n)[n]: y
  Command is being executed, please wait...
  Command has been executed successfully
huawei(config-mvlan101)#igmp match group ip 224.1.1.10 to-ip 224.1.1.50
huawei(config-mvlan101)#igmp program add name movie ip 224.1.1.1 sourceip 
10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#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
huawei(config-mvlan101)#igmp version v3
```

Assume that:

- MVLAN ID: 101
- Program configuration mode: static configuration; program IP address:ffff::1
- Source IPv6 address: 2000::1
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/19/0
- Protocol: IGMP proxy; IGMP version: v2

To configure the MVLAN and multicast program for the IPv6 multicast, do as follows:

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode enable
huawei(config-mvlan101)#igmp program add name movie ipv6 ffff::1 source-ipv6 
2000::1
 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/19/0
huawei(config-mvlan101)#igmp ipv6 mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

```
huawei(config-mvlan101)#igmp ipv6 version v2
```

9.4 Configuring the Multicast GPON ONT

When the MA5600T/MA5603T is connected with an ONT or an MDU, you need to configure the multicast interconnection data to forward the multicast traffic streams.

Prerequisites

Before configuring the multicast GPON ONT, you must add the ONT correctly. For the configuration method, see **Configuring the GPON ONT**.

Context

- When the OLT is connected with an ONT such as the HG850e, the MA5600T/MA5603T manages the ONT in the OMCI mode. In this case, you need to configure the ONT line profile and the ONT service profile, configure the multicast data in the ONT service profile, and bind the profiles to the ONT to issue the multicast service.
- When the OLT is connected with an MDU such as the MA5620 or MA5616, the MA5600T/ MA5603T manages the MDU in the SNMP mode. In this case, you do not need to configure the ONT service profile. You only need to configure the multicast data on the MDU interconnected with the MA5600T/MA5603T to forward the multicast traffic streams.

Procedure

Step 1 Add an ONT line profile.

For the configuration method, see **Configuring the GPON ONT Line Profile**.

Step 2 Add an ONT service profile.

Run the **ont-srvprofile gpon** command to add a GPON ONT service profile, and then enter the GPON ONT service profile mode.

If the ONT management mode is the SNMP mode, you do not need to configure the service profile. After adding a GPON ONT service profile, directly enter the GPON ONT service profile mode to configure the related multicast data.

1. Run the **ont-port** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.
2. Run the **port vlan** command to configure the port VLAN of the ONT.
3. Configure the multicast mode of the ONT.

   Run the **multicast mode** { **igmp-snooping**|**olt-control**|**unconcern** } command to select the multicast mode.

   - **igmp-snooping**: IGMP snooping obtains related information and maintains the multicast forwarding entries by listening to the IGMP packets in the communication between the user and the multicast router.
   - **olt-control**: It is the dynamic controllable multicast mode. A multicast forwarding entry can be created for the multicast join packet of the user only after the packet passes the authentication.

- **unconcern**: It is the unconcern mode. After this mode is selected, the OLT does not limit the multicast mode, and the multicast mode on the OLT automatically matches the multicast mode on the ONT.

4. (Optional)Configure the multicast forwarding mode.

   Run the **multicast-forward** { **untag** | **tag** { **translation***vlanid* | **transparent** } | **unconcern** command to configure the multicast forwarding mode and multicast forwarding VLAN. The forwarding mode is not concerned by default.

   - **tag**: Specifies the multicast forwarding mode as tag. If the VLAN tag of the multicast packet needs to be transparently transmitted, use **transparent**; if the VLAN tag of the multicast packet needs to be switched, use **translation** and set the VLAN tag used after the switching. When the ONT is directly connected to the home gateway in the application, use this parameter.
   - **untag**: Specifies the multicast forwarding mode as untag, that is, the downstream multicast packet from the ONT's Ethernet port to a next directly connected device does not carry the VLAN tag. When the ONT is directly connected to the set top box (STB) or PC, use this parameter.
   - **unconcern**: Indicates that the multicast forwarding mode is not concerned. When the ONT multicast mode need not be configured by the OLT and is determined by the ONT condition, use **unconcern**. This value is the default value.

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

   NOTE

   For an ONT that is added through the **ont add** command or an automatically found ONT that is confirmed through the **ont confirm** command, if you run the **commit** command after modifying the ONT line profile parameters and the ONT service profile parameters, the modified profile parameters take effect immediately.

----End

Example

To configure the ONT service profile 10 of 4 ETH ports, 2 POTS ports, the VLAN of the ETH port as 10, the multicast mode as IGMP snooping, the multicast forwarding mode as unconcern, do as follows:

```
huawei(config)#ont-srvprofile gpon profile-id 10
huawei(config-gpon-srvprofile-10)#ont-port eth 4 pots 2
huawei(config-gpon-srvprofile-10)#port vlan eth 1 10
huawei(config-gpon-srvprofile-10)#multicast mode igmp-snooping
huawei(config-gpon-srvprofile-10)#multicast-forward unconcern
huawei(config-gpon-srvprofile-10)#commit
huawei(config-gpon-srvprofile-10)#quit
```

9.5 Configuring a Multicast User

This topic describes how to configure a multicast user and the related authority to provision the multicast service.

Prerequisites

Before configuring a multicast user, you need to create the service channel. The procedure is as follows:

- Configure a GPON multicast user
  1. **Configure the VLAN**
  2. **Configure the upstream port**
  3. **Configure the multicast GPON ONT**
  4. **Configure the GPON user port**
  5. **Configure the GPON traffic stream**

Context

Add a multicast user and bind the multicast user to the multicast VLAN to create a multicast member. Bind the multicast user to an authority profile to implement multicast user authentication.

Table 9-5 lists the default settings of the multicast user attributes.

Table 9-5 Default settings of the multicast user attributes

Parameter	Default Setting
Maximum number of programs that can be watched by the multicast user	8
Maximum number of programs of different priorities that can be watched by the multicast user	no-limit
Quick leave mode of the multicast user	mac-based
Global switch of multicast user authentication	enable

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Configure a multicast user and the multicast user attributes.

1. Add a multicast user.

   Run the **igmp user add service-port** command to add a multicast user.

2. Configure the maximum number of programs that can be watched by the multicast user.
   - Run the **igmp user add service-port** *index* **max-program** { **max-program-num** | **no-limit** } command to set the maximum number of programs that can be watched by the multicast user concurrently. Up to 32 programs can be watched by the multicast user concurrently. By default, it is 8.
   - Run the **igmp user watch-limit service-port** { **hdtv** | **sdtv** | **streaming-video** } command to set the maximum number of programs at various levels that can be watched by the multicast user.

3. Set the quick leave mode of the multicast user.

Run the **igmp user add service-port** *index* **quickleave** { **immediate** | **disable** | **mac-based** } command to set the quick leave mode of the multicast user. By default, the quick leave mode is the mac-based mode.

- **immediate**: After receiving the leave request packet of the multicast user, the system immediately deletes the multicast user from the multicast group. This setting is applicable to the scenario where only one terminal is connected to the same port or the terminal works in the IGMP proxy mode.
- **disable**: Disables quick leave, allowing multicast users to leave in a normal way. After receiving the leave request packet of the multicast user, the system sends ACK packets to confirm that the multicast user leaves, and then deletes the multicast user from the multicast group. This is a standard mode defined in the IGMP protocol.
- **mac-based**: It is the quick leave mode based on the MAC address. The system detects the MAC address in the leave packet of the user. If it is the same as the MAC address in the report packet of the user, the system immediately deletes the multicast user from the multicast group. Otherwise, the system does not delete the multicast user. In this mode, the application scenario with multiple terminals is supported.

NOTE

For details about the working principle and selection principle of quick leave, see User-side Interoperating Technologies.

4. Set the IGMP version for the multicast user.

   Run **igmp user add service-port** *index* **igmp-version** { **v2** | **v3** | **v3-forced** } command to set the IGMP version for the multicast user. Each multicast users has an independent querier instance. This command specifies the IGMP version (default: v3) for the multicast user querier.

   - v2: specifies the IGMP version to v2 for the multicast user querier. When this setting applies, the system processes only IGMP v2 packets and directly drops IGMP v1 packets and IGMP v3 packets.
   - v3: specifies the v3–compatible mode (default setting for the system). When this setting applies, the system automatically specifies the IGMP version according to the version of the IGMP packets sent by users, but it directly drops IGMP v1 packets.
   - v3-forced: forcibly specifies the IGMP version to V3 for the multicast user querier. When this setting applies, the system processes only IGMP v3 packets but directly drops IGMP v1 packets and IGMP v2 packets.

Step 3 Configure multicast user authentication.

To control the authority of a multicast user, you can enable the multicast user authentication function.

1. Configure the multicast user authentication switch.

   Run the **igmp user add service-port** *index* { **auth** | **no-auth** } command to configure whether to authenticate a multicast user. The default configuration is no-auth.

   NOTE

   After configuring multicast user authentication, you need to enable the global authentication switch to make the configuration take effect. By default, the global switch of multicast user authentication is enabled. You can run the **igmp proxy authorization** command to change the configuration.

2. Bind the multicast user to a global profile. The multicast user is bound to an authority profile to implement user authentication.

Run the **igmp user bind-profile** command to bind the user to an authority profile. After the binding, the multicast user uses the authority of the programs configured in the bound profile.

Step 4 Bind the multicast user to a multicast VLAN.

In the multicast VLAN mode, run the **igmp multicast-vlan member** command to bind the user to the multicast VLAN. Then, the user becomes a multicast member of the multicast VLAN and can order programs configured for the multicast VLAN.

Step 5 Run the **display igmp user** command to check whether the related information about the multicast user is correct.

----End

Example

To add multicast user (port) 0/2/1 to multicast VLAN 101, enable user authentication, enable log report, set the maximum bandwidth to 10 Mbit/s,, set IGMP version of the multicast user to v3-forced, and bind the user to right profile **music**, do as follows:

```
huawei(config)#service-port 100 vlan 101 gpon 0/2/1 ont 0 gemport 1 rx-cttr 2 tx-
cttr 2
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 100 auth log enable max-bandwidth
10240 v3-forced
huawei(config-btv)#igmp user bind-profile service-port 100 profile-name music
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
```

9.6 (Optional) Configuring the Multicast Bandwidth

To limit the multicast bandwidth of a user, you can enable multicast bandwidth management, that is, connection admission control (CAC), and then control the bandwidth of a multicast user by setting the program bandwidth and the user bandwidth.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

If the CAC function (not the dynamic ANCP CAC function) is enabled and a user demands a multicast program, the system compares the remaining bandwidth of the user (bandwidth configured for the user - total bandwidth of the online programs of the user) with the bandwidth of the multicast program. If the remaining bandwidth of the user is sufficient, the system adds the user to the multicast group. If the bandwidth is insufficient, the system does not respond to the request of the user.

If the CAC function is disabled, the system does not guarantee the bandwidth of the multicast program. When the bandwidth is not guaranteed, problems such as mosaic and delay occur in the multicast program.

Table 9-6 lists the default settings of the CAC parameters.

Table 9-6 Default settings of the CAC parameters

Parameter	Default Setting
Global CAC switch	enable
Bandwidth of the multicast program	5000 kbit/s
Bandwidth of the multicast user	no-limit
Bandwidth of the GPON port	716800 kbit/s

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Enable the global CAC switch.

By default, the global CAC switch is already enabled. You can run the **igmp bandwidthCAC** { **enable** | **disable** } command to change the setting.

Step 3 Configure the bandwidth of the multicast program.

- Run the **igmp program add ip** *ip-addr* **bandwidth** command to configure the bandwidth of a single multicast program. The program bandwidth is an attribute of a multicast program, specifying the bandwidth requirement of the program being played.
- Run the **igmp bandwidth port** *frameid/slotid/portid* **max-bandwidth**{ *bandwidth* | **no-limit** } command to configure the program bandwidth of a physical port on a board. This command is available for only the GPON port. The default bandwidth of a port is 716800 kbit/s. Configuring the total program bandwidth for a single port is a way of traffic management, which helps avoid network congestion caused by the excessively-large total program bandwidth on a port. When the total program bandwidth of a port exceeds the value configured using the **igmp bandwidth port** *frameid/slotid/portid* **max-bandwidth**{ *bandwidth* | **no-limit** } command, subsequent programs ordered by users on this port cannot be played.

Step 4 Configure the bandwidth of the multicast user.

Run the **igmp user add service-port** *index* **max-bandwidth** command to allocate the bandwidth that is available to the multicast user.

Step 5 Check whether the multicast bandwidth configuration is correct.

- Run the **display igmp config global** command to check the status of the global CAC switch.
- Run the **display igmp program** command to query the bandwidth allocated to the multicast program.
- Run the **display igmp user** command to query the maximum bandwidth and the occupied bandwidth of the multicast user.

----End

Example

To enable bandwidth management for multicast users, set the user bandwidth to 10 Mbit/s when adding multicast user 0/2/1, and configure the program bandwidth to 1 Mbit/s when adding multicast program 224.1.1.1.

```
huawei(config)#btv
huawei(config-btv)#igmp bandwidthcAC enable
huawei(config-btv)#igmp user add port 0/2/1 max-bandwidth 10240
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 bandwidth 1024
```

9.7 (Optional) Configuring Multicast Preview

Multicast preview is an advertising method provided by carriers for ISPs. The purpose is to allow users to have an overview of a program in a controlled way. In other words, the duration, interval, and count of the user previews are controlled.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

The difference between program preview and normal program watching is that, after the user goes online, the duration of the preview is restricted. When the duration expires, the user goes offline. The user can request the program again only after the preview interval expires. The count by which the user can request the program within a day (the start time can be configured) is restricted by the preview count of the user.

Multicast preview parameters are managed through the preview profile. One program can be bound to only one preview profile, but one preview profile can be referenced by multiple programs.

Table 9-7 lists the default settings of the multicast preview parameters.

Table 9-7 Default settings of the multicast preview parameters

Parameter	Default Value
Global multicast preview function	enable
Preview profile	Preview profile with index 0
Preview profile parameters	Maximum preview duration: 120s Maximum preview count: 8 Minimum interval between two previews: 120s
Time for resetting the preview record	4:00:00 am
Valid duration of multicast preview	30s

NOTE

The IPv6 multicast does not support the multicast preview function.

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Enable the global multicast preview function.

By default, the global multicast preview function is enabled. You can run the **igmp preview**{ **enable** | **disable** } command to change the setting.

Step 3 Configure the preview profile.

Run the **igmp preview-profile add** command to configure the preview profile, and set the parameters: maximum preview duration, maximum preview count, and minimum interval between two previews. The system has a default preview profile with index 0.

Step 4 Bind the program to the preview profile.

In the multicast VLAN mode, run the **igmp program add ip** *ip-addr* **preview-profile** *index* command to bind the program to be previewed to the preview profile so that the program has the preview attributes as defined in the preview profile. By default, the program is bound to the preview profile with index 0.

Step 5 Change the time for resetting the preview record.

Run the **igmp preview auto-reset-time** command to change the time for resetting the preview record. The preview record of the user remains valid within one day. On the second day, the preview record is reset. By default, the system resets the preview record at 4:00:00 a.m.

Step 6 Modify the valid duration of multicast preview.

Run the **igmp proxy recognition-time** or **igmp preview recognition-time** command to modify the valid duration of multicast preview. If the actual preview duration of the user is shorter than the valid duration, the preview is not regarded as a valid one and is not added to the preview count. By default, the valid duration of multicast preview is 30s.

NOTE

If you use **igmp proxy recognition-time** and **igmp preview recognition-time** commands to set the valid duration of multicast preview concurrently, the one set by **igmp preview recognition-time** takes effect.

Step 7 Run the **display igmp config global** command to check whether the values of the multicast preview parameters are correct.

----End

Example

To enable preview of multicast programs by using the system default preview profile, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp preview enable
```

To enable preview of multicast programs, create preview profile 1, set the maximum preview time to 150s, the maximum preview count to 10, and apply this preview profile when adding program 224.1.1.1, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp preview enable
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 10
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 preview-profile 1
```

9.8 (Optional) Configuring Program Prejoin

The channel change request sent by a user needs to be processed by different intermediate devices on the network, which brings a channel change delay. Program prejoin is able to shorten the channel change delay, improving user experience.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

Multicast program prejoin is the same as program request. The MA5600T/MA5603T plays the role of a user and sends the report packet for receiving in advance the multicast stream from the upper-layer multicast router to the upstream port.

After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, the unsolicited report function needs to be enabled so that the user can request the program quickly. Generally, the upper-layer multicast router processes the user request by responding to the group-specific query and the general query.

Table 9-8 lists the default settings of the prejoin parameters.

Table 9-8 Default settings of the prejoin parameters

Parameter	Default Value
Prejoin function	disable
Unsolicited report of IGMP packets	disable

Procedure

Step 1 Enable the prejoin function.

Run the **igmp program add ip** *ip-addr* **prejoin enable** command to enable the prejoin function of a program. By default, the prejoin function is disabled.

Step 2 After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, the unsolicited report function needs to be enabled for IGMP packets.

- Run the **igmp program add ip** *ip-addr* **unsolicited enable** command to enable the unsolicited report function for IGMP packets. By default, the unsolicited report function is disabled.
- Run the **igmp unsolicited-report interval** command to modify the interval for unsolicitedly reporting IGMP packets. By default, the interval is 10s.

Step 3 Check whether the prejoin function is configured correctly.

- Run the **display igmp program** command to query the status of the prejoin function and the unsolicited report function.
- Run the **display igmp config vlan** command to query the interval for unsolicitedly reporting IGMP packets.

----End

Example

Assume that the MVLAN ID is 101. To configure the IPv4 multicast and enable the prejoin function of multicast program 224.1.1.1 to reduce the waiting time for ordering this program, do as follows:

```
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 prejoin enable
```

Assume that the MVLAN ID is 101. To configure the IPv6 multicast and enable the prejoin function of multicast program ffff::1 to reduce the waiting time for ordering this program, do as follows:

```
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ipv6 ffff::1 prejoin enable
```

9.9 (Optional) Configuring the Multicast Logging Function

Multicast log serves as a criterion for carriers to evaluate the viewership of multicast programs.

Prerequisites

If the syslog is used for reporting multicast logs, the syslog server must be properly configured.

If the syslog server is not configured, you can run the **igmp syslog disable** command to disable the multicast syslog reporting function to save system resources.

Context

Multicast logs have three control levels: multicast VLAN level, multicast user level, and multicast program level. The system generates logs only when the logging functions at the three levels are enabled.

When the user stays online for longer than the valid time for generating logs, the system generates logs in any of the following conditions:

- The user goes offline naturally, by force, or abnormally.
- The user is blocked or deleted.
- The program is deleted.
- The program priority is changed.
- The upstream port to which the program is bound changes.
- The VLAN of the upstream port to which the program is bound changes.
- The right mode is switched.
- The user preview times out.
- The IGMP mode is switched.

- The bandwidth CAC is not passed.

The system supports up to 10K logs. When the user goes online, the system records only the online date and time. The system generates a complete log only when the user goes offline.

The MA5600T/MA5603T can report the multicast log to the log server in the syslog mode and the call detailed record (CDR) mode. By default, the MA5600T/MA5603T reports the log in the syslog mode.

- Syslog mode: Logs are reported to the syslog server in the form of a single log.
- CDR mode: Logs are reported to the log server in the form of a log file (.cvs). One log file contains multiple logs.

Table 9-9 lists the default settings of the multicast logging parameters.

Table 9-9 Default settings of the multicast logging parameters

Parameter	Default Value
Report mode of the multicast log	Syslog mode
Logging function at the multicast VLAN level	enable
Logging function at the multicast user level	enable
Logging function at the multicast program level	enable
Action report function of the multicast user	disable
Interval for automatically logging	2 hours
Minimum online duration for generating a valid log	30s
Parameters of the log report in the CDR mode	Report interval: 600s Maximum number of logs that can be reported each time: 200

Procedure

- Configure the parameters of the logging function of the multicast host.
  1. Enable the multicast logging functions.

     Multicast logs have three control levels: multicast VLAN level, multicast user level, and multicast program level. The system generates logs only when the logging functions at the three levels are enabled. By default, the three functions are enabled.

     - In the BTV mode, run the **igmp log** { **enable** | **disable** } command to configure the logging function at the multicast VLAN level.

   - In the BTV mode, run the **igmp user add service-port** *index* **log** { **enable** | **disable** } command to configure the logging function at the multicast user level.

     In the BTV mode, run the **igmp log record** { **user** | **mac** } command to configure the log record object. After the configuration, the device can record ordering action of users or multicast terminals identified by MAC addresses.
   - In the Multicast VLAN mode, run the **igmp program add ip** *ip-addr* **log** { **enable** | **disable** } command to configure the logging function at the multicast program level.

2. Modify the interval for automatically logging.

   In the BTV mode, run the **igmp proxy log-interval** command to modify the interval for automatically logging. When the user stays online for a long time, the system generates logs at the preset interval. This is to prevent the problem that a log is not generated when the user leaves the multicast group without sending a leave packet, which can affect the accounting. By default, the interval is two hours.

3. Modify the minimum online duration for generating a valid log.

   In the BTV mode, run the **igmp proxy recognition-time** or **igmp log recognition-time** command to modify the minimum online duration for generating a valid log. If the user is in a multicast group (such as to preview a program) for shorter than the preset duration, the user operation is not regarded as a valid one and a log is not generated. A log is generated only when a user stays online for longer than the specified duration. By default, the minimum online duration is 30s.

   NOTE

   If you use **igmp proxy recognition-time** and **igmp log recognition-time** commands to set the minimum online duration for generating a valid log concurrently, the one set by the **igmp log recognition-time** command takes effect.

- (Optional) Configure the action report function of the multicast user.

  By default, the system uses the syslog mode to report multicast logs. You can run the **igmp user-action-report** command to configure the action report function of the multicast user. By default, the action report function of the multicast user is disabled.

  - **enable**: Enables the action report function of the multicast user. Logs are reported to the syslog server when a multicast user goes online and offline.
  - **disable**: Disables the action report function of the multicast user. Logs are reported to the syslog server only when a multicast user goes offline.

- Configure the function of CDR-mode log report.

  1. Configure the multicast log server and the data transmission mode for the CDR-mode log report.

     Run the **file-server auto-backup cdr** command to configure the active and standby multicast log servers.

  2. Enable the function of CDR-mode log report.

     In the BTV mode, run the **igmp cdr** { **enable** | **disable** } command to configure the function of CDR-mode log report. After the function is enabled, the MA5600T/MA5603T reports the local multicast logs to the multicast log server in the form of a file. After the function is disabled, the MA5600T/MA5603T reports each single log to the syslog server in the default syslog mode.

  3. Configure the parameters of the log report in the CDR mode.

   - In the BTV mode, run the **igmp cdr-interval** command to set the report interval. By default, the interval is 600s.
   - In the BTV mode, run the **igmp cdr-number** command to set the maximum number of logs that can be reported each time. When the number of the multicast logs in the CDR file reaches the preset value, the MA5600T/MA5603T reports the logs. By default, the maximum number is 200.
4. Check whether the configuration is correct.
   - Run the **display file-server** command to query the configuration of the CDR multicast log server.
   - Run the **display igmp config global** command to query the status and other parameters of the function of CDR-mode log report.

----End

Example

To configure the multicast log to be reported to log server 10.10.10.1 in the CDR mode, and use the TFTP transmission mode, do as follows:

```
huawei(config)#file-server auto-backup cdr primary 10.10.10.1 tftp
huawei(config)#btv
huawei(config-btv)#igmp cdr enable
```

9.10 (Optional) Configuring the Maximum Number of Programs That Can Be Watched by the Multicast User

This topic describes how to configure the maximum number of programs that can be ordered by the multicast user at the same time. You can configure the maximum number of all programs that can be watched by the multicast user at the same time, or configure the maximum number of the different-level programs that can be watched by the multicast user.

Prerequisites

When you configure the maximum number of programs based on the program level, the program level must be configured at the same time and the programs must be configured statically.

Context

During automatic program generation, the number of the programs generated based on the same IGMP join request varies with the group filter mode. When the group filter mode of an MVLAN is configured to **asm-only** or **asm-ssm**, only one program with the unique multicast IP address is generated in the MVLAN. The [*, G] multicast forwarding table is used for this MVLAN instance on the forwarding plane. When the group filter mode of an MLVAN is configured to **ssm-only**, multiple programs with the same multicast IP addresses but different source IP addresses can be generated in the MVLAN. The [S, G] multicast forwarding table is used for this VLAN instance on the forwarding plane. The maximum number of programs is calculated according to the number of actually-generated programs. For example, when a multicast user joins an MVLAN with the multicast filter mode **asm-ssm** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates only one multicast program with the multicast IP address G1 for the multicast user; when a multicast user joins an MVLAN with the multicast filter mode **ssm-only** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates two multicast programs with IP addresses [S1, G1] and [S2, G1].

ASM Message

IGMP v2 message type:

- Join
- Leave

IGMP v3 message type:

- TO_IN({})
- IS_IN({})
- TO_EX({})
- IS_EX({})

Table 9-10 lists the actions of the ASM messages in different group filter modes.

Table 9-10 Actions of the ASM messages in different group filter modes

asm-only	ssm-only	asm-ssm
The system processes the [*, G] messages. The multicast packets are forwarded only according to the multicast IP addresses.	The system does not process the [*, G] messages.	The system processes the [*, G] messages. If there is no program with its multicast IP address identical to that carried in the message, the system generates a program without a source IP address according to the MVLAN and multicast IP address. If there is a program with the MVLAN, multicast IP address (identical to the multicast IP address of the message), and source IP address, the system does not generate a new program and users directly join this program. The multicast packets are forwarded only according to the multicast IP addresses.

SSM message

IGMP v2 message type:NA

IGMP v3 message type:

- ALLOW(S,G)
- BLOCK(S,G)

- TO_IN(S,G)
- IS_IN(S,G)

Table 9-11 lists the actions of the ASM and SSM messages in different group filter modes.

Table 9-11 Actions of the SSM messages in different group filter modes

asm-only	ssm-only	asm-ssm
The system does not process the [S, G] messages.	If messages with [S1, G1] and [S2, G2] are received, two programs with [S1, G1] and [S2, G2] are generated. The multicast packets are forwarded according to the multicast IP address and source IP address.	The system processes the [S, G] messages. If there is no program with its multicast IP address identical to that carried in the message in an MVLAN, the system generates the program with source IP address according to the VLAN, and multicast IP address and source IP address. If there is a program with the VLAN, multicast IP address (identical to the multicast IP address of the message), and source IP address (different from the source IP address of the message), the system does not process user's ordering requests. If there is a program without a source IP address but with the VLAN, and multicast IP address (identical to the multicast IP address of the message), the system does not generate a new program and users directly join this program. The multicast packets are forwarded only according to the multicast IP addresses.

Table 9-12 lists the default settings of the max-program parameters.

Table 9-12 Default settings of the multicast max-program parameters

Parameter	Default Value
Maximum number of programs that can be watched by the multicast user	8

Parameter	Default Value
Grade of the multicast program	no-grade
Maximum number of programs of different priorities that can be watched by the multicast user	no-limit

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Configure the max-program of the multicast user.

Run the **igmp user add service-port** ***index*** **max-program** ***max-program-num*** command to set the maximum number of programs that can be watched by the multicast user.

Step 3 Configure the maximum number of programs of different priorities that can be watched by the multicast user.

Run the **igmp user watch-limit service-port** ***index*** command to set the maximum number of programs of different priorities that can be watched by the multicast user.

Step 4 Configure the grade of the multicast program.

In the multicast VLAN mode, run the **igmp program add ip** ***ip-addr*** **grade**command to configure the grade of a multicast program.

Step 5 Check whether the multicast max-program configuration is correct.

- Run the **display igmp user** command to query the maximum number of programs that can be watched and watching by the multicast user.
- Run the **display igmp program** command to query the grade of the multicast program.
- Run the **display igmp user extended-attributes** command to query the maximum number of programs that can be watched and watching by the multicast user.

----End

Example

To set the user max-program to 10 when adding multicast service-port 0, set the user can watch 2 HDTV program, and configure the program grade to hdtv when adding multicast program 224.1.1.1, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 0 max-program 10
huawei(config-btv)#igmp user watch-limit service-port 0 hdtv 2
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-multicast-vlan 101)#igmp program add ip 224.1.1.1 grade hdtv
```

9.11 (Optional) Configuring the Maximum Rate for Sending IGMP Packets

When the multicast and anti-DoS attack functions are enabled, the system reports DoS attack alarms and drops IGMP packets over the rate limit, if a user port sends such IGMP packets to the CPU. When the anti-DoS attack function is disabled, the system always sends IGMP packets to the CPU. If they are sent to the CPU at a rate higher than the limit, the system drops the IGMP packets that exceed the rate limit but does not report DoS attack alarms.

Prerequisites

The multicast function is enabled.

Context

When the multicast function is enabled, the system will always send the received IGMP packets to the CPU if no control is implemented over the process. Then if a user port receives a large number of IGMP packets, the IGMP packets for other users will not be processed and directly dropped instead.

Table 9-13 lists the default system settings.

Table 9-13 Default system settings

Parameter	Default Value
Anti-DoS attack function	disable
Maximum rate for sending IGMP packets to the CPU	63 pps

Procedure

Step 1 Enable the anti-DoS attack function.

Run the **security anti-dos** { **enable** | **disable** } command to enable the anti-DoS attack function, which is disabled by default.

Step 2 Specify the maximum rate for sending IGMP packets to the CPU.

Run the **security anti-dos control-packet igmp rate** *frameid/slotid/portid* { **value** | **no-limit** } command to specify the maximum rate for sending IGMP packets to the CPU, which is 63 by default.

----End

Example

Example: Specify the maximum rate for sending IGMP packets to the CPU to 63 pps for user port 0/1/1, and enable the system to report the port to the blacklist if it sends IGMP packets over the rate limit to the CPU.

```
huawei(config)#security anti-dos enable
huawei(config)#security anti-dos control-packet igmp rate 0/1/1 20
```

10 Configuring the Voice Service

About This Chapter

The MA5600T/MA5603T supports user access through copper cables to provide the voice service.

Context

The MA5600T/MA5603T can provide the voice service through the following protocols:

- The system communicates with the MGC through MGCP, and the voice service is provided under the control of the MGC.
- The system communicates with the MGC through H.248, and the voice service is provided under the control of the MGC.
- The system communicates with the IMS core network device through SIP to provide the voice service.

The MA5600T/MA5603T supports the configuration of the following services:

- VoIP service

  Supports the voice over IP service through MGCP, H.248, or SIP.
- VoIP ISDN service

  Supports the ISDN over IP service through H.248.
- FoIP service

  Supports the fax over IP service through MGCP, H.248, or SIP.
- MoIP service

  Supports the modem over IP service through MGCP, H.248, or SIP.

To ensure the normal voice service, the MA5600T/MA5603T supports the following security and reliability configurations:

- Device authentication

  Supports authentication of the MG interface through MGCP or H.248 and authentication of the SIP interface through SIP.
- Emergency standalone

Supports emergency standalone of the MG interface through H.248.

- Dual homing

  Supports dual homing from the MG to the MGC through MGCP or H.248 and authentication from the SIP AG to the SIP proxy server.

NOTE

- In this document, the MG, AG, gateway, or SIP AG refers to the MA5600T/MA5603T, unless otherwise stated.
- The VoIP service on MA5600T/MA5603T supports only the SCU upstream transmission or GIU upstream transmission.

10.1 Configuring the VoIP Service (H.248-based or MGCP-based)

This topic describes how to configure the VoIP service when the protocol adopted by the MA5600T/MA5603T is H.248 or MGCP.

Application Context

The voice over IP (VoIP) service uses the IP packet switched network for transmission after the traditional analog voice signals are compressed and packetized, to lower the cost of the voice service.

In the NGN network, the MA5600T/MA5603T functions as an access gateway (AG) and exchanges signaling with the media gateway controller (MGC) through the MG control protocol (mainly H.248 and MGCP). In this way, the VoIP, FoIP, and MoIP services are implemented under the control of the MGC. The MG interface, as an interface for the communication between the MA5600T/MA5603T (AG) and the MGC, plays a decisive role in the H.248-based or MGCP-based VoIP service. Therefore, to implement the VoIP service, the MG interface must be configured and must be in the normal state.

H.248, also called MeGaCo, is a protocol developed based on MGCP by combining the features of other media gateway control protocols. Compared with MGCP, H.248 supports more types of access technologies and supports mobility of terminals; however, the configuration of the H.248-based VoIP service is the same as that of the MGCP-based VoIP service.

Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T to the MGC must be configured to ensure that the MA5600T/MA5603T and the MGC are reachable from each other.
- The voice daughter board on the control board works in the normal state.
- Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported) If the SCUB control board is used. For details about how to configure the electronic switch, see **electro-switch**.

Precautions

The MG control protocols (H.248 and MGCP) are master/slave protocols, and the MGC controls the AG to implement the call connection. Therefore, the data on the AG for interconnection with the MGC, including the attributes of the MG interface and the attributes of the VoIP user, must be the same as the corresponding data on the MGC. Before configuring the VoIP service, you must make the data plan by considering interconnection with the MGC.

Data Plan

Table 10-1 provides the data plan for configuring the VoIP service.

Table 10-1 Data plan for configuring the H.248-based or MGCP-based VoIP service

Item			Remarks
MG interface data (The data configuration must the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	It is used as the upstream VLAN of the VoIP service to be configured. Standard VLAN is recommended.
		Media and signaling upstream port	It is used as the upstream port of the VoIP service to be configured.
		Media and signaling IP addresses	These IP addresses must be selected from the media and signaling IP address pools. The media and signaling IP address pools consists of all the IP addresses of the Layer 3 interface of the media and signaling upstream VLAN. **CAUTION** The MGCP interface on the MA5600T/MA5603T does not support the isolation of media streams and signaling flows. Therefore, when the MGCP protocol is used, the media IP address pool and the signaling IP address pool must be the same. When the H.248 or SIP protocol is used, the media IP address pool and the signaling IP address pool can be the same or different.
		Default IP address of the MG	It is the next hop IP address from the MA5600T/MA5603T to the MGC.
	Parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	It is the MG interface ID used for the VoIP service to be configured, which determines the virtual access gateway (VAG) specified for the user.
		Signaling port ID of the MG interface	It is the transport layer protocol port ID used for the signaling exchange between the MA5600T/MA5603T (AG) and the MGC. ● Default signaling port ID defined in H.248: 2944 (text) and 2945 (binary) ● Default signaling port ID defined in MGCP: 2727
		IP address of the primary MGC to which the MG interface belongs	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 also need to be configured.
		Port ID of the primary MGC to which the MG interface belongs	

Item			Remarks
		Coding mode of the MG interface	Currently, the **text** coding mode is supported. NOTE For the MG interface that supports MGCP, the default coding mode is the **text** coding mode. This parameter can be queried, but cannot be configured.
		Transmission mode of the MG interface	The transmission mode is selected according to the requirements on the MGC side. Generally, UDP is adopted. NOTE For the MG interface that supports MGCP, the default transmission mode is UDP. This parameter can be queried, but cannot be configured.
		Domain name of the MG interface	It corresponds to the parameter **domainName** of the MG interface. ● When the MGCP protocol is used, this parameter must be configured. Otherwise, the MG interface fails to be enabled. ● When the H.248 protocol is used, this parameter must be configured if the parameter **MIDType** of the H.248 message is configured as the domain name. Otherwise, the MG interface fails to be enabled. In other situations, this parameter is optional.
		Profile index of the MG interface	If the MGC interconnected with the MG is also made by Huawei, set the profile index to 1 or do not set it (it is 1 by default); if the MGC interconnected with the MG is made by another manufacturer, set the profile index to the corresponding value of the manufacturer.

Item			Remarks
		Device name of the MG interface	It is supported by the H.248 protocol, and corresponds to the parameter **deviceName** of the MG interface that uses the H.248 protocol. When the H.248 protocol is used, this parameter must be configured if the parameter **MIDType** of the H.248 message is configured as the domain name. Otherwise, the MG interface fails to be enabled. In other situations, this parameter is optional.
	Digitmap of the MG interface		The digitmaps here are used for certain special applications such as emergency calls and emergency standalone. The digitmaps for common phone services are issued to the AG by the MGC, and therefore such digitmaps do not need to be configured on the AG. If the services such as emergency calls and emergency standalone are not required, the digitmaps do not need to be configured.
	Software parameters of the MG interface		According to the service requirements, the configuration of software parameters determines whether the MG interface supports the functions such as dual homing and emergency standalone.
	Ringing mode of the MG interface		According to the service requirements, the ringing modes of the MG interface need to be determined.
	Terminal ID (TID) format of the MG interface		The TID format determines the generation mode of various types of user terminals on an MG interface.
Voice user data (The data configuration must be the same as the data configuration on the MGC.)	Slot of the voice service board		-
	User data	Phone number	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.
		TID	If the TID template with which the PSTN user is bound does not support terminal layering, this parameter needs to be configured.

Item			Remarks
		User priority	According to the service requirements, user priority needs to be specified. The user priority includes the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)
		User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
	System parameters		The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	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 do not need to be modified if there is no special requirement.
	Ringing current attributes		You can adjust the ringing tone volume by modifying the attributes of the ringing current. In general, the attributes of the ringing current do not need to be modified. You need to modify the parameters of the ringing current attributes according to the local standards only when the default ringing current attributes do not meet the local standards.

Procedure

10.1.1 Configuring an MG Interface

This topic describes how to configure an MG interface for implementing the communication between the MA5600T/MA5603T (AG) and the MGC.

Context

- The MA5600T/MA5603T communicates with the MGC through either the H.248 or the MGCP protocol. One MA5600T/MA5603T can run only one protocol.
- One MA5600T/MA5603T supports up to eight MG interfaces. Each MG interface can be configured with the attributes (such as authentication and ringing mapping) independently.

Procedure

Configuring the Upstream VLAN Interface

This topic describes how to specify the upstream VLAN interface for the media stream and the signaling flow, and how to configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the media and signaling IP address pools.

Context

Multiple IP addresses can be configured for the same VLAN Layer 3 interface. Only one IP address functions as the primary address, and other IP addresses function as the secondary addresses.

Procedure

Step 1 Run the **vlan** command to add an upstream VLAN for the media stream and the signaling flow.

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

Step 3 Configure the IP addresses of the VLAN Layer 3 interface.

1. Run the **interface vlanif** command to enter the Layer 3 interface of the upstream VLAN for the media stream and the signaling flow.
2. Run the **ip address** command to configure the IP addresses of the Layer 3 interface.

Step 4 Run the **display interface vlanif** command to check whether the IP addresses of the Layer 3 interface are the same as those in the data plan.

----End

Example

Assume that the media stream and the signaling stream are transmitted upstream through upstream port 0/19/0. To create media and signaling upstream VLAN 3 and configure IP addresses 10.13.4.116/16 and 10.13.4.117/16 of the Layer 3 interfaces for the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#vlan 3 standard
huawei(config)#port vlan 3 0/19 0
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 10.13.4.116 16
huawei(config-if-vlanif3)#ip address 10.13.4.117 16 sub
huawei(config-if-vlanif3)#quit
huawei(config)#display interface vlanif 3
vlanif3 current state : UP
Line protocol current state : UP
Description : HUAWEI, SmartAX Series, vlanif3 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is 10.13.4.116/16
Internet Address is 10.13.4.117/16 Secondary
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc32-1118
```

Configuring the Media and Signaling IP Address Pools

The media IP address pool defines all media IP addresses that can be used by the AG, and the signaling IP address pool defines all signaling IP addresses that can be used by the AG.

Prerequisites

The IP address of the Layer 3 interface of the media and signaling upstream VLAN must be configured. For details about how to configure the IP address, see **Configuring the Upstream VLAN Interface**.

Context

- The media IP address and the signaling IP address for the MG interface must be selected from the IP address pools configured here.
- The signaling IP address pool is used to store the IP addresses of the MG interfaces, and the media IP address pool is used to store the IP addresses of the media streams controlled by the signaling.
- The media IP address pool and the signaling IP address pool can be the same. Similarly, the media IP address and the signaling IP address can be the same.

⚠ **CAUTION**

The MGCP interface on the MA5600T/MA5603T does not support the isolation of media streams and signaling flows. Therefore, when the MGCP protocol is used, the media IP address pool and the signaling IP address pool must be the same. When the H.248 or SIP protocol is used, the media IP address pool and the signaling IP address pool can be the same or different.

Procedure

Step 1 Run the **voip** command to enter the VoIP mode.

Step 2 Configure the media IP address pool.

1. Run the **ip address media** command to add the media IP address to the media IP address pool.

The media IP address needs to be selected from the IP addresses of the Layer 3 interface of the media and signaling upstream VLAN.

2. Run the **display ip address media** command to check whether the media IP address pool is the same as that in the data plan.

Step 3 Configure the signaling IP address pool.

1. Run the **ip address signaling** command to add the signaling IP address to the signaling IP address pool.

   The signaling IP address needs to be selected from the IP addresses of the Layer 3 interface of the media and signaling upstream VLAN.

2. Run the **display ip address signaling** command to check whether the signaling IP address pool is the same as that in the data plan.

----End

Example

To add IP addresses 10.13.4.116/16 and 10.13.4.117/16 of Layer 3 interfaces of the media and signaling upstream VLAN to the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.13.4.116 10.13.0.1
huawei(config-voip)#ip address media 10.13.4.117 10.13.0.1
huawei(config-voip)#ip address signaling 10.13.4.116
huawei(config-voip)#ip address signaling 10.13.4.117
huawei(config-voip)#display ip address media
  Media:
  IP Address...........: 10.13.4.116
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.0.1
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.0.1
  MAC Address..........: 00-E0-FC-AF-91-33
huawei(config-voip)#display ip address signaling
  Signaling:
  IP Address...........: 10.13.4.116
  Subnet Mask..........: 255.255.0.0
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  MAC Address..........: 00-E0-FC-AF-91-33
```

Adding an MG Interface

This topic describes how to add an MG interface, through which the MA5600T/MA5603T can communicate with the MGC.

Context

- One MA5600T/MA5603T supports up to eight MG interfaces. Each MG interface can be configured with the interface attributes independently.
- The configuration of the attributes of an MG interface is valid only to the MG interface.

Procedure

- Add an MG interface that supports H.248.
  1. Run the **display protocol support** command to query the current system protocol.
     - If the current system protocol is H.248, go to **Step 8**.
     - If the current system protocol is MGCP, proceed to **Step 2**.
  2. Run the **display if-mgcp all** command to query whether an MG interface that supports MGCP exists.
     - If such an MG interface does not exist, go to **Step 5**.
     - If such an MG interface exists, proceed to **Step 3**.
  3. Delete all user data of this MG interface, and then run the **shutdown(mgcp)** command to disable the MG interface.

     CAUTION

     This operation directly interrupts all the services on the MG interface. Hence, exercise caution when performing this operation.
  4. Run the **undo interface mgcp** command to delete the MG interface.
  5. Run the **protocol support** command to change the system protocol to H.248.
  6. Run the **save** command to save the configuration data, and then run the **reboot system** command to restart the system to make the new configuration data take effect.
  7. After the system is restarted, log in to the system, and enter the global config mode.
  8. Run the **interface h248** command to add an MG interface that supports H.248.
  9. Run the **if-h248 attribute** command to configure the attributes of the MG interface according to the data plan.
  10. Run the **display if-h248 attribute** command to check whether the attributes of the MG interface are the same as those in the data plan.
- Add an MG interface that supports MGCP.
  1. Run the **display protocol support** command to query the current system protocol.
     - If the current system protocol is MGCP, go to **Step 8**.
     - If the current system protocol is H.248, proceed to **Step 2**.
  2. Run the **display if-h248 all** command to query whether an MG interface that supports H.248 exists.
     - If such an MG interface does not exist, go to **Step 5**.
     - If such an MG interface exists, proceed to **Step 3**.
  3. Delete all user data of this MG interface, and then run the **shutdown(h248)** command to disable the MG interface.

WARNING

This operation directly interrupts all the services on the MG interface. Hence, exercise caution when performing this operation.

4. Run the **undo interface h248** command to delete the MG interface.
5. Run the **protocol support** command to change the system protocol to MGCP.
6. Run the **save** command to save the configuration data, and then run the **reboot system** command to restart the system to make the new configuration data take effect.
7. After the system is restarted, log in to the system, and enter the global config mode.
8. Run the **interface mgcp** command to add an MG interface that supports MGCP.
9. Run the **if-mgcp attribute** command to configure the attributes of the MG interface according to the data plan.
10. Run the **display if-mgcp attribute** command to check whether the attributes of the MG interface are the same as those in the data plan.

----End

Example

Assume that the MG interface ID is 0 and the H.248 protocol is used for interconnecting with the MGC. To add the MG interface, do as follows:

```
huawei(config)#display protocol support
System support H248 protocol
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Assume that the MG interface ID is 0 and the MGCP protocol is used for interconnecting with the MGC. The current system protocol, however, is the H.248 protocol. It is confirmed that the H.248 interface exists in the system but is not in use. To add MG interface 0, do as follows:

```
huawei(config)#display protocol support
System support H248 protocol
huawei(config)#display if-h248 all
  ----------------------------------------------------------------------------
  MGID     TransMode State     MGPort MGIP            MGCPort MGCIP/DomainName
  ----------------------------------------------------------------------------
  0        -         Close     -      -               -       -
  ----------------------------------------------------------------------------
huawei(config)#undo interface h248 0
  Are you sure to del MG interface?(y/n)[n]:y
huawei(config)#protocol support mgcp
huawei(config)#save
huawei(config)#reboot system
  Please check whether data has saved, the unsaved data will lose if reboot
system, are you sure to reboot system? (y/n)[n]:y
```

After the system is restarted, re-log in to the system.

```
huawei(config)#display protocol support
System support MGCP protocol
huawei(config)#interface mgcp 0
  Are you sure to add MG interface?(y/n)[n]:y
```

(Optional) Configuring the Digitmap of an MG Interface

This topic describes how to configure the digitmaps for certain special applications such as emergency calls and emergency standalone. The digitmaps for common phone services are issued to the AG by the MGC, and therefore such digitmaps do not need to be configured on the AG. If the services such as emergency calls and emergency standalone are not required, the digitmaps do not need to be configured.

Prerequisites

⚠ **CAUTION**

The digitmap configuration is relatively complicated. The information such as the meanings and usage of the characters in a digitmap is defined in the protocol, and is not described here. This topic provides only some basic information. It is recommended that you refer to the digitmap description in ITU-T H248.1 (applicable to H.248) or RFC 3435 (applicable to MGCP) before configuring the digitmap.

Context

- A digitmap is a set of digit collection descriptors. It is a dialing scheme resident in the MG and is used for detecting and reporting digit events received on a termination. The digitmap is used to improve the efficiency of the MG in sending the callee number. That is, if the callee number matches a dialing scheme defined by the digitmap, the MG sends the callee number collectively in a message.
- A digitmap consists of strings of digits with certain meanings. When the received dialing sequence matches one of the strings, the digits are collected completely.
- To configure the emergency standalone function, you must configure the internal digitmap.

The H.248-based MG interface supports the following types of digitmaps:

- Internal digitmap
- Emergency digitmap
- Emergency call digitmap (due to call restriction in case of an overload)
- Automatic redial digitmap of the card service

Table 10-2 provides the valid characters in the strings and their meanings in the H.248 protocol. For details about the digitmap in the H.248 protocol, refer to ITU-T H248.1, which provides a better guide to the digitmap configuration.

Table 10-2 Digitmap format in the H.248 protocol

Digit or Character	Description
0-9	Indicate dialed digits 0-9.
A-D	-
E	Indicates * in the DTMF mode.
F	Indicates for # in the DTMF mode.
X	Indicates for a wildcard, indicating any digit from 0 to 9.

Digit or Character	Description
S	Indicates the short timer. When detecting the timer timeout, the system reports a phone number digit by digit if the phone number is detected after the dialing scheme is matched.
L	Indicates the long timer. When detecting the timer timeout, the system reports a phone number digit by digit if the phone number is detected after the dialing scheme is matched.
Z	Indicates the duration modifier, which indicates a dialing event of a long duration. It is before the event character with a fixed location. When the event duration exceeds the threshold, the dialing event fills the location.
.	Indicates that there can be multiple digits (including 0) or characters before it.
|	Used to separate the strings and indicates that each string is an optional dialing scheme.
[]	Indicates that one digit or string can be selected from the options.

The MGCP-based MG interface supports the following types of digitmaps:

- Emergency call digitmap (due to call restriction in case of an overload)
- Automatic redial digitmap of the card service

Table 10-3 provides the valid characters in the strings and their meanings in the MGCP protocol.

Table 10-3 Digitmap format in the MGCP protocol

Digit or Character	Description
0-9	Indicate dialed digits 0-9.
A-D	-
X	Indicates for a wildcard, indicating any digit from 0 to 9.
T	Indicates that when detecting the timer timeout, the system reports a phone number digit by digit if the phone number is detected after the dialing scheme is matched.
*	Indicates * in the DTMF mode.
#	Indicates for # in the DTMF mode.
.	Indicates that there can be multiple digits (including 0) or characters before it.
|	Used to separate the strings and indicates that each string is an optional dialing scheme.

Digit or Character	Description
[]	Indicates that one digit or string can be selected from the options.

Procedure

- When the system protocol is H.248, perform the following operations to configure the digitmap.
  1. In the global config mode, run the **interface h248** command to enter the H.248 mode.
  2. Run the **digitmap set** command to configure the digitmap listed in the data plan.
  3. (Optional) Run the **digitmap-timer** command to configure the digitmap timer.

     Generally, the digitmap timer is issued by the MGC. In this case, the issued digitmap timer prevails regardless of whether a timer is configured on the AG. When the MGC does not issue the digitmap timer and the default digitmap timer does not meet the service requirements, you can configure the digitmap timer in this step.
  4. Check whether the configuration of the digitmap timer is the same as that in the data plan.
     - Run the **display digitmap** command to check whether the digitmap is configured correctly.
     - Run the **display digitmap-timer** command to check whether the digitmap timer is configured correctly.
- When the system protocol is MGCP, perform the following operations to configure the digitmap.
  1. In the global config mode, run the **interface mgcp** command to enter the MGCP mode.
  2. Run the **digitmap set** command to configure the digitmap listed in the data plan.
  3. (Optional) Run the **digitmap-timer** command to configure the digitmap timer.

     Generally, the digitmap timer is issued by the MGC. In this case, the issued digitmap timer prevails regardless of whether a timer is configured on the AG. When the MGC does not issue the digitmap timer and the default digitmap timer does not meet the service requirement, you can configure the digitmap timer in this step.
  4. Check whether the configuration of the digitmap timer is the same as that in the data plan.
     - Run the **display digitmap** command to check whether the digitmap is configured correctly.
     - Run the **display digitmap-timer** command to check whether the digitmap timer is configured correctly.

----End

Example

Assume that the inner digitmap of the H.248-based MG interface is configured. According to the data plan, the inner digitmap format is 1234xxxx. The digitmap timer is not configured because it is issued by the MGC. To configure the inner digitmap, do as follows:

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#digitmap set inner 1234xxxx
huawei(config-if-h248-0)#display digitmap
  ----------------------------------------------------------------------
  Inner digitmap                                          : 1234xxxx
  Emergency digitmap                                      : -
  Urgent digitmap (for overload or bandwidth restrict)    : -
  Dualdial digitmap for card service                      : -
  ----------------------------------------------------------------------
```

(Optional) Configuring the Software Parameters of an MG Interface

The software parameters of an MG interface mainly define certain common service attributes of the MG interface. After the configuration of the software parameters of an MG interface, the software parameters take effect immediately and the configuration is valid only to the MG interface.

Context

There are 34 software parameters (numbered from 0 to 33) of an MG interface that supports H. 248. **Table 10-4** lists the configurable parameters, and the other parameters are reserved in the system.

Table 10-4 Software parameters of an MG interface that supports H.248

Parameter	Description	Default Setting
2	Indicates whether the MG interface supports dual homing. To configure an MG interface to or not to support dual homing, use this parameter. If the MG interface does not support dual homing (value: 0), even if the secondary MGC is configured, the MG interface does not switch to registering with the secondary MGC when the MG interface fails to register with the primary MGC. If the MG interface supports dual homing and auto-switching (value: 2), even if the MG interface has registered with the secondary MGC, the MG interface can automatically switch back to the primary MGC when the primary MGC recovers.	0: indicates that dual homing is not supported.

Parameter	Description	Default Setting
4	Indicates whether a wildcard is used for the registration of the MG interface. To configure whether a wildcard is used for the registration of an MG interface, use this parameter. Using a wildcard for registration can reduce the quantity of messages between the MG interface and the MGC. When the wildcard is not used for registration, all the terminals on the MG interface need to register with the MGC in order. The registration without a wildcard is also called "single-endpoint registration".	0: indicates that a wildcard is used.
6	Indicates whether the MG interface supports device authentication. To configure an MG interface to or not to support authentication, use this parameter. After the device authentication is supported, run the **auth (h.248)** command to configure the authentication parameters, and then run the **reset (h.248)** command to reset the MG interface. In this way, the MGC can manage the security of the MGs and avoid illegal registration with the MGC.	1: indicates that device authentication is not supported.
7	Indicates whether the MG interface supports security header. To configure an MG interface to or not to support security header, use this parameter.	1: indicates that security header is not supported.

Parameter	Description	Default Setting
11	Indicates whether the MG interface supports emergency standalone. To configure whether an MG interface supports emergency standalone, use this parameter. If the MG interface supports emergency standalone, the users on the MG interface can make phone calls even if the MG fails to communicate with the MGC.	0: indicates that no call is permitted.
13	Digitmap matching mode	2: indicates the minimum matching.
15	Indicates whether the function of filtering media streams by source port is enabled on an MG interface. To enable or disable the function of filtering media streams by source port on an MG interface, use this parameter. When the function of filtering media streams by source port is enabled on the MG interface, only the media streams from the specific ports can be received.	0: indicates that media streams are not filtered by source port.
16	Indicates the length of the timer for filtering the media stream source port of the MG interface. To configure the length of the timer for filtering the media stream source port of an MG interface, use this parameter. When an MG interface does not filter the source port, the MG interface automatically filters the source port if the filtering timer times out.	5s

Parameter	Description	Default Setting
22	Indicates the type of the prompt tone that is played after the communication between the MG and the MGC is interrupted. To configure the type of the prompt tone after the communication between the MG and the MGC is interrupted, use this parameter.	0: indicates the busy tone.
23	Indicates the length of the timer for synchronizing the port status. To configure the length of the timer for synchronizing the port status, use this parameter.	35s
24	Indicates the maximum value of the Real-Time Transport Protocol (RTP) termination ID.	-
25	Indicates the maximum random value for the protection against avalanche of the H.248 interface.	-
26	Indicates the type of local blocking play tone.	0: indicates the busy tone.
27	Indicates the type of remote blocking play tone.	0: indicates the busy tone.
28	Indicates the duration of the howler tone.	60s
29	Indicates the duration of message waiting tone.	3s
30	Indicates the time limit of the alarm for extra long call.	60 minutes
31	Indicates whether to report the alarm for extra long call.	1: indicates that the alarm is not reported.
32	Min. auto registration interval of remotely-blocked port(s).	1800s
33	Whether MG heartbeat is shut down.	1: No, heartbeat is enabled

There are 17 software parameters (numbered from 0 to 16) of an MG interface that supports MGCP. **Table 10-5** lists the configurable parameters, and the other parameters are reserved in the system.

Table 10-5 Software parameters of an MG interface that supports MGCP

Parameter	Description	Default Setting
1	Indicates whether the ongoing call is maintained if the communication between the MG interface and the MGC is abnormal. To maintain the ongoing call when the communication between the MG interface and the MGC is abnormal, use this parameter.	1: disconnects all the calls at once.
2	Indicates whether the MG interface supports dual homing. To configure whether an MG interface supports dual homing, use this parameter. If the MG interface does not support dual homing (value: 1), even if the secondary MGC is configured, the MG interface does not switch to register with the secondary MGC when the MG interface fails to register with the primary MGC.	0: indicates that dual homing is supported.
3	Indicates whether the heartbeat message between the MG and the MGC is disabled. To configure whether the heartbeat message between the MG and the MGC is disabled, use this parameter.	1: indicates that the heartbeat message is not disabled.

Parameter	Description	Default Setting
4	Indicates whether a wildcard is used for the registration of the MG interface. To configure whether a wildcard is used for the registration of an MG interface, use this parameter. Using a wildcard for registration can reduce the quantity of messages between the MG interface and the MGC. When a wildcard is not used for registration, all the terminals on the MG interface need to register with the MGC in order. The registration without a wildcard is also called "single-endpoint registration".	0: indicates that a wildcard is used.
5	Indicates the MGC type. To select the MGC of a different type, use this parameter.	0
6	Indicates the maximum time threshold for responding to the heartbeat messages. To configure the maximum times for transmitting the heartbeat message continuously, use this parameter.	3
7	Indicates whether to report the heartbeat with the MG as an endpoint. To configure whether to report the heartbeat with the MG as an endpoint, use this parameter.	0: indicates that reporting the heartbeat with the MG as an endpoint is not supported.
10	Indicates the point-to-point (P2P) fault reporting. To configure whether the MG interface supports the P2P fault reporting from the ISDN terminals, use this parameter.	0: indicates that the P2P fault is reported.

Parameter	Description	Default Setting
11	Indicates the point-to-multipoint (P2MP) fault reporting. To configure whether the MG interface supports the P2MP fault reporting from the ISDN terminals, use this parameter.	1: indicates that the P2MP fault is not reported.
12	Indicates the type of local blocking play tone.	0: indicates the busy tone.
13	Indicates the type of remote blocking play tone.	0: indicates the busy tone.
14	Indicates the RTP filtering switch of the MGCP interface. To configure whether the RTP filtering function is enabled, use this parameter. When the RTP filtering function is enabled, only the media stream from the specific ports can be received.	1: indicates that the RTP filtering function is not enabled.
15	Indicates the duration of the howler tone.	60s
16	Whether the timer symbol "T" follows the number string reported by the signaling.	0: Yes

Procedure

- When the system protocol is H.248, perform the following operations to configure the software parameters of an MG interface.
  1. In the global config mode, run the **interface h248** command to enter the MG interface mode.
  2. Run the **mg-software parameter** command to configure the software parameters listed in the data plan.
  3. Run the **display mg-software parameter** command to check whether the software parameters of the MG interface are the same as those in the data plan.
- When the system protocol is MGCP, perform the following operations to configure the software parameters of an MG interface.
  1. In the global config mode, run the **interface mgcp** command to enter the MG interface mode.
  2. Run the **mg-software parameter** command to configure the software parameters listed in the data plan.

3. Run the **display mg-software parameter** command to check whether the software parameters of the MG interface are the same as those in the data plan.

----End

Example

To configure software parameter 11 of H.248-based MG interface 0 to 1 so that the MG interface supports emergency standalone and allows only internal calls, do as follows:

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#mg-software parameter 11 1
huawei(config-if-h248-0)#display mg-software parameter 11
  -------------------------------------------------
  Interface Id:0           para index:11  value:1
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
   Interface software parameter name:
   11: Stand alone support
       0: None
       1: Inner
       2: Emergency
       3: Both
```

(Optional) Configuring the Ringing Mode of an MG Interface

This topic describes how to configure the ringing mode of an MG interface to meet different user requirements.

Procedure

- If the system protocol is H.248, perform the following operations to configure the ringing mode of an MG interface.
  1. Check whether the preset ringing mode in the system meets the requirements according to the Usage Guidelines of the **mg-ringmode add** command.
     - If the preset ringing mode meets the requirements, go to **Step 3**.
     - If the preset ringing mode does not meet the requirements, proceed to **Step 2**.
  2. In the global config mode, run the **user defined-ring modify** command to configure the break-make ratio of user-defined ringing mode to form a ringing mode that meets the user requirement.

     CAUTION

     - After configuring the user-defined ringing mode, you need to reset the corresponding service board to make the configuration data take effect. Thus, the user of the service board can use the new user-defined ringing mode. If the service board has been in service for a period, evaluate the impact on the online users before resetting the service board, and then determine whether to perform this operation.
     - The system supports 16 user-defined ringing modes, which can be modified but cannot be added or deleted.

3. Run the **interface h248** command to enter the H.248 mode.
4. Run the **mg-ringmode add** command to add a ringing mapping.

⚠ **CAUTION**

1. The parameter *mgcpara* on the MG must be the same as the parameter *mgcpara* on the MGC.
2. User-defined ringing modes 0 to 15 correspond to cadence ringing modes 128 to 143 respectively, and correspond to initial ringing modes 144 to 159 respectively. For example, if the cadence ringing mode is 128, user-defined ringing mode 0 is selected. If the initial ringing mode is 144, user-defined ringing mode 0 is selected.

5. Run the **display mg-ringmode attribute** command to check whether the ringing mapping is the same as that in the data plan.

- If the system protocol is MGCP, perform the following operations to configure the ringing mode of an MG interface.
  1. According to the Usage Guidelines of the **mg-ringmode add** command, check whether the preset ringing mode in the system meets the requirement.
     - If the preset ringing mode meets the requirement, go to **Step 3**.
     - If the preset ringing mode does not meet the requirement, proceed to **Step 2**.
  2. In the global config mode, run the **user defined-ring modify** command to configure the user-defined ringing mode.

⚠ **CAUTION**

After configuring the user-defined ringing mode, you need to reset the corresponding service board to make the configuration data take effect. Thus, the user of the service board can use the new user-defined ringing mode. If the service board has been in service for a period, evaluate the impact on the online users before resetting the service board, and then determine whether to perform this operation.

  3. Run the **interface mgcp** command to enter the MGCP mode.
  4. Run the **mg-ringmode add** command to add a ringing mapping.

⚠ **CAUTION**

The parameter *mgcpara* on the MG must be the same as the parameter *mgcpara* configured on the MGC.

  5. Run the **display mg-ringmode attribute** command to check whether the ringing mapping is the same as that in the data plan.

----End

Example

Assume that the MG interface ID is 0, the peer parameter ID issued by the MGC is 0, the cadence ringing is 1:4 (the value of the corresponding parameter *cadence* is 0), and the initial ringing is 1:2 (the value of the corresponding parameter *initialring* is 17). To configure the ringing mode of MG interface 0, do as follows:

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#mg-ringmode add 0 0 17
huawei(config-if-h248-0)#display mg-ringmode attribute
{ <cr>|mgcpara<U><0,15> }:

  Command:
          display mg-ringmode attribute
  -------------------------------------------------------
   MGID       PeerPara   CadenceRing   InitialRing
  -------------------------------------------------------
   0          0          0             17
  -------------------------------------------------------
```

Assume that the MG interface ID is 0, the peer parameter ID issued by the MGC is 0, the break-make ratio of user-defined ringing mode 0 is 0.4sec On, 0.2sec Off, 0.4sec On, 2.0sec Off, and the initial ringing and the cadence ringing use user-defined ringing mode 0 (the values of the corresponding parameters *cadence* and *initialring* are 128 and 144 respectively). To configure the ringing mode of MG interface 0, do as follows:

```
huawei(config)#user defined-ring modify 0 para1 400 para2 200 para3 400 para4 2000
  Note: Please reset the service board to make configured parameter be valid
huawei(config)#display user defined-ring
  --------------------------------------------------
  RingType Para1 Para2 Para3 Para4 Para5 Para6
  --------------------------------------------------
  0         400   200   400   2000     0      0
  1           0     0     0      0     0      0
  2           0     0     0      0     0      0
  3           0     0     0      0     0      0
......
  14          0     0     0      0     0      0
  15          0     0     0      0     0      0
  --------------------------------------------------
huawei(config)#interface h248 0
huawei(config-if-h248-0)#mg-ringmode add 1 128 144
huawei(config-if-h248-0)#display mg-ringmode attribute
{ <cr>|mgcpara<U><0,15> }:
{ <cr>|mgcpara<U><0,15> }:

  Command:
          display mg-ringmode attribute
  -------------------------------------------------------
   MGID       PeerPara   CadenceRing   InitialRing
  -------------------------------------------------------
   0          1          128           144
  -------------------------------------------------------
```

(Optional) Configuring the TID Format of an MG Interface

The TID format determines how various user terminal IDs on the MG interface are generated.

Prerequisites

⚠ **CAUTION**

The configuration of the TID format is relatively complicated. The information such as the syntax rules with which the terminal prefix must comply and the requirements for the character string of the TID template is defined in the protocol, and is not described here. This topic describes only some basic information. It is recommended that you refer to the TID description in ITU-T H248.1 (applicable to H.248) or RFC 3435 (applicable to MGCP) before configuring the TID format.

Context

The TID format consists of the terminal prefix and the TID template. The TID template defines the generation mode of the TID excluding the terminal prefix. A TID consists of a terminal prefix and a character string generated by a TID template.

The TID templates that are bound to various types of users on the MG interface determine whether the users support terminal layering.

- If the parameter list of the TID template includes only keyword "G", the TID template is used by the non-layering users. Users bound with this template do not support terminal layering.
- If the parameter list of the TID template includes only keywords "F", "S", "P", "B" ("B" is not available to PSTN users), the TID template is used by the layering users. Users bound with this template support terminal layering.

NOTE

The meaning of each keyword is as follows:

- F indicates the subrack ID.
- S indicates the slot ID.
- P indicates the port ID.
- B indicates the B channel ID (only for ISDN BRA and ISDN PRA terminals).
- G indicates the general permanent termination index.
- R indicates the RTP ephemeral termination index (only for the RTP ephemeral termination, which exists only when the system protocol is H.248. This termination is not involved unless special remarks are provided.)

When adding a user that supports terminal layering, you cannot and do not have to specify the parameter **terminalid** because the system automatically allocates a terminal ID. When adding a user that does not support terminal layering, you must specify the parameter **terminalid**.

You can run the **display tid-format(h248)** command or **display tid-format(mgcp)** command to query the TID formats of various types of users on the current MG interface. In the query result, **template-index** indicates the index of the TID template that is bound to the type of users. Then, run the **display tid-template** command to check whether the TID template supports the layering configuration. Hence, you can check whether the user supports terminal layering.

Precautions

- There are 19 default TID templates (templates 0-18) in the system. The default TID templates can be referenced, but cannot be added, modified, or deleted.
- The configuration of terminal layering on the MG must be the same as that on the MGC.
- If certain type of terminals exists on an interface and the interface is not disabled, the terminal prefix of this type of terminals cannot be modified.
- If a certain type of terminals exists on an interface, the TID format (including the terminal prefix and the index of the TID template) of this type of terminals cannot be changed.
- The terminal prefix must comply with the following syntax rules: The prefix must not exceed 64 characters. Only letters, digits, "_", and "/" are the characters allowed for input. The first character must be a letter, and the last character must not be a digit.
- The length of the TID, which is generated by combining the TID template and the terminal prefix that you configured, must not exceed 64 characters.

Procedure

- If the system protocol is H.248, to configure the TID format on the current MG interface, do as follows:
  1. Run the **display tid-template** command to query the information about the default TID template of the system.
  2. If the default TID template cannot meet the service requirements, run the **tid-template add** command to add a TID template that meets the service requirements. If the default TID template meets the service requirements, proceed to **Step 3**.
  3. Run the **interface h248** command to enter the H.248 mode.
  4. Configure the TID templates and the terminal prefix of various types of users on the current MG (VAG).

     CAUTION

     The terminal prefix of PSTN, BRA and PRA must be all identical or unique.

     - In the H.248 mode, run the **tid-format rtp** command to configure the TID template and the terminal prefix of the RTP ephemeral termination.
     - In the H.248 mode, run the **tid-format pstn** command to configure the TID template and the terminal prefix of the PSTN user.
     - In the H.248 mode, run the **tid-format bra** command to configure the TID template and the terminal prefix of the ISDN BRA user.
     - In the H.248 mode, run the **tid-format pra** command to configure the TID template and the terminal prefix of the ISDN PRA user.
  5. Run the **display tid-format(h248)** command to check whether the TID templates and the terminal prefixes of various types of users on the current MG interface are the same as those in the data plan.
- If the system protocol is MGCP, to configure the TID format on the current MG interface, do as follows:
  1. Run the **display tid-template** command to query the information about the default TID template of the system.

2. If the default TID template cannot meet the service requirements, run the **tid-template add** command to add a TID template that meets the service requirements. If the default TID template meets the service requirements, proceed to **Step 3**.
3. Run the **interface mgcp** command to enter the MGCP mode.
4. Configure the TID templates and the terminal prefix of various types of users on the current MG (VAG).
   - In the MGCP mode, run the **tid-format pstn** command to configure the TID template and the terminal prefix of the PSTN user.
   - In the MGCP mode, run the **tid-format bra** command to configure the TID template and the terminal prefix of the ISDN BRA user.
   - In the MGCP mode, run the **tid-format pra** command to configure the TID template and the terminal prefix of the ISDN PRA user.
5. Run the **display tid-format(mgcp)** command to check whether the TID templates and the terminal prefixes of various types of users on the current MG interface are the same as those in the data plan.

----End

Example

Assume that in the H.248 mode, the terminal prefix of the PSTN user on MG interface 1 is aln/, and the layering TID template 3 is used. To add a PSTN user on port 0/2/0 and check whether the system automatically allocates a TID generated according to the template, do as follows:

```
huawei(config)#display tid-template 3//Query the information about TID template 3
  -------------------------------------------------
  Index      : 3
  Format     : %u/%u/%u
  Para-list  : F+1,S+1,P+1  //The parameter list of the TID template includes
keyword "F", "S",
                   //and "P", which indicates that this template supports terminal
layering.
  Name       : Aln_Not_Fixed_1
  -------------------------------------------------
huawei(config)#interface h248 1
huawei(config-if-h248-1)#tid-format pstn prefix aln template 3
huawei(config-if-h248-1)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser add 0/2/0 1
huawei(config-esl-user)#display mgpstnuser 0/2/0
{ <cr>|endframeid/slotid/portid<S><1,15> }:

  Command:
          display mgpstnuser 0/15/0
  ------------------------------------------------------------------------
  F  /S /P    MGID     TelNo            Priority PotsLineType TerminalID
  ------------------------------------------------------------------------
  0  /2 /0    1        -                Cat3     DEL          aln/1/3/1
             //The system allocates the terminal ID according to the TID format.
  ------------------------------------------------------------------------
```

Enabling an MG Interface

Enabling an MG interface is to reset an MG interface to make the MG interface register with the MGC (or to make the modified attributes of the MG interface take effect) after the configuration of the MG interface is complete, so that the MG interface can work in the normal state.

Precautions

WARNING

For the MG interface that has been in service, this operation interrupts the ongoing services carried on the MG interface. Hence, exercise caution when performing this operation.

Procedure

- Enable the MG interface that adopts the H.248 protocol.
  1. Run the **interface h248** command to enter the H.248 mode.
  2. Run the **reset coldstart** command to enable the MG interface.
  3. Run the **quit** command to return to the global config mode, and then run the **display if-h248 all** command to check whether the MG interface is in the normal state.
- Enable the MG interface that adopts the MGCP protocol.
  1. Run the **interface mgcp** command to enter the MGCP mode.
  2. Run the **reset** command to enable the MG interface.
  3. Run the **quit** command to return to the global config mode, and then run the **display if-mgcp all** command to check whether the MG interface is in the normal state.

----End

Example

To enable H.248-based MG interface 0, do as follows:

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
huawei(config)#display if-h248 all
--------------------------------------------------------------------------------
MGID     TransMode State          MGPort MGIP           MGCPort MGCIP/DomainName
--------------------------------------------------------------------------------
0        UDP       Normal         2944   10.10.10.11     2944   10.10.20.11
--------------------------------------------------------------------------------
```

To enable MGCP-based MG interface 0, do as follows:

```
huawei(config)#interface mgcp 0
huawei(config-if-mgcp-0)#reset
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#quit
huawei(config)#display if-mgcp all
  ------------------------------------------------------------------------
  MGID     State          MGPort MGIP            MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------
  0        Normal         2727   10.10.10.11     2727    10.10.20.11
  1        Wait ack       2527   10.10.10.12     2727    10.10.20.12
  ------------------------------------------------------------------------
```

10.1.2 Configuring the VoIP User

After an MG interface is configured, you can add plain old telephone service (POTS) users on the MG interface to implement the VoIP service.

Procedure

Configuring the PSTN User Data

This topic describes how to configure the PSTN user data (the same as the corresponding data on the MGC) on the MG interface to provide the POTS terminal with the access to the network for VoIP service.

Prerequisites

The POTS service board must be inserted into the planned slot, and the RUN ALM LED of the board must be green and must be on for 1s and off for 1s repeatedly.

NOTE

You can add a service board in two ways (see the Usage Guideline of the **board add** command). It is recommended that you insert the service board into the planned slot and then confirm the board.

Context

Table 10-6 lists the default settings of the attributes of the PSTN user. When configuring the attributes of the PSTN user, you need to modify them according to the service requirements.

Table 10-6 Default settings of the attributes of the PSTN user

Parameter	Default Settings
Sequence of sending the phone number of the caller	Ringing and then sending the phone number
Format of the phone number of the caller	FSK simple data message format
Power-off interval	10 ms
FSK delay interval	10 ms
Whether to enable or disable VQE automatic gain	Disable
Whether to enable or disable VQE noise suppression	Disable
Target value of VQE automatic gain	-22 dBm0
Target value of VQE noise suppression	12 dB
Input gain of the DSP chip	0 dB
Output gain of the DSP chip	0 dB
Name of the DSP parameter profile	- (indicates that the DSP parameter profile is not configured)

Procedure

Step 1 In the global config mode, run the **board confirm** command to confirm the service board.

Step 2 Add a PSTN user.

1. In the global config mode, run the **esl user** command to enter the ESL user mode.
2. Run the **mgpstnuser add** or **mgpstnuser batadd** command to add a PSTN user or add PSTN users in batches.

CAUTION

- When you add a PSTN user, the terminal ID must be configured and must be different from the terminal ID of an existing PTSN user if the TID template with which the PSTN user on the MG interface is bound is not a layering template.
- When you add a PSTN user, the configuration of the terminal ID is not required and the system automatically allocates the terminal ID if the TID template with which the PSTN user on the MG interface is bound is a layering template.
- When adding a PSTN user, you can configure the phone number (parameter *telno*). The phone number configured, however, can be used only as the paging number for emergency standalone. Phone numbers for normal call services are allocated by the MGC. It is recommended that the phone number configured here be the same as the phone number allocated by the MGC. In addition, the phone number must be unique in the MG. This is to avoid the number conflict that may occur when emergency standalone is enabled. If this parameter is not set, the phone number is null by default.
- For details about the relation between the TID template and the terminal layering, see the Background Information in **(Optional) Configuring the TID Format of an MG Interface**.

3. Run the **display mgpstnuser** command to check whether the PSTN user data is the same as that in the data plan.

Step 3 (Optional) Configure the attributes of the PSTN user.

The attributes of a PSTN user need to be configured when the default settings are not consistent with the actual application.

1. Run the **mgpstnuser attribute set** or **mgpstnuser attribute batset** command to configure the attributes of the PSTN user.
2. Run the **display mgpstnuser attribute** command to check whether the attributes of the PSTN user are the same as those in the data plan.

----End

Example

Assume that the phone numbers of 32 PSTN users are 83110000-83110031, the **terminalid** values are 0-31 (the TID template to which the PSTN users under the MG interface are bound does not support layering and **terminalid** should be allocated manually), and the default values are used for other attributes. To add the 32 PSTN users in slot 0/2 under MG 0 in batches, do as follows:

```
huawei(config)#board confirm 0/2
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/2/0 0/2/31 0 terminalid 0 telno
83110000
huawei(config-esl-user)#display mgpstnuser 0 0 32
  ------------------------------------------------------------------------
  F  /S /P    MGID     TelNo            Priority PotsLineType TerminalID
  ------------------------------------------------------------------------
  0  /2 /0    0        83110000         Cat3     DEL          A0
  0  /2 /1    0        83110001         Cat3     DEL          A1
  ......
  0  /2 /30   0        83110030         Cat3     DEL          A30
  0  /2 /31   0        83110031         Cat3     DEL          A31
  ------------------------------------------------------------------------
```

(Optional) Configuring the System Parameters

This topic describes how to configure the system parameters including the overseas version flag and message waiting indication (MWI) mode according to the local standards to ensure that the response of the user terminal complies with the local standards.

Context

Table 10-7 lists the system parameters supported by the MA5600T/MA5603T.

Table 10-7 System parameters supported by the MA5600T/MA5603T

Parameter	Description	Default Settings
0	Indicates the howler tone sending flag.	1: indicates that the howler tone is sent.
1	Indicates the overseas version flag.	0: indicates China.
2	Indicates the initial ringing stop flag.	0: indicates that the initial ringing stop flag is not issued.
3	Indicates the MWI mode.	1: indicates that the FSK is sent with ringing.
4	Indicates the global digitmap support flag.	1: indicates that the global digitmap is supported.
5	Indicates the media stream forwarding mode within the same device.	0: indicates that the media stream is forwarded within the device.
9	Indicates the QoS alarm number.	20
12	Indicates the howler tone source.	0: Analog subscriber line board.
15	whether a PRA Q.921 link will be created initiatively.	1:the MA5600T will not create a PRA 0.921 link.
16	whether a TEI status indication will be reported.	1: the TEI status indication will be reported.

Parameter	Description	Default Settings
17	whether an alarm will be reported when the subscriber line contacts the power cable.	0: the alarm will not be reported.

Procedure

Step 1 Run the **system parameters** command to configure the system parameters.

Step 2 Run the **display system parameters** command to check whether the system parameters are the same as those in the data plan.

----End

Example

To configure the overseas version flag (system parameter 1) to Hong Kong (parameter value 1), do as follows:

```
huawei(config)#system parameters 1 1
huawei(config)#display system parameters 1
  ----------------------------------------------------------------------------
  Parameter name index: 1     Parameter value: 1
  Mean: Overseas version flag, 0:China, 1:HongKong, 2:Brazil, 3:Egypt, 4:
Singapore, 5:Thailand, 6:France, 7:Britain MSFUK, 8:Britain ETSI, 9:Bulgaria,
10:Reserved, 11:Austria, 12:Hungary, 13:Poland
  ----------------------------------------------------------------------------
```

(Optional) Configuring the Overseas Parameters

By default, the overseas parameters are configured according to the Chinese standards. In the actual service configuration, the attributes such as the upper and lower thresholds of the flash-hooking duration can be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.

Context

Table 10-8 lists the overseas parameters supported by the MA5600T/MA5603T.

Table 10-8 Overseas parameters supported by the MA5600T/MA5603T

Parameter	Description	Default Settings
0	Indicates the upper threshold of the flash-hooking duration.	350 ms (complies with the Chinese standards)
1	Indicates the lower threshold of the flash-hooking duration.	100 ms (complies with the Chinese standards)
2	Indicates whether the current is limited when the user port is locked.	0: indicates that the current is not limited.

Parameter	Description	Default Settings
3	Indicates the detect time of flash upper limit to onhook	0 ms
4	Indicates the standard of the DTMF signal tone detection parameter	0: means to comply with the ITU-T Q.24 protocol standard. It is the common configuration for the detection parameter.
5	The flag of whether to change the terminal equipment identifier (TEI) value when an OLT interconnects with the softswitch in the ISDN PRA application.	The universal standard, which does not need to be modified.

Procedure

Step 1 Run the **oversea parameters** command to configure the overseas parameters.

Step 2 Run the **display oversea parameters** command to check whether the overseas parameters are the same as those in the data plan.

----End

Example

To set the upper flash-hooking threshold (overseas feature parameter 0) to 800 ms (in compliance with the Hong Kong standard) and the lower flash-hooking threshold (overseas feature parameter 1) to 100 ms (in compliance with the Hong Kong standard), do as follows:

```
huawei(config)#oversea parameters 0 800
huawei(config)#oversea parameters 1 100
huawei(config)#display oversea parameters
{ <cr>|name<U><0,99> }:

  Command:
          display oversea parameters
  -----------------------------------------------------------------------------
  Parameter name index: 0     Parameter value: 350
  Mean: Hooking upper threshold(ms), reference: China:350, HongKong:800
  -----------------------------------------------------------------------------
  Parameter name index: 1     Parameter value: 90
  Mean: Hooking lower threshold(ms), reference: China:100, HongKong:100
  -----------------------------------------------------------------------------
  Parameter name index: 2     Parameter value: 0
  Mean: Flag of applying PARKED LINE FEED or not when user port is locked, 0:not
 apply, 1:apply
  -----------------------------------------------------------------------------
  Parameter name index: 3     Parameter value: 0
  Mean: The detect time of flash upper limit to onhook, default value: 0ms
  -----------------------------------------------------------------------------
  Parameter name index: 4     Parameter value: 1
  Mean: DTMF Detector Tuning, 0:Q.24, 1:Russia
-----------------------------------------------------------------------------
  Parameter name index: 5     Parameter value: 0
  Mean: Flag of changing TEI value for software switch, 0:no change, 1:set TEI
value to 1, 2:set TEI value to 0. Default: 0
  -----------------------------------------------------------------------------
```

(Optional) Configuring the Attributes of a PSTN Port

This topic describes how to configure the attributes of a PSTN port to ensure that the PSTN port can meet the actual application requirements.

Context

The MA5600T/MA5603T supports the following attributes of a PSTN port:

- Physical attributes (including whether to support the polarity reversal pulse, whether to support the port locking, and dialing mode). For details about how to configure the physical attributes of a PSTN port, see **pstnport attribute set**.
- Electrical attributes (including the impedance and the current). For details about how to configure the electrical attributes of a PSTN port, see **pstnport electric set**.
- KC attributes (including the KC accounting mode and the valid voltage). For details about how to configure the KC attributes of a PSTN port, see **pstnport kc set**.

Procedure

Step 1 In the global config mode, run the **pstnport** command to enter the PSTN port mode.

Step 2 Run the **pstnport attribute batset** or **pstnport attribute set** command to configure the physical attributes of the PSTN port.

Step 3 Run the **pstnport electric batset** or **pstnport electric set** command to configure the electrical attributes of the PSTN port.

⚠ **CAUTION**

- The physical attributes and the electrical attributes take effect immediately after the configuration. The KC attributes, however, take effect after the service board where the port is located is reset through the **board reset** command.
- Resetting the service board interrupts all the ongoing services that are carried. Hence, exercise caution when performing this operation.

Step 4 Run the **pstnport kc batset** or **pstnport kc set** command to configure the KC attributes of the PSTN port.

Step 5 Check whether the attribute configuration of the PSTN port is the same as that in the data plan.

- Run the **display pstnport attribute** command to query the physical attributes of the PSTN port.
- Run the **display pstnport electric** command to query the electrical attributes of the PSTN port.
- Run the **display pstnport kc** command to query the KC attributes of the PSTN port.

----End

Example

To configure the 32 PSTN ports of the board in slot 0/3 to support the polarity reversal accounting, do as follows:

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
huawei(config-pstnport)#display pstnport attribute 0/3
  --------------------------------------------------------------------
  F  /S  /P                0/3 /0
  ReversePolepulse         Enable
  PulseLevel               100(ms)
  PolarityReverseMode      Hard-polarity-reverse
  Dial-Mode                DTMF-Pulse-Both
  LineLock                 Enable
  NlpMode                  Nlp normal mode
  PolarityReverseWhenCLIP  Disable
  PulsePeriodUpperLimit    200(ms)
  PulsePeriodLowerLimit    50(ms)
  PulseDurationUpperLimit  90(ms)
  PulseDurationLowerLimit  30(ms)
  PulsePauseUpperLimit     90(ms)
  PulsePauseLowerLimit     30(ms)
  --------------------------------------------------------------------
  F  /S  /P                0/3 /1
  ReversePolepulse         Enable
  PulseLevel               100(ms)
  PolarityReverseMode      Hard-polarity-reverse
  Dial-Mode                DTMF-Pulse-Both
  LineLock                 Enable
  NlpMode                  Nlp normal mode
  PolarityReverseWhenCLIP  Disable
  PulsePeriodUpperLimit    200(ms)
  PulsePeriodLowerLimit    50(ms)
  PulseDurationUpperLimit  90(ms)
  PulseDurationLowerLimit  30(ms)
  PulsePauseUpperLimit     90(ms)
  PulsePauseLowerLimit     30(ms)
  ----------------------------------------------------------------------------
...
  F  /S  /P                0/3 /31
  ReversePolepulse         Enable
  PulseLevel               100(ms)
  PolarityReverseMode      Hard-polarity-reverse
  Dial-Mode                DTMF-Pulse-Both
  LineLock                 Enable
  NlpMode                  Nlp normal mode
  PolarityReverseWhenCLIP  Disable
  PulsePeriodUpperLimit    200(ms)
  PulsePeriodLowerLimit    50(ms)
  PulseDurationUpperLimit  90(ms)
  PulseDurationLowerLimit  30(ms)
  PulsePauseUpperLimit     90(ms)
  PulsePauseLowerLimit     30(ms)
  ----------------------------------------------------------------------------
```

NOTE

When a call begins and ends, the MG shows the start time and the end time based on the polarity reversal on the subscriber line. The billing terminal that supports the polarity reversal accounting function, such as a charging phone set, implements the polarity reversal accounting function based on the start time and the end time of a call.

(Optional) Configuring the Attributes of the Ringing Current

You can adjust the ringing volume and ringing tone by modifying the attributes of the ringing current. In general, the attributes of the ringing current do not need to be modified. You need to modify the attributes of the ringing current according to the local standards only when the default ringing current attributes do not meet the local standards.

Context

The attributes of the ringing current include the following two parameters:

- Ringing current frequency: A higher frequency indicates a sharper ringing tone. The default ringing current frequency is 25 Hz.
- AC amplitude (AC voltage): A greater amplitude indicates a louder ringing tone. The default AC amplitude is 75 Vrms.

Procedure

Step 1 In the global config mode, run the **voip** command to enter the VoIP mode.

Step 2 Run the **ring attribute set** command to configure the attributes of the ringing current according to the data plan.

Step 3 Run the **display ring attribute** command to check whether the attributes of the ringing current are the same as those in the data plan.

----End

Example

To set the ringing current frequency to 50 Hz (parameter value 2), AC amplitude to 50 Vrms (parameter value 2), do as follows:

```
huawei(config-voip)#ring attribute set frequency 2 acamplitude 2
huawei(config-voip)#display ring attribute
  ringing current frequency  : 50HZ
  ringing current acamplitute: 50VRMS
```

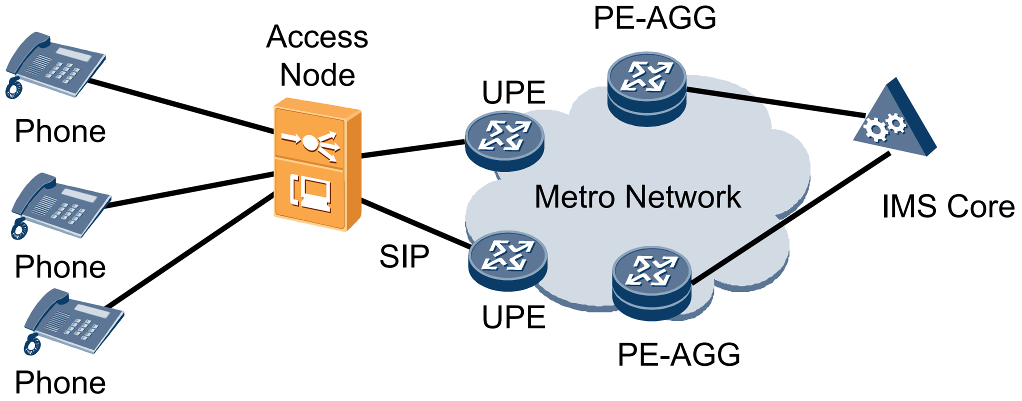
10.2 Configuring the VoIP Service (SIP-based)

The SIP-based VoIP technology makes the transport network evolve to the IP network without decreasing the voice quality, provides more value-added functions for users, and saves expense.

Application Context

As shown in **Figure 10-1**, the MA5600T/MA5603T functions as an SIP access gateway. In the downstream direction, it provides the access to PSTN users; in the upstream direction, it is connected to the IMS system, working with the IMS core to provide the VoIP service based on SIP.

Figure 10-1 Example network of the SIP voice service



Prerequisite

- The current system protocol is the SIP protocol. If the current system protocol is not the SIP protocol, change the current system protocol to the SIP protocol with reference to the **Adding an SIP Interface**.
- According to the actual network, a route from the MA5600T/MA5603T to the IMS core network device must be configured to ensure that the MA5600T/MA5603T and the IMS core network device are reachable from each other.
- The voice daughter board on the control board works in the normal state.
- Electronic switch 1 must be in location-0 (indicating that the VoIP service is supported) If the SCUB control board is used. For details of the configuration method, see **electro-switch**.

Data Plan

Table 10-9 provides the data plan for configuring the VoIP service.

Table 10-9 Data plan for configuring the SIP-based VoIP service

Item			Remarks
SIP interface data (Must be the same as that on the IMS core network device.)	Parameters related to the media stream and the signaling flow	Media and signaling upstream VLAN	It is used as the upstream VLAN of the VoIP service to be configured. Note that the media stream and the signaling stream can use the same VLAN or different VLANs. The result is determined according to the negotiation with the upstream device.
		Signaling upstream port	Upstream port for configuring the SIP signaling.
		Media IP address and signaling IP address	These IP addresses must be selected from the media and signaling IP address pools. The media and signaling IP address pools consists of all the IP addresses of the Layer 3 interface of the media and signaling upstream VLAN.
		Default IP address of the MG	Next hop address from the MA5600T/MA5603T to the IMS core network device. **CAUTION** If the media IP address and the signaling IP address are different and the media and the signaling are transmitted upstream through different gateways, ensure that they correspond to correct gateways. Otherwise, normal calls may not be made.

Item			Remarks
	Parameters of the SIP interface **NOTE** Parameters listed here are mandatory, which means that the SIP interface fails to be enabled if these parameters are not configured.	SIP interface ID	It is SIP interface ID used for the VoIP service to be configured, which determines the virtual access gateway (VAG) specified for the user.
		Signaling port ID of the SIP interface	The value range is 5000-5999. The protocol defines the port ID as 5060.
		IP address of the active IMS core network device to which the SIP interface belongs	When dual homing is not configured, parameters of only one IMS core network device are required. If dual homing is configured, the IP address and the port ID of the standby IMS core network device must be configured.
		Port ID of the active IMS core network device to which the SIP interface belongs	
		Transmission mode of the SIP interface	The transmission mode is selected according to the requirements on the IMS core network device. Generally, UDP is adopted.
		Home domain of the SIP interface	It corresponds to parameter **home-domain** in the MG interface attributes.
		Index of the profile used by the SIP interface	It corresponds to parameter **Profile-index** in the MG interface attributes.
		IP address obtaining mode of the proxy server	● In the IP mode, the IP address and the port ID of the active proxy server must be configured. ● In the DNS-A or DNS-SRV mode, the domain of the active proxy server must be configured.
	Ringing mode of the SIP interface		According to the service requirements, the ringing mode of the SIP interface is determined.
Voice user data (Must be the same as that on the IMS core network device.)	Slot for the voice service board		-
	User data	Phone number	The phone number that the IMS core network device allocates to the user must be configured.

Item			Remarks
		User priority	According to the service requirements, user priority needs to be specified. The user priority includes the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)
		User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
	System parameters		The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	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 do not need to be modified if there is no special requirement.
	Ringing current attributes		You can adjust the ringing volume by modifying the attributes of the ringing current. Generally, the parameters of the ringing current attributes do not need to be modified. You do not need to modify the parameters of the ringing current attributes according to the local standards only when the default ringing current attributes do not meet the local standards.

Procedure

10.2.1 Configuring an SIP Interface

As an interface used for the intercommunication between the MA5600T/MA5603T and the MGC, the interface is vital to the SIP-based VoIP service. Therefore, to implement the VoIP service, the SIP interface must be configured and must be in the normal state.

Procedure

Configuring the Upstream VLAN Interface

This topic describes how to specify the upstream VLAN interface for the media stream and the signaling flow, and how to configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the media and signaling IP address pools.

Context

Multiple IP addresses can be configured for the same VLAN Layer 3 interface. Only one IP address functions as the primary address, and other IP addresses function as the secondary addresses.

Procedure

Step 1 Run the **vlan** command to add an upstream VLAN for the media stream and the signaling flow.

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

Step 3 Configure the IP addresses of the VLAN Layer 3 interface.

1. Run the **interface vlanif** command to enter the Layer 3 interface of the upstream VLAN for the media stream and the signaling flow.
2. Run the **ip address** command to configure the IP addresses of the Layer 3 interface.

Step 4 Run the **display interface vlanif** command to check whether the IP addresses of the Layer 3 interface are the same as those in the data plan.

----End

Example

Assume that the media stream and the signaling stream are transmitted upstream through upstream port 0/19/0. To create media and signaling upstream VLAN 3 and configure IP addresses 10.13.4.116/16 and 10.13.4.117/16 of the Layer 3 interfaces for the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#vlan 3 standard
huawei(config)#port vlan 3 0/19 0
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 10.13.4.116 16
huawei(config-if-vlanif3)#ip address 10.13.4.117 16 sub
huawei(config-if-vlanif3)#quit
huawei(config)#display interface vlanif 3
vlanif3 current state : UP
```

```
Line protocol current state : UP
Description : HUAWEI, SmartAX Series, vlanif3 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is 10.13.4.116/16
Internet Address is 10.13.4.117/16 Secondary
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc32-1118
```

Configuring the Media and Signaling IP Address Pools

The media IP address pool defines all media IP addresses that can be used by the AG, and the signaling IP address pool defines all signaling IP addresses that can be used by the AG.

Prerequisites

The IP address of the Layer 3 interface of the media and signaling upstream VLAN must be configured. For details about how to configure the IP address, see **Configuring the Upstream VLAN Interface**.

Context

- The media IP address and the signaling IP address for the MG interface must be selected from the IP address pools configured here.
- The signaling IP address pool is used to store the IP addresses of the MG interfaces, and the media IP address pool is used to store the IP addresses of the media streams controlled by the signaling.
- The media IP address pool and the signaling IP address pool can be the same. Similarly, the media IP address and the signaling IP address can be the same.

CAUTION

The MGCP interface on the MA5600T/MA5603T does not support the isolation of media streams and signaling flows. Therefore, when the MGCP protocol is used, the media IP address pool and the signaling IP address pool must be the same. When the H.248 or SIP protocol is used, the media IP address pool and the signaling IP address pool can be the same or different.

Procedure

Step 1 Run the **voip** command to enter the VoIP mode.

Step 2 Configure the media IP address pool.

1. Run the **ip address media** command to add the media IP address to the media IP address pool.

   The media IP address needs to be selected from the IP addresses of the Layer 3 interface of the media and signaling upstream VLAN.

2. Run the **display ip address media** command to check whether the media IP address pool is the same as that in the data plan.

Step 3 Configure the signaling IP address pool.

1. Run the **ip address signaling** command to add the signaling IP address to the signaling IP address pool.

The signaling IP address needs to be selected from the IP addresses of the Layer 3 interface of the media and signaling upstream VLAN.

2. Run the **display ip address signaling** command to check whether the signaling IP address pool is the same as that in the data plan.

----End

Example

To add IP addresses 10.13.4.116/16 and 10.13.4.117/16 of Layer 3 interfaces of the media and signaling upstream VLAN to the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.13.4.116 10.13.0.1
huawei(config-voip)#ip address media 10.13.4.117 10.13.0.1
huawei(config-voip)#ip address signaling 10.13.4.116
huawei(config-voip)#ip address signaling 10.13.4.117
huawei(config-voip)#display ip address media
  Media:
  IP Address...........: 10.13.4.116
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.0.1
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.0.1
  MAC Address..........: 00-E0-FC-AF-91-33
huawei(config-voip)#display ip address signaling
  Signaling:
  IP Address...........: 10.13.4.116
  Subnet Mask..........: 255.255.0.0
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  MAC Address..........: 00-E0-FC-AF-91-33
```

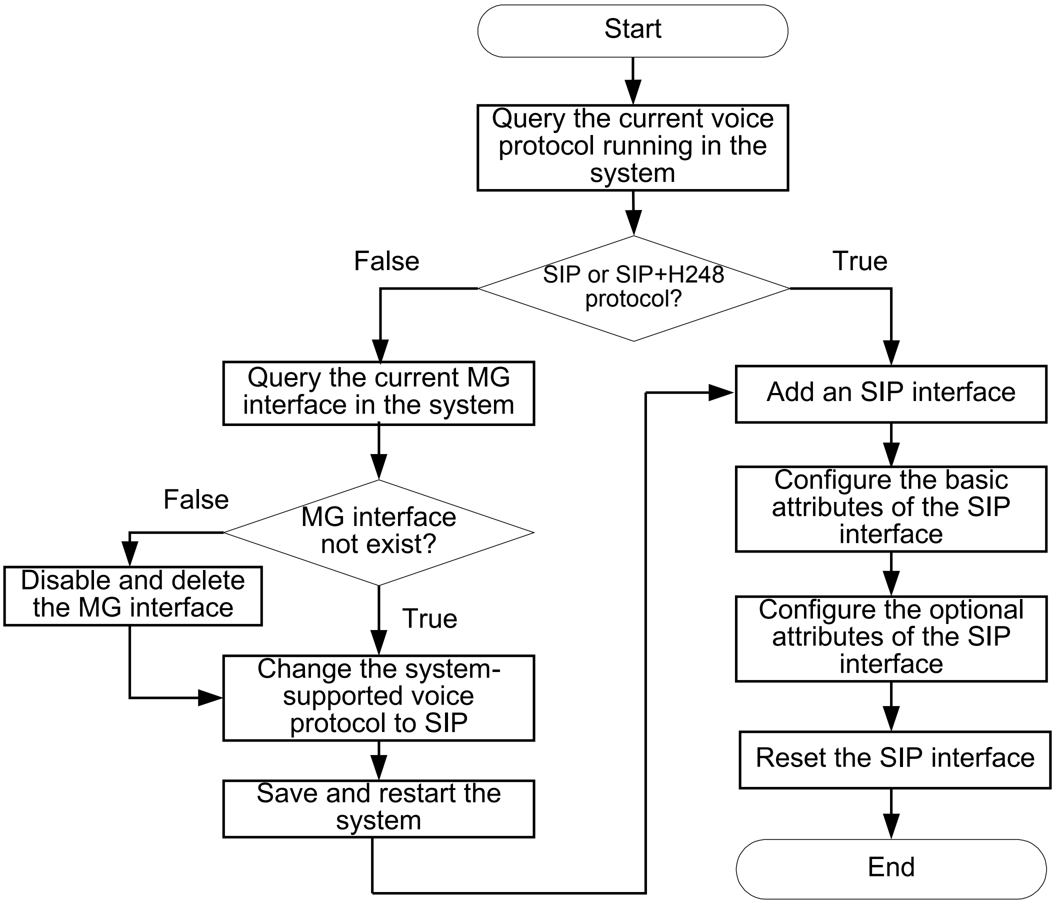
Adding an SIP Interface

The MA5600T/MA5603T exchanges the signaling and protocol packets with the information management system (IMS) through an SIP interface. To ensure uninterrupted signaling and protocol packet exchange, ensure that the status of the SIP interface is in a normal state after you add it.

Context

- One MA5600T/MA5603T supports up to eight SIP interfaces. Each SIP interface can be configured with the interface attributes separately.
- The SIP attributes configured for an SIP interface take effect on this interface only.
- The attributes of an SIP interface, including the signaling IP address, media IP address, transport-layer protocol, port ID of the transport-layer protocol, IP address (or domain name) of the proxy server, port ID of the proxy server, home domain name, profile index, are mandatory. In addition, the attributes of an SIP interface must be consistent with those configured on the IMS side so that the status of the SIP interface is normal.

Configuration Flowchart


Start
Query the current voice protocol running in the system
SIP or SIP+H248 protocol?
False
True
Query the current MG interface in the system
MG interface not exist?
False
Disable and delete the MG interface
True
Change the system-supported voice protocol to SIP
Save and restart the system
Add an SIP interface
Configure the basic attributes of the SIP interface
Configure the optional attributes of the SIP interface
Reset the SIP interface
End

Procedure

Step 1 Query the current voice protocol running in the system.

Run the **display protocol support** command to query the voice protocol that is currently supported by the system.

- If the system voice protocol is the SIP protocol, go to **Step 6**.
- If the system voice protocol is not the SIP protocol, go to **Step 2**.

Step 2 Query the current MG interface in the system.

Run the **display if-mgcp all** or **display if-h248 all** command to query whether an MGCP interface or an H.248 interface currently exists in the system.

- If there is no such an MG interface, go to **Step 4**.
- If there is such an MG interface, go to **Step 3**.

Step 3 Disable and delete the MG interface.

1. Delete the user data of this MG interface, and then run the **shutdown(mgcp)** or **shutdown (h248)** command to disable the MG interface according to the protocol type of the interface.

⚠ **CAUTION**

This operation interrupts all the ongoing services carried on the MG interface. Hence, exercise caution when performing this operation. Before performing this operation, you must check whether the operation is allowed.

2. Run the **undo interface mgcp** or **undo interface h248** command to delete the MG interface.

Step 4 Change the system-supported voice protocol to SIP.

Run the **protocol support** command to change the system-supported voice protocol to SIP.

Step 5 Save the configuration data and restart the system.

Save the configuration data by running the **save** command. Then run the **reboot** command to restart the system to make the new configuration data take effect.

Step 6 Run the **interface sip** command to add an SIP interface.

Step 7 Run the **if-sip attribute basic** command to configure the basic attributes of the SIP interface.

NOTE

- Between **proxy IP** and **proxy domain**, which are basic attributes, at least one attribute must be configured. If both attributes are configured, the system determines which attribute is used according to the configured address mode of the proxy server.
- The profile index must be configured.

Step 8 Run the **if-sip attribute optional** command to configure the optional attributes of the SIP interface.

The optional attributes include some new service types supported by the SIP interface, such as the conference call, message waiting indicator, UA-profile subscription, and REG-state subscription, and also include the SIP proxy configuration mode. The optional attributes require the IMS-side support, and must be consistent with those on the IMA-side.

After the configuration is completed, run the **display if-sip attribute config** command to query the attributes of the SIP interface.

Step 9 Reset the SIP interface.

Run the **reset** command to reset the SIP interface for the new configuration data to take effect. Otherwise, the configuration data does not take effect but is only stored in the database.

After the SIP interface is reset successfully, run the **display if-sip attribute running** command to query the running status of the SIP interface. If the active (or standby) proxy is **up**, the SIP interface is normal.

----End

Example

Assume that: the media IP address is 10.10.10.13, signaling IP address is 10.10.10.13, transmission protocol is UDP, port ID is 5000, active proxy server IP address 1 is 10.10.10.14, port ID of the active proxy server is 5060, active proxy server domain name is proxy.domain, standby proxy server IP address 1 is 10.10.10.15, port ID of the standby proxy server is 5060, home domain name is sip.huawei.com, and profile index is 1. To configure the attributes of SIP interface 0, do as follows:

```
huawei(config)#interface sip 0
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.13 signal-ip 10
.10.10.13 signal-port 5000 transfer udp primary-proxy-ip1 10.10.10.14 primary-pr
oxy-port 5060 primary-proxy-domain proxy.domain secondary-proxy-ip1 10.10.10.15
secondary-proxy-port 5060 home-domain sip.huawei.com sipprofile-index 1
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#
  Resetting SIP interface 0 succeeded
huawei(config-if-sip-0)#display if-sip attribute running
  ------------------------------------------------------------
  ...//The rest information in response to this command is omitted.
  Primary Proxy State                 up   //Indicates that the SIP interface is
in the normal state.
  Secondary Proxy State               down
  ...
  ------------------------------------------------------------
```

(Optional) Configuring the Ringing Mode of the SIP Interface

This topic describes how to configure the ringing mode of the SIP interface to support the break-make ratios of various new ringing modes and make the ringing mode meet the local standards.

Prerequisites

The SIP interface must be added successfully.

Context

- If the preset ringing modes of the system can meet the user requirements, you can select the required ringing mode and configure the corresponding ringing mapping.
- If the system-defined ringing modes cannot meet the user requirements, you can use the user-defined ringing mode and configure the corresponding ringing mapping.
- The user can configure the cadence duration for the user-defined ringing to form different ringing modes.
- The user-defined ringing modes are 0-15, which correspond to the cadence ringing modes 128-143 and initial ringing modes 144-159 defined by the user. For example, if the user-defined cadence ringing mode is 128, user-defined ringing mode 0 is selected. If the user-defined initial ringing mode is 144, user-defined ringing mode 0 is selected.
- The system supports up to 16 records of the ringing mode mapping.

Precautions

- The ringing mapping name must be unique on the same SIP interface.
- An index can be used for adding only one ringing mode on the same SIP interface.
- The 16 user-defined ringing modes can be modified but cannot be added.

Procedure

Step 1 According to the Usage Guidelines of the **ringmode add** command, check whether the preset ringing mode in the system meets the requirement.

- If the requirement is met, proceed to **step 4**.
- If the requirement is not met, go to **step 2**.

Step 2 In the global config mode, run the **user defined-ring modify** command to configure the user-defined ringing mode.

NOTE

- To use the user-defined ringing mode, perform this step and you can define the ringing types numbered 0-15.
- After configuring the user-defined ringing mode, you need to reset the corresponding service board to make the configuration data take effect, so that the user of the service board can use the new user-defined ringing mode. If the service board has been in service for a period, evaluate the impact on the online users before resetting the service board, and then determine whether to perform this operation.

Step 3 Run the **display user defined-ring** command to query the user-defined ringing.

Step 4 Run the **interface sip** command to enter the SIP mode.

Step 5 Run the **ringmode add** command to add a ringing mapping.

Run this command to configure the ringing mode for the users of the same SIP interface. The key parameters are described as follows:

- cadencering: Indicates the cadence ringing mode. The range 128-143 of this parameter corresponds to user-defined ringing modes 0-15.
- initialring: Indicates the initial ringing mode. The range 144-159 of this parameter corresponds to user-defined ringing modes 0-15.

Step 6 Run the **display user defined-ring** command to query ringing mapping records.

----End

Example

To add such a ringing mode mapping record on SIP interface 0, assume that:

- Index of the ringing mode mapping record: 1
- Name of the ringing mode mapping record: alert-group
- Cadence ringing mode: 1
- Initial ringing mode: 4

do as follows:

```
huawei(config)#interface sip 0
huawei(config-if-sip-0)#ringmode add 1 alter-group cadencering 1 initialring 4
huawei(config-if-sip-0)#display ringmode 1
  -----------------------------------------------------------------
  MGID: 0
  Index: 1
  Ringmode-name: alter-group
  CadenceRing: Special Ring 1:2
  InitialRing: Normal Ring (FSK) 1:4
  -----------------------------------------------------------------
```

10.2.2 Configuring the VoIP User

After an SIP interface is configured, you can add plain old telephone service (POTS) users on the SIP interface to implement the VoIP service.

Procedure

Configuring the PSTN User Data

This topic describes how to configure the PSTN user data (the same as the corresponding data on the IMS) on the SIP interface to provide the POTS terminal with the access to the network for VoIP service.

Prerequisites

The POTS service board must be inserted into the planned slot, and the RUN ALM LED of the board must be green and must be on for 1s and off for 1s repeatedly.

NOTE

You can add a service board in two ways (see the Usage Guideline of the **board add** command). It is recommended that you insert the service board into the planned slot and then confirm the board.

Context

Table 10-10 lists the default configuration of the attributes of the PSTN user. When configuring the attributes of the PSTN user, you need to modify them according to the service requirements.

Table 10-10 Default settings of the attributes of the PSTN user

Parameter	Default Setting
Sequence of sending the phone number of the caller	Ringing and then sending the phone number
Format of the phone number of the caller	FSK simple data message format
Power-off interval	10 ms
FSK delay interval	10 ms
Whether to enable or disable VQE automatic gain	Disable
Whether to enable or disable VQE noise suppression	Disable
Target value of VQE automatic gain	-22 dBm0
Target value of VQE noise suppression	12 dB
Input gain of the DSP chip	0 dB
Output gain of the DSP chip	0 dB
Name of the DSP parameter profile	- (indicates that the DSP parameter profile is not configured)

Procedure

Step 1 In the global config mode, run the **board confirm** command to confirm the service board.

Step 2 Add a PSTN user.

1. In the global config mode, run the **esl user** command to enter the ESL user mode.
2. Run the **sippstnuser add** or **sippstnuser batadd** command to add the PSTN user.

⚠ **CAUTION**

- When adding a user, you can configure the phone number (parameter **telno**). When the public ID is generated by the phone number, you must enter the phone number. It is recommended that you configure this phone number the same as the phone number configured on the IMS. In addition, ensure that the phone number is unique inside the AG.

3. Run the **display sippstnuser** command to check whether the PSTN user data is the same as that in the data plan.

Step 3 (Optional) Configure the attributes of the PSTN user.

The attributes of a PSTN user need to be configured when the default configuration is not consistent with the actual application.

1. Run the **sippstnuser attribute set** or **sippstnuser attribute batset** command to configure the attributes of the PSTN user.
2. Run the **display sippstnuser attribute** command to check whether the attributes of the PSTN user are the same as those in the data plan.

----End

Example

Assume that the ASPB service board is located in slot 0/2. To configure the attributes of the 64 SIP PSTN users (phone numbers are from 83110000 to 83110063) connected to SIP interface 0, set the PSTN user type of ports from 0/2/0 to 0/2/31 to payphone, the call priorities of PSTN users from ports 0/2/32 to 0/2/63 to Cat2, and use default values for other parameters, do as follows:

```
huawei(config-esl-user)#sippstnuser batadd 0/2/0 0/2/63 0 telno 83110000 step 1
huawei(config-esl-user)#sippstnuser attribute batset 0/2/0 0/2/31 potslinetype p
ayphone
huawei(config-esl-user)#sippstnuser attribute batset 0/2/32 0/2/63 priority cat2
```

(Optional) Configuring the System Parameters

This topic describes how to configure the system parameters including the overseas version flag and message waiting indication (MWI) mode according to the local standards to ensure that the response of the user terminal complies with the local standards.

Context

Table 10-11 lists the system parameters supported by the MA5600T/MA5603T.

Table 10-11 System parameters supported by the MA5600T/MA5603T

Parameter	Description	Default Settings
0	Indicates the howler tone sending flag.	1: indicates that the howler tone is sent.
1	Indicates the overseas version flag.	0: indicates China.
2	Indicates the initial ringing stop flag.	0: indicates that the initial ringing stop flag is not issued.
3	Indicates the MWI mode.	1: indicates that the FSK is sent with ringing.
4	Indicates the global digitmap support flag.	1: indicates that the global digitmap is supported.
5	Indicates the media stream forwarding mode within the same device.	0: indicates that the media stream is forwarded within the device.
9	Indicates the QoS alarm number.	20
12	Indicates the howler tone source.	0: Analog subscriber line board.
15	whether a PRA Q.921 link will be created initiatively.	1:the MA5600T will not create a PRA 0.921 link.
16	whether a TEI status indication will be reported.	1: the TEI status indication will be reported.
17	whether an alarm will be reported when the subscriber line contacts the power cable.	0: the alarm will not be reported.

Procedure

Step 1 Run the **system parameters** command to configure the system parameters.

Step 2 Run the **display system parameters** command to check whether the system parameters are the same as those in the data plan.

----End

Example

To configure the overseas version flag (system parameter 1) to Hong Kong (parameter value 1), do as follows:

```
huawei(config)#system parameters 1 1
huawei(config)#display system parameters 1
  ----------------------------------------------------------------------------
  Parameter name index: 1     Parameter value: 1
  Mean: Overseas version flag, 0:China, 1:HongKong, 2:Brazil, 3:Egypt, 4:
Singapore, 5:Thailand, 6:France, 7:Britain MSFUK, 8:Britain ETSI, 9:Bulgaria,
10:Reserved, 11:Austria, 12:Hungary, 13:Poland
  -----------------------------------------------------------------------------
```

(Optional) Configuring the Overseas Parameters

By default, the overseas parameters are configured according to the Chinese standards. In the actual service configuration, the attributes such as the upper and lower thresholds of the flash-hooking duration can be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.

Context

Table 10-12 lists the overseas parameters supported by the MA5600T/MA5603T.

Table 10-12 Overseas parameters supported by the MA5600T/MA5603T

Parameter	Description	Default Settings
0	Indicates the upper threshold of the flash-hooking duration.	350 ms (complies with the Chinese standards)
1	Indicates the lower threshold of the flash-hooking duration.	100 ms (complies with the Chinese standards)
2	Indicates whether the current is limited when the user port is locked.	0: indicates that the current is not limited.
3	Indicates the detect time of flash upper limit to onhook	0 ms
4	Indicates the standard of the DTMF signal tone detection parameter	0: means to comply with the ITU-T Q.24 protocol standard. It is the common configuration for the detection parameter.
5	The flag of whether to change the terminal equipment identifier (TEI) value when an OLT interconnects with the softswitch in the ISDN PRA application.	The universal standard, which does not need to be modified.

Procedure

Step 1 Run the **oversea parameters** command to configure the overseas parameters.

Step 2 Run the **display oversea parameters** command to check whether the overseas parameters are the same as those in the data plan.

----End

Example

To set the upper flash-hooking threshold (overseas feature parameter 0) to 800 ms (in compliance with the Hong Kong standard) and the lower flash-hooking threshold (overseas feature parameter 1) to 100 ms (in compliance with the Hong Kong standard), do as follows:

```
huawei(config)#oversea parameters 0 800
huawei(config)#oversea parameters 1 100
huawei(config)#display oversea parameters
{ <cr>|name<U><0,99> }:

  Command:
          display oversea parameters
  -----------------------------------------------------------------------------
  Parameter name index: 0     Parameter value: 350
  Mean: Hooking upper threshold(ms), reference: China:350, HongKong:800
  -----------------------------------------------------------------------------
  Parameter name index: 1     Parameter value: 90
  Mean: Hooking lower threshold(ms), reference: China:100, HongKong:100
  -----------------------------------------------------------------------------
  Parameter name index: 2     Parameter value: 0
  Mean: Flag of applying PARKED LINE FEED or not when user port is locked, 0:not
 apply, 1:apply
  -----------------------------------------------------------------------------
  Parameter name index: 3     Parameter value: 0
  Mean: The detect time of flash upper limit to onhook, default value: 0ms
  -----------------------------------------------------------------------------
  Parameter name index: 4     Parameter value: 1
  Mean: DTMF Detector Tuning, 0:Q.24, 1:Russia
-----------------------------------------------------------------------------
  Parameter name index: 5     Parameter value: 0
  Mean: Flag of changing TEI value for software switch, 0:no change, 1:set TEI
value to 1, 2:set TEI value to 0. Default: 0
  -----------------------------------------------------------------------------
```

(Optional) Configuring the Attributes of a PSTN Port

This topic describes how to configure the attributes of a PSTN port to ensure that the PSTN port can meet the actual application requirements.

Context

The MA5600T/MA5603T supports the following attributes of a PSTN port:

- Physical attributes (including whether to support the polarity reversal pulse, whether to support the port locking, and dialing mode). For details about how to configure the physical attributes of a PSTN port, see **pstnport attribute set**.
- Electrical attributes (including the impedance and the current). For details about how to configure the electrical attributes of a PSTN port, see **pstnport electric set**.
- KC attributes (including the KC accounting mode and the valid voltage). For details about how to configure the KC attributes of a PSTN port, see **pstnport kc set**.

Procedure

Step 1 In the global config mode, run the **pstnport** command to enter the PSTN port mode.

Step 2 Run the **pstnport attribute batset** or **pstnport attribute set** command to configure the physical attributes of the PSTN port.

Step 3 Run the **pstnport electric batset** or **pstnport electric set** command to configure the electrical attributes of the PSTN port.

CAUTION

- The physical attributes and the electrical attributes take effect immediately after the configuration. The KC attributes, however, take effect after the service board where the port is located is reset through the **board reset** command.
- Resetting the service board interrupts all the ongoing services that are carried. Hence, exercise caution when performing this operation.

Step 4 Run the **pstnport kc batset** or **pstnport kc set** command to configure the KC attributes of the PSTN port.

Step 5 Check whether the attribute configuration of the PSTN port is the same as that in the data plan.

- Run the **display pstnport attribute** command to query the physical attributes of the PSTN port.
- Run the **display pstnport electric** command to query the electrical attributes of the PSTN port.
- Run the **display pstnport kc** command to query the KC attributes of the PSTN port.

----End

Example

To configure the 32 PSTN ports of the board in slot 0/3 to support the polarity reversal accounting, do as follows:

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
huawei(config-pstnport)#display pstnport attribute 0/3
  --------------------------------------------------------------------
  F  /S  /P                0/3 /0
  ReversePolepulse         Enable
  PulseLevel               100(ms)
  PolarityReverseMode      Hard-polarity-reverse
  Dial-Mode                DTMF-Pulse-Both
  LineLock                 Enable
  NlpMode                  Nlp normal mode
  PolarityReverseWhenCLIP Disable
  PulsePeriodUpperLimit    200(ms)
  PulsePeriodLowerLimit    50(ms)
  PulseDurationUpperLimit 90(ms)
  PulseDurationLowerLimit 30(ms)
  PulsePauseUpperLimit     90(ms)
  PulsePauseLowerLimit     30(ms)
  --------------------------------------------------------------------
  F  /S  /P                0/3 /1
  ReversePolepulse         Enable
  PulseLevel               100(ms)
  PolarityReverseMode      Hard-polarity-reverse
  Dial-Mode                DTMF-Pulse-Both
  LineLock                 Enable
  NlpMode                  Nlp normal mode
  PolarityReverseWhenCLIP Disable
  PulsePeriodUpperLimit    200(ms)
  PulsePeriodLowerLimit    50(ms)
  PulseDurationUpperLimit 90(ms)
  PulseDurationLowerLimit 30(ms)
  PulsePauseUpperLimit     90(ms)
  PulsePauseLowerLimit     30(ms)
  ----------------------------------------------------------------------------
```

```
...
  F  /S  /P                 0/3 /31
  ReversePolepulse          Enable
  PulseLevel                100(ms)
  PolarityReverseMode       Hard-polarity-reverse
  Dial-Mode                 DTMF-Pulse-Both
  LineLock                  Enable
  NlpMode                   Nlp normal mode
  PolarityReverseWhenCLIP   Disable
  PulsePeriodUpperLimit     200(ms)
  PulsePeriodLowerLimit     50(ms)
  PulseDurationUpperLimit   90(ms)
  PulseDurationLowerLimit   30(ms)
  PulsePauseUpperLimit      90(ms)
  PulsePauseLowerLimit      30(ms)
  ----------------------------------------------------------------------------
```

NOTE

When a call begins and ends, the MG shows the start time and the end time based on the polarity reversal on the subscriber line. The billing terminal that supports the polarity reversal accounting function, such as a charging phone set, implements the polarity reversal accounting function based on the start time and the end time of a call.

(Optional) Configuring the Attributes of the Ringing Current

You can adjust the ringing volume and ringing tone by modifying the attributes of the ringing current. In general, the attributes of the ringing current do not need to be modified. You need to modify the attributes of the ringing current according to the local standards only when the default ringing current attributes do not meet the local standards.

Context

The attributes of the ringing current include the following two parameters:

- Ringing current frequency: A higher frequency indicates a sharper ringing tone. The default ringing current frequency is 25 Hz.
- AC amplitude (AC voltage): A greater amplitude indicates a louder ringing tone. The default AC amplitude is 75 Vrms.

Procedure

Step 1 In the global config mode, run the **voip** command to enter the VoIP mode.

Step 2 Run the **ring attribute set** command to configure the attributes of the ringing current according to the data plan.

Step 3 Run the **display ring attribute** command to check whether the attributes of the ringing current are the same as those in the data plan.

----End

Example

To set the ringing current frequency to 50 Hz (parameter value 2), AC amplitude to 50 Vrms (parameter value 2), do as follows:

```
huawei(config-voip)#ring attribute set frequency 2 acamplitude 2
huawei(config-voip)#display ring attribute
  ringing current frequency  : 50HZ
  ringing current acamplitute: 50VRMS
```

10.2.3 (Optional) Configuring the Centrex

Centrex refers to a virtual user group. The MA5600T/MA5603T supports the following functions: Members in a centrex can call each other by dialing short numbers, and members in a centrex can call the members outside of the centrex by dialing centrex prefix + the complete phone number. Generally, a softswitch issues centrex parameters. If a softswitch does not issue centrex parameters, use the parameters preset on the MA5600T/MA5603T. These parameter values must be the same as these on the softswitch.

Context

- Centrex prefix: When attempting to call a user in another centrex group, a user must dial the centrex prefix before dialing the called number. A centrex prefix contains 0 to 9 digits.
- The function that the members in a centrex can call each other by dialing short numbers need not be configured on the MA5600T/MA5603T through the command line interface (CLI).
- The function that the members in a centrex can call the members outside of the centrex by dialing centrex prefix + the complete phone number can be supported only when the SIP protocol is used.
- The centrex attribute of a centrex can be direct centrex or two-stage centrex. The similarity and difference are as follows:
  - Similarity: When the members in a centrex need to call the members outside of the centrex, they must dial the centrex prefix.
  - Difference: If the centrex attribute is set to two-stage centrex, the members in a centrex can hear the dial tone again after dialing the centrex prefix. If the centrex attribute is set to direct centrex, no out-group dial tone is played.

Procedure

Step 1 Configure the centrex call function for a centrex group.

The MA5600T/MA5603T supports the configuration of the centrex prefix through one of two methods. In method 1, configure the centrex prefix and centrex attributes for a single user in ESL user mode. In method 2, configure the centrex prefix and centrex attributes for all the users in global config mode. When both methods are used, method 1 takes effect.

- Use method 1:

1. In ESL user mode, run the **sippstnuser servicedata parameter set** command to configure the centrex prefix and centrex attributes of a centrex group.
2. Run the **display sippstnuser servicedata** command to check whether the centrex parameter settings of a centrex are the same as the data plan.

- Use method 2:

NOTE

If method 2 is used, the MA5600T/MA5603T uses the centrex digitmap to match the centrex prefix, and uses the call digitmap, or the normal digitmap, to match the phone number dialed by a user.

1. In global config mode, run the **local-digitmap add** command to configure a direct centrex digitmap or a two-stage centrex digitmap.

NOTE

- The system does not support the adding of a direct centrex digitmap and a two-stage centrex digitmap at the same time. Add a digitmap based on site requirements.
- When you add a direct centrex digitmap, the system centrex attribute is direct centrex. When you add a two-stage centrex digitmap, the system centrex attribute is two-stage centrex.

2. Run the **display local-digitmap** command to check whether the local digitmap is the same as the data plan.

Step 2 Check whether the value of the sipprofile control point 148 is the same as the data plan.

Run the **display sipprofile syspara detail** command to check whether the value of control point 148 is the same as the data plan. If they are different, run the **sipprofile modify** command in SIP mode to change the control point value.

NOTE

- The sipprofile control point 148 can be set to 0 or 1. When it is set to 0, a phone number does not contain a centrex prefix; when it is set to 1, a phone number contain a centrex prefix. By default, it is 1.
- Run the **if-sip attribute basic** *sipprofile-index 0* command to specify a user-defined profile for the current SIP interface, and run the **sipprofile modify** command to change the value for the sipprofile control point 148.

----End

MA5600T/MA5603T

Assume that the centrex prefix of the MA5600T/MA5603T user with phone number 88627792 is 8100, the centrex attribute is two-stage centrex, and the control point of the Sipprofile uses the default value.

To configure the centrex call function for such a user by using method 1, do as follows:

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser servicedata parameter set 0/2/1 telno 88627792
centrexprefix 8100 centrexflag dialsecondary
huawei(config-esl-user)#display sippstnuser servicedata 0/2/1 telno 88627792
  ------------------------------------------
  F /S /P                  : 0/2/1
  telno                    : 88627792
  centrexno                : -
  centrexprefix            : 8100
  centrexflag              : dialsecondary
  mwimode                  : deferred
  hottime(s)               : 100
  hotlinenum               : -
  dialtone                 : normal
  cfbnum                   : -
  cfnrnum                  : -
  cfunum                   : -
  cfnrtime(s)              : 100
  displayname              : -
  permanent-hold-mode      : norecall
  permanent-hold-time(s)   : 20
  ---------------------------------------------------
```

To configure the centrex call function for such a user by using method 2, and plan the digitmap body to (8100) and the digitmap name to **huawei1** for the two-stage centrex digitmap according to the centrex prefix, do as follows:

```
huawei(config)#local-digitmap add huawei1 second-centrex (8100)
huawei(config)#display local-digitmap all
  -------------------------------------------
  Name     : huawei1
  Type     : second-centrex
  Body     : (8100)
  Protocol: sip
  ------------------------------------------
```

10.2.4 (Optional) Configuring Line Hunting

When multiple E1 lines exist in the upstream direction of a private branch exchange (PBX), hunting is performed based on the pilot number or other accounts required by the PBX. The line hunting function allows one or multiple accounts to share a group of ports by configuring hunting groups and hunting policies.

Context

- A hunting group consists of ports, subhunting groups, and hunting rules. A sub hunting group also consists of ports, sub hunting groups, and hunting rules.
- A wildcard number can be configured for hunting groups, for example, 024545*. You can also configure a direct dialing number.
- A port can belong to multiple hunting groups which must be in the same VAG.
- Only the Session Initiation Protocol (SIP) supports the line hunting function.

Procedure

Step 1 Run the **hunting-group add** command to add a hunting group. Then the hunting group is added to the specified SIP interface.

Step 2 Run the **hunting-group member add** command to add hunting group members. A hunting group member can be a single port or a sub hunting group. After hunting group members are added, hunting is performed based on configurations.

Step 3 Run the **group-number add** command to add a hunting group account. After the group account is used by the hunting group, the account is called in based on hunting policies.

----End

Example

For example, when number 2878000 is dialed, hunting is cyclically performed between 0/2/1, 0/3/1, and 0/4/1 ports. When number 2878001 is dialed, the 0/2/1 is selected with preference. When the 0/2/1 port is busy, the 0/3/1 port is selected and then the 0/4/1 port. Configurations are as follows.

Parameter	HG1	HG2
hunting-mode		round-robin
inherit-flag		disable
Group members	0/2/1, 0/3/1, 0/4/1	0/2/1, 0/3/1, 0/4/1

```
huawei(config)#interface sip 0
Are you sure to add the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#hunting-group add HG1 hunting-mode order inherit-flag
```

```
disable
huawei(config-if-sip-0)#hunting-group add HG2 hunting-mode round-robin inherit-
flag disable
huawei(config-if-sip-0)#hunting-group member add HG1 0/2/1 6
huawei(config-if-sip-0)#hunting-group member add HG1 0/3/1 6
huawei(config-if-sip-0)#hunting-group member add HG1 0/4/1 6
huawei(config-if-sip-0)#hunting-group member add HG2 0/2/1 8
huawei(config-if-sip-0)#hunting-group member add HG2 0/3/1 7
huawei(config-if-sip-0)#hunting-group member add HG2 0/4/1 6
huawei(config-if-sip-0)#group-number add 2878000 hunting-group HG1
huawei(config-if-sip-0)#group-number add 2878001 hunting-group HG2
```

10.2.5 (Optional) Configuring Digitmap for SIP Interfaces

The digitmap, also called number list, refers to the dialing plan on the access gateway (AG), which is used to detect and report dialing events received at the termination point. The digitmap defines number collection rules. It allows dialing events to be reported by groups, which reduces signaling exchanges between the AG and IMS.

Prerequisites

CAUTION

The digitmap configuration is relatively complicated. The information such as the meanings and usage of the characters in a digitmap is defined in the protocol, and is not described here. This topic provides only some basic information. You are advised to refer to digitmap description in SIP standard before configuring a digitmap.

Context

- Different digitmaps are required for different services. A digitmap group includes different digitmaps, providing customized digitmaps to accommodate to users' requirements. In this way, signaling exchanges are reduced between the AG and IMS.
- A digitmap consists of digit and character strings. When the received dialing sequence matches one of the character strings, you can infer that all numbers are received.
- The priority sequence of the digitmap is: user digitmap group > interface digitmap group > global local digitmaps. If a digitmap group used by a user does not have corresponding digitmaps, this user does not have the corresponding digitmaps. For example, digitmap group A is configured in user attributes, and digitmap group B is configured in the interface of the user. Besides, two-stage out-group digitmaps are not specified in digitmap group A, but two-stage out-group digitmaps are specified in digitmap group B. When digitmaps are used, the user does not load any two-stage out-group digitmaps because digitmap group A with a highest priority does not have two-stage out-group digitmaps (although two-stage out-group digitmaps are specified in digitmap group B and local digitmaps have two-stage out-group digitmaps). If the user cannot find any user-level or interface-level digitmap groups, the user uses global local digitmaps.
- If digitmaps are not configured, the system provides a default digitmap for the user, in which all telephone numbers can be matched.

Table 10-13 provides the characters defined in the SIP protocol for digitmaps. For details, refer to the SIP standard, which provides a better guide to the digitmap configuration.

Table 10-13 SIP digitmap format

Digit or Character	Description
0-9	Indicates dialed digits 0-9.
A-D	-
E	Indicates the asterisk (*) in dual tone multiple frequency (DTMF) mode.
F	Indicates the pound key (#) in DTMF mode.
X	Indicates a wildcard, which is a digit ranging from 0 to 9.
S	Indicates the short timer. After the timer times out; that is, the dialing plan matching is complete, the system reports numbers one by one if numbers remain.
L	Indicates the long timer. After the timer times out; that is, the dialing plan matching is complete, the system reports numbers one by one if numbers remain.
Z	Indicates duration modifier, which is a dialing event with a long duration. The dialing event is located in front of the event symbol with a specified position. When the duration of the dialing event exceeds the threshold, the dialing event satisfies this position.
.	Indicates that 0 or multiple digits or characters can exist before this character.
|	Is used to isolate character strings. Each character string is a selectable dialing plan.
[]	Indicates that one of the digits or characters in the square bracket is selected.

Procedure

- Configure a digitmap.
  1. In global configuration mode, run the **local-digitmap add** command to add a local preset digitmap.
  2. (Optional) In SIP mode, run the **digitmap timer (sip)** command to configure a digitmap timer.
- Configure a digitmap group.
  1. In global configuration mode, run the **local-digitmap add** command to add a local preset digitmap.
  2. (Optional) In SIP mode, run the **digitmap timer (sip)** command to configure a digitmap timer.
  3. Run the **local-digitmap-group add** command to add a digitmap group.
  4. Run the **local-digitmap-group include** command to add local digitmap members to the digitmap group.

     The new digitmap group takes effect only when the user uses it in the next call.

5. Run the **mg-digitmap-group** command to configure the digitmap group used by the interface. The new digitmap group takes effect only when the user uses it in the next call.
6. Run the **sippstnuser attribute set** command to configure the digitmap group used by the user. The new digitmap group takes effect only when the user uses it in the next call.

----End

Example

For example, according to the data plan, digitmap group 1 is applied to users connected to the 0/6/0 port in the SIP interface. The digitmap group includes normal digitmaps and emergency digitmaps, whose formats are 8882xxxx and 8000xxxx respectively.

```
huawei(config)#local-digitmap add huawei normal 8882xxxx sip
huawei(config)#local-digitmap add huawei1 emergency 8000xxxx sip
huawei(config)#local-digitmap-group add DigitmapGroup1
huawei(config)#local-digitmap-group include DigitmapGroup1 huawei
huawei(config)#local-digitmap-group include DigitmapGroup1 huawei2
huawei(config)#interface sip 1
huawei(config-if-sip-1)#mg-digitmap-group DigitmapGroup1
huawei(config-if-sip-1)#quit
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser attribute set 0/6/0 cliptransseq digitmap-
group DigitmapGroup1
```

10.3 Configuring the H.248/MGCP-based FoIP Service

This topic describes how to configure the H.248/MGCP-based FoIP service.

Prerequisites

The VoIP service must be configured. For details, see **10.1 Configuring the VoIP Service (H.248-based or MGCP-based)**.

The voice service port used for the FoIP service must be in the normal state, and the voice communication on the port must be normal.

Context

Fax over Internet Protocol (FoIP) provides fax services on IP networks or between IP networks and PSTN networks. The FoIP service can be classified from two aspects:

- In terms of coding mode, the fax mode can be transparent fax (G.711 coding) or T.38 fax (T.38 coding).
- In terms of the participation of the MGC, one is the softswitch controlled flow, and the other is the self-switch flow (controlled by the gateway itself).

Data Plan

Before the data configuration, it is recommended that you plan the working mode of the FoIP service on the entire NGN network to ensure that the configurations on the entire network are consistent.

Table 10-14 Fax flows

Item	Flow	Remarks
Coding negotiation mode	Negotiation	The gateway negotiates the coding mode with the MGC through signaling.
	Self-switch	The gateway determines the coding mode to be adopted.
Coding mode	Transparent transmission fax	The G.711 coding mode is adopted.
	T.38 flow	The T.38 coding mode is adopted.
Negotiation flow	V2 flow (auto-negotiation flow)	The V2 flow is adopted as the fax/modem flow.
	V3 flow	The V3 flow is adopted as the fax/modem flow.
	V5 flow	The V5 flow is adopted as the fax/modem flow.

NOTE

V2, V3, and V5 flows refer to the versions of the fax/modem flow, which is defined by Huawei. If self-switch is adopted as the coding negotiation mode, the negotiation flow does not need to be configured.

Default Configuration

Table 10-15 lists the default settings of the FoIP flow.

Table 10-15 Default settings of the FoIP flow

Item	Default Setting
Coding negotiation mode	Negotiation
Coding mode	Transparent transmission fax
Negotiation flow	V3 flow
Enable packet interval of fax and modem to use only 10 ms or not	Disable
RFC2198 startup mode	DisableRfc2198SmartStartup
Event transmit mode	ControlledByMGC

Procedure

Step 1 Configure public fax and modem parameters.

In the global config mode, run the **fax-modem parameters negomode** command to configure public fax and modem parameters. The purpose of this step is to configure the coding negotiation mode. Two options are available: negotiation and self-switch.

Step 2 Configure the fax coding mode and negotiation flow.

In the global config mode, run the command to configure the fax transmission mode. There are three key parameters, which are described as follows:

- **transmode**: The value 0 indicates the transparent transmission mode with the G.711 coding; the value 1 indicates the T.38 mode, which is a coding mode dedicated to the fax service. The default value is 0.
- **flow**: Options are V2, V3, and V5. The default value is V3.
- **is-port+2**: This parameter should be consistent with the T.38 fax port configured on the peer MGC. When **transmode** is T.38 and **flow** is V2, this parameter must be configured.

CAUTION

In the high-speed fax mode, the fax mode cannot be configured as the auto-negotiation (V2 flow) T.38 mode or the self-switch transparent transmission mode. If the fax mode is the auto-negotiation (V2 flow) T.38 mode or the self-switch transparent transmission mode, modify the configuration according to step 1 and step 2.

Step 3 Query the common parameters of the fax and modem or the fax parameter configuration.

1. Run the **display fax-modem parameters** command to query the fax negotiation flow.
2. Run the **display fax parameters** command to query the fax coding mode.

----End

Example

To configure the negotiation mode of the FoIP service on the MA5600T/MA5603T to negotiation, enable 10 ms packetization, enable RFC2198 smart startup mode, configure the event transfer mode of fax to RFC2833, and the fax working mode of the MA5600T/MA5603T to thoroughly, and configure the fax flow to V2 flow, do as follows:

```
huawei(config)#fax-modem parameters negomode selfswitch packet-interval-10ms en
able rfc2198-start-mode enableRfc2198SmartStartup transevent rfc2833
huawei(config)#fax parameters flow v2 workmode thoroughly
huawei(config)#display fax-modem parameters
  -----------------------------------------------------------------------------
  Negomode               : Self switch
  Packet-interval-10ms   : Enable
  Rfc2198-start-mode     : Enable Rfc2198SmartStartup
  TransEvent             : RFC2833
  Vbd-codec              : G.711A
  Vbd-payload-type       : Static
  -----------------------------------------------------------------------------

huawei(config)#display  fax parameters
  -----------------------------------------------------------------------------
  FAX transfers mode                   :Thoroughly
  T38 Fax Port                         :RTP port
  FAX flow                             :V2 Flow
  -----------------------------------------------------------------------------
```

10.4 Configuring the SIP-based FoIP Service

This topic describes how to configure the SIP-based FoIP service.

Prerequisites

- The SIP-based VoIP service must be configured. For details, see **10.2 Configuring the VoIP Service (SIP-based)**.
- The voice service port used for the FoIP service must be in the normal state, and the voice communication on the port must be normal.

Context

According to the fax coding mode, the FoIP service is classified into two modes:

- Transparent transmission fax: uses the G.711 coding
- T.38 fax: uses the T.38 coding

In the fax service application, according to whether the SIP signaling is involved in controlling the transmission, the FoIP service is classified into two modes:

- Negotiate mode, in which the SIP signaling is involved in controlling the transmission
- Self-switch mode, in which the SIP signaling is not involved in controlling the transmission

Data Plan

Before the data configuration, it is recommended that you plan the working mode of the FoIP service on the entire IMS network to ensure that the configurations on the entire network are consistent.

Table 10-16 Fax flows

Item	Flow	Remarks
Coding negotiation mode	Negotiate	The gateway negotiates the coding mode with the IMS through SIP signaling.
	Self-switch	The gateway determines the coding mode to be adopted.
Coding mode	Transparent transmission fax	The G.711 coding mode is adopted.
	T.38 flow	The T.38 coding mode is adopted.

Default Configuration

Table 10-17 lists the default settings of the FoIP flow.

Table 10-17 Default settings of the FoIP flow

Item	Default Setting
Coding negotiation mode	negotiate
Coding mode	Transparent transmission fax

Procedure

Step 1 Configure the common parameters of fax and modem.

1. In the global config mode, run the **interface sip** command to enter the SIP interface mode.
2. In the SIP interface mode, run the **fax-modem parameters negomode** command to configure the coding negotiation mode.

   The purpose of this step is to configure the coding negotiation mode. Key parameter **negomode**: includes the self-switch mode and the negotiate mode. By default, the negotiate mode is adopted.:

Step 2 Configure the fax coding mode.

In the SIP interface mode, run the **fax parameters** command to configure the fax transmission mode. There is only one key parameter, which is described as follows:

transmode: The value 0 indicates the transparent transmission mode with the G.711 coding; the value 1 indicates the T.38 mode, which is a coding mode dedicated to the fax service. By default, the value 0 is adopted.

Step 3 Query the common parameters of the fax and modem or the fax parameter configuration.

1. Run the **display fax-modem parameters** command to query the fax negotiation flow.
2. Run the **display fax parameters** command to query the fax coding mode.

----End

Example

To configure the negotiation mode of the FoIP service on the SIP interface 0 to negotiate, enable 10 ms packetization, configure the RFC2198 negotiate mode to fixed start, RFC2198 start mode to smart2198 start, configure the event transfer mode of fax to fixed start, and the fax working mode to thoroughly, do as follows:

```
huawei(config-if-sip-0)#fax-modem parameters negomode negotiate packet-interval-
10ms enable rfc2198-negomode fixedstart rfc2198-startmode smart2198 transevent f
ixedsta
huawei(config-if-sip-0)#fax parameters transmode 0
huawei(config-if-sip-0)#display fax-modem parameters
 ------------------------------------------------------------------------------
 MGID                  :0
 Nego-mode             :negotiate
 Packet-interval-10ms  :enable
 Rfc2198-nego-mode     :fixedstart
 Rfc2198-start-mode    :smart2198
 Vbd-codec             :G.711A
 Vbd-pt-type           :static
 Transfer-event        :fixedstart
 ------------------------------------------------------------------------------

huawei(config-if-sip-0)#display fax parameters
 ---------------------------------------
 MGID      Transmode
 ---------------------------------------
 0         Thoroughly
 ---------------------------------------
```

10.5 Configuring the MoIP Service

This topic describes how to configure the H.248/MGCP/SIP-based MoIP service for transmitting the traditional narrowband modem data service over the IP network.

Prerequisites

For the H.248/MGCP-based MoIP service:

- The MG interface must be configured. For details, see **10.1.1 Configuring an MG Interface**.
- The VoIP users must be configured. For details, see **10.1.2 Configuring the VoIP User**.

For the SIP-based MoIP service:

- The SIP interface must be configured. For details, see **10.2.1 Configuring an SIP Interface**.
- The VoIP users must be configured. For details, see **10.1.2 Configuring the VoIP User**.

Context

The MoIP service can be transmitted in two modes:

- One is the transparent transmission mode, also called the voice-band data (VBD) transparent transmission. In this mode, the MG adopts the G.711 coding to encode and decode modem signals, and processes modem signals as common RTP data. In other words, the MG does not process modem signals, and the modem modulation signals are transparently transmitted over the IP network through the VoIP channel.
- The other is the redundancy mode, also called the relay mode.

CAUTION

Currently, the MA5600T/MA5603T supports the modem service only in the transparent transmission mode.

The modem event report mode is classified into the delay mode, direct mode, and high-speed signal immediate mode.

- In the delay mode, the MA5600T/MA5603T does not report the modem event immediately after receiving an event. Instead, it waits for a period of time until the event times out and no V21flag event is reported. In this manner, when the high-speed fax machines fail in the high-speed transmission (the modem mode on the host) negotiation, the low-speed transmission mode (the fax mode on the host) can still be used for transmitting data.
- In the direct mode, the MA5600T/MA5603T reports the modem event to the MGC immediately after receiving the event from the drive. To enable the MGC to quickly respond to a modem event, configure the modem event report mode to the direct mode.
- In the high-speed signal immediate mode, the MA5600T/MA5603T reports low-speed modem signals after a delay of 5.5s and reports high-speed modem signals without delay.

The configuration of the MoIP service is mainly the configuration of the modem event report mode and the transmission mode. The default settings are direct mode and transparent transmission mode. If configuration is required, you only need to configure the event report mode. This is because currently the MA5600T/MA5603T supports the modem service only in the transparent transmission mode. Hence, you do not need to configure the transmission mode.

Procedure

- Configure the H.248/MGCP-based modem event report mode.

In the global config mode, run the **modem parameters eventmode** command to configure the modem event report mode. By default, the direct mode is used.

- Configure the SIP-based modem event report mode.
  1. Run the **interface sip** command to enter the SIP interface mode.
  2. (Optional) Run the **modem parameters transmode** command to configure the modem event report mode.

----End

Example

To enable the MA5600T/MA5603T to communicate with the MGC through H.248, and configure the transmission mode of the modem to transparent transmission and the modem event report mode to delay mode, do as follows:

```
huawei(config)#modem parameters eventmode 0
huawei(config)#save
```

10.6 Adding a POTS IP SPC

A semi-permanent connection (SPC) exclusively occupies a voice channel to meet the communication requirements and to ensure the communication quality for particular and vital access subscribers. To configure an IP SPC, configure the data such as the local IP address, local UDP port ID, remote IP address, and remote UDP port ID, and set up a direct IP connection between the two ends of the VoIP service. In this manner, the voice media data can be directly transmitted to the peer end.

Prerequisites

- The electrical switch is already switched to the VoIP daughter board.
- The IP address of the VLAN Layer 3 interface is already configured.
- The remote VLAN Layer 3 interface can be routed and reached from the local VLAN Layer 3 interface.

Procedure

Step 1 Run the **voip** command to enter the VoIP mode.

Step 2 Run the **ip address** command to configure the media IP address for the VoIP service.

Step 3 Run the **quit** command to quit the VoIP mode.

Step 4 Run the **dsp-para-template add** command to configure the DSP parameter profile.

Step 5 Run the **spc** command to enter the SPC mode.

Step 6 Run the **ipspc add** command to add an SPC.

----End

Example

To add a POTS IP SPC with the parameters listed in **Table 10-18**, do as follows:

Table 10-18 Data plan for adding a POTS IP SPC

Item	Data
IP address of the local VLAN Layer 3 interface	192.168.0.10/24
Local UDP port ID	56988
IP address of the gateway	192.168.0.1
Media IP address	192.168.0.10
Remote IP address	192.168.1.100
Remote UDP port ID	56988
DSP parameter profile	● Profile name: **ecopen** ● Status of echo suppression: 0 (enabled) ● Jitter buffer mode: 1 (static mode) ● Non-linear processing mode: 0 (disabled) ● Status of silence compression: 1 (disabled) ● DSP working mode: 0 (voice service)
Subrack ID/slot ID/port ID/ channel ID	0/2/0/0 **NOTE** The channel ID for a PSTN subscriber must be 0.

```
huawei(config)#voip
huawei(config-voip)#ip address media 192.168.0.10 192.168.0.1
huawei(config-voip)#quit
huawei(config)#dsp-para-template add ecopen 0 1 0 1 0
huawei(config)#spc
huawei(config-spc)#ipspc add 0/2/0/0 local-ip 192.168.0.10 local-port 56988 remote-
ip
 192.168.1.100 remote-port 56988 dsp-para-template ecopen
```

10.7 Configuring the R2 Service

With the R2 access technology, the MA5600T/MA5603T provides access services on common twisted pair cables when interconnecting with the PBX using R2 signaling.

Prerequisites

- The signaling type of ports on the EDTB board must be configured as channel associated mode, which can be configured using the **e1port signal** command.
- The working mode of the EDTB board must be configured as voice mode, which can be configured using the **runmode** command.
- The operation mode of the EDTB board must be configured as service mode, which can be configured using the **board workmode** command.

For the H.248-based MoIP service:

- An MG interface has been configured. For details, see **10.1.1 Configuring an MG Interface**.
- A VoIP user has been configured. For details, see **10.1.2 Configuring the VoIP User**.

For the SIP-based MoIP service:

- A SIP interface has been configured. For details, see **10.2.1 Configuring an SIP Interface**.
- A VoIP user has been configured. For details, see **10.1.2 Configuring the VoIP User**.

Context

- R2 signaling is channel associated signaling (CAS), which is international standard signaling based on E1 digital network.
- The MA5600T/MA5603T connects the PBX and NGN network using R2 signaling, achieving transition from the PSTN network to the NGN network.

Procedure

Step 1 Run the **r2 profile** command to add an R2 profile. Define the R2 signaling with a specific feature as an R2 profile which can be used when an R2 user is added.

Step 2 (Optional) Run the **profile attribute** command to configure the signaling type of the R2 profile.

Step 3 (Optional) Configure adaptation data of the R2 profile.

The ITU-T Q.400-Q.490 standard has defined R2 signaling standard, but different countries and regions implement R2 signaling in different ways. You do not need to change parameter values if the parameter values defined in the signaling standard of a country are consistent with the default values defined by the MA5600T/MA5603T. Otherwise, you need to change the parameter values based on actual conditions.

- Run the **address-receive attribute** command to configure the receive attribute of R2 addresses.
- Run the **address-send attribute** command to configure the transmit attribute of R2 addresses.
- Run the **profile attribute** command to configure the signaling type of the R2 profile.
- Run the **line-signaling attribute** command to configure the R2 line signaling attribute.
- Run the **register-signaling attribute** command to configure the R2 register signaling attribute.

Step 4 (Optional) Run the **multi-r2-adapt add** command to add parameters of the state machine of register signaling and line signaling in adaptation profiles for multiple countries. To comply with the R2 standards of different countries, parameter configuration for the R2 state machine is added, so that mappings between logical commands and physical commands can be changed by changing configurations without adding logical commands.

Step 5 Run the **mgr2user add** command (for H.248 protocol) or **sipr2user add** command (for SIP protocol) to add an R2 user.

Step 6 (Optional) Run the **mgr2user attribute set** command (for H.248 protocol) or **sipr2user attribute set** command (for SIP protocol) to set the priority of R2 users. When congestion occurs, packets of the user with a high priority is forwarded first.

----End

Example

For example, configure R2 users at the 0/2/1 port when using SIP protocol. Parameters are shown in **Table 10-19**.

Table 10-19 Data plan for R2 user configuration

Configuration Item	Data
R2 profile	0
Signaling type of the R2 profile	10
Wait-answer-time	200s
Wait-protect-time	300 ms
SIP interface	0
Subrack ID/slot ID/port number	0/2/1
The terminal priority of an R2 user	cat2

```
huawei(config)#r2 profile 0
  Are you sure to add r2 profile?(y/n)[n]:y
huawei(config-r2-0)#profile attribute name normal signaling-type 10
huawei(config-r2-0)#line-signaling attribute wait-answer-time 200 wait-protect-
time 300
huawei(config-r2-0)#quit
huawei(config)#esl user
huawei(config-esl-user)#sipr2user add 0/2/1 0 0
huawei(config-esl-user)#sipr2user attribute set 0/2/1 priority cat2
```

10.8 Configuring the Security and Reliability of the Voice Service

The security configuration of the voice service includes the H.248-based, MGCP-based, or SIP-based device authentication configuration, and the reliability configuration of the voice service includes the dual-homing configuration and the emergency standalone configuration.

10.8.1 Configuring Device Authentication

Device authentication is a method to improve the security of the core network and prevent illegal devices from registering with the core network device.

Configuring Device Authentication (H.248-based)

This topic describes how to configure the H.248-based device authentication to prevent illegal MGs from registering with the MGC.

Prerequisite

- The MG interface must be configured successfully.
- The parameters, including the encryption type, the initial key and the DH authentication, and the MG ID, must be configured on the MGC. These parameters must be the same as the parameters configured on the MA5600T/MA5603T.

Precautions

If Huawei products such as the SoftX3000 is used as the MGC, the authentication MG ID must be a character string with more than eight bits.

Procedure

Step 1 In the global config mode, run the **interface h248** command to enter the MG interface mode.

Step 2 Run the **mg-software parameter 4** command to configure the registration mode.

Step 3 Run the **mg-software parameter 6 0** command to configure the device authentication function on the MG interface.

Step 4 Run the **auth** command to configure the authentication MG ID and the initial key.

Step 5 Run the **display auth** command to query the authentication parameters.

Step 6 Run the **reset coldstart** command to reset the MG interface.

Reset the MG interface to make the MG interface register with the MGC (and to make the modified attributes of the MG interface take effect) so that the MG interface can work in the normal state. The MG interface can be enabled in different ways (see Parameters of the **reset** command). For a newly configured MG interface, enable the MG interface through cold start.

----End

Example

Configure the authentication parameters for the MA5600T/MA5603T as listed in **Table 10-20**.

Table 10-20 Data plan for configuring the H.248-based authentication

Item	Data
MG ID	0
Whether the wildcard is used in the registration	Yes
Authentication MG ID	MA5600T/MA5603T. It must be the same as the authentication MG ID on the MGC. Otherwise, the MG cannot register with the MGC.
Initial key	0123456789ABCDEF. It must be the same as the initial key configured on the MGC.

The following is a configuration example based on the data plan:

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#mg-software parameter 4 0
huawei(config-if-h248-0)#display mg-software parameter 4
  -------------------------------------------------
  Interface Id:0          para index:4   value:0
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
   Interface software parameter name:
   4: Whether MG register to MGC with wildcard
      0: Yes
      1: No
huawei(config-if-h248-0)#mg-software parameter 6 0
huawei(config-if-h248-0)#display mg-software parameter 6
  -------------------------------------------------
  Interface Id:0          para index:6   value:0
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
   Interface software parameter name:
   6: Whether MG support authentication
      0: Yes
      1: No
huawei(config-if-h248-0)#auth auth_mgid MA5600T/MA5603T initial_key
0123456789ABCDEF
huawei(config-if-h248-0)#display auth
 [AUTH_PARA config]
  Initial Key    : 0123456789ABCDEF
  Auth MGid      : MA5600T/MA5603T
  Algorithm      : MD5
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

Configuring Device Authentication (MGCP-based)

This topic describes how to configure the MGCP-based authentication parameters for the MG interface on the MA5600T/MA5603T to implement device authentication and prevent illegal MGs from registering with the MGC.

Prerequisite

- The MG interface must be configured successfully.
- The parameters, including the encryption type, the initial key and the DH authentication, and the MG ID, must be configured on the MGC. These parameters must be the same as the parameters configured on the MA5600T/MA5603T.

Procedure

Step 1 In the global config mode, run the **interface mgcp** command to enter the MG interface mode.

Step 2 Run the **mg-software parameter 4** command to configure the registration mode.

Step 3 Run the **auth** command to configure the authentication MG ID and the initial key.

If Huawei products such as the SoftX3000 is used as the MGC, the authentication MG ID must be a character string with more than eight bits.

NOTE

When the MGCP protocol is used, the MG interface supports two authentication modes:

- Passive authentication mode: In this mode, the device registers with the MGC and is authenticated only after required by the MGC.
- Active authentication mode: In this mode, the device is authenticated when the device registers with the MGC.

In actual applications, you can select the authentication mode according to the requirements.

Step 4 Run the **display auth** command to query the authentication parameters.

Step 5 Run the **reset** command to reset the MG interface.

----End

Example

To configure the authentication parameters for the MA5600T/MA5603T as listed in **Table 10-21**, do as follows:

Table 10-21 Data plan for configuring the MGCP-based device authentication

Item	Data
MG ID	0
Whether the wildcard is used in the registration	Yes
Authentication mode	Active authentication mode
Authentication MG ID	MA5600T/MA5603T. It must be the same as the authentication MG ID on the MGC. Otherwise, the MG cannot register with the MGC.
Initial key	0123456789ABCDEF. It must be the same as the initial key configured on the MGC.

The following is a configuration example based on the data plan:

```
huawei(config)#interface mgcp 0
huawei(config-if-mgcp-0)#mg-software parameter 4 0
huawei(config-if-mgcp-0)#display mg-software parameter 4
  -------------------------------------------------
  Interface Id:0           para index:4   value:0
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
   Interface software parameter name:
   4: Whether MG register to MGC with wildcard
      0: Yes
      1: No
huawei(config-if-mgcp-0)#auth mode2 auth_mgid MA5600T/MA5603T initial_key
0123456789ABCDEF
huawei(config-if-mgcp-0)#display auth
  active request authentication mode config:
  Initial Key    : 0123456789ABCDEF
  Auth MGid      : MA5600T/
```

```
MA5603T
  Algorithm      : MD5
huawei(config-if-mgcp-0)#reset
  Are you sure to reset MG interface?(y/n)[n]:y
```

Configuring Device Authentication (SIP-based)

When the Session Initiation Protocol (SIP) is used, the voice service of the MA5600T/MA5603T supports the authentication for a SIP interface and single user in user name+password or user name+HA1 mode.

Prerequisite

- The SIP interface must be added successfully. For details, see **10.2.1 Configuring an SIP Interface**.
- The authentication information has been configured on the proxy server.

Context

The device authentication requires the support of the IMS side, and the authentication data should be consistent with that of IMS side.

Procedure

- Perform the authentication for a SIP interface.
  1. In the global config mode, run the **interface sip** command to enter the SIP interface mode.
  2. Run the **sip-auth-parameter** command to configure the authentication user name and password for the SIP interface.

     Security authentication information includes password authentication mode, user name, password, and user authentication mode.

     - Password authentication mode includes **password** and **ha1**. In **password** mode, the original user password is configured. In **ha1** mode, a password is generated after the original user password is encrypted by using the message digest 5 (MD5) algorithm.
     - User authentication mode includes **interface** and **single-user**. The **interface** mode indicates that authentication is performed based on interface. This means that all users under an interface share an authentication user name. The **single-user** mode indicates that each user has a unique identity.
  3. Run the **reset** command to reset the SIP interface.
- Perform the authentication for a single user.
  1. In global config mode, run the **esl user** command to enter extend signaling link (ESL) user mode.
  2. According to the service type, run the **sippstnuser auth set** command or the **sipbrauser auth set** command or the **sipprauser auth set** command to configure the authentication user name, password for single user.
  3. Run the **display sippstnuser authinfo** command or the **display sipbrauser authinfo** command or the **display sipprauser authinfo** command to query the security authentication information.

----End

Example

Configure the security authentication information of SIP interface 0 on the MA5600T/MA5603T, where,

- User authentication mode is **interface**
- Password authentication mode is **password**
- User name is **huawei.com**
- Password is **123456789**

```
huawei(config)#interface sip 0
huawei(config-if-sip-0)#sip-auth-parameter auth-mode interface password-mode pas
sword
  User Name(<=64 characters, "-" indicates deletion):huawei.com
  User Password(<=64 characters, "-" indicates deletion):    //Input password
here
  The configuration will take effect after resetting the interface
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
```

Assume that the PSTN user under port 0/2/1 is configured with:

- Telephone number: 88810001
- Authentication password mode: password
- User name: huawei
- Password: huawei123

To configure the authentication data of such a PSTN user, do as follows:

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser auth set 0/2/1 telno 88810001 password-mode
password
  User Name(<=64 characters, "-" indicates deletion):huawei
  User Password(<=64 characters, "-" indicates deletion):    //Input password here
```

10.8.2 Configuring Inner Standalone (Based on H.248/SIP Protocol)

This topic describes how to configure the inner standalone. After the inner standalone is configured, the internal phones can call each other using the internal extension numbers even if the interface between the gateway and the softswitch is interrupted.

Context

- The MG interface supports the inner standalone function only when it uses the H.248 protocol.
- When the MG interface works in the inner standalone state, only the internal users of the MG interface can communicate in the normal state.
- To maintain the same user phone number in the standalone state as the one used in normal condition, configure the phone number on the MG to be the same as that on the MGC.

Prerequisite

- The voice service users are configured properly on the H.248/SIP interface and the users can call each other successfully.

- The user phone number of the H.248 interface/SIP interface is configured to be the same as that on the softswitch. (Command: **mgpstnuser modify** (H.248 interface)/**sippstnuser modify** (SIP interface)).

Procedure

- Configure inner standalone (based on H.248 protocol)
  1. Run the **mg-software parameter 11 1** command to configure the MG interface to support the inner standalone function.
  2. Run the **digitmap set inner** command to configure the internal digitmap.

     NOTE

     The configured digitmap should correspond to the user phone number.
  3. (Optional) Run the **standalone parameters** command to configure the inner standalone timers.
     - The inner standalone timers include the dial tone timer (default: 10s), the busy tone timer (default: 40s), and the ringing tone timer (default: 50s).
     - Generally, the default inner standalone timers can be used.
- Configure inner standalone (based on SIP protocol)
  1. Run the **mg-software parameter 2 1** command to configure the SIP interface to support the inner standalone function.

     By default, the SIP inner standalone function is disabled.
  2. (Optional) Run the **local-digitmap add** command to add a digitmap used in SIP inner standalone.

     The system has a digitmap named **defaultnormal**, which can match any phone numbers. Therefore, a new digitmap does not need to be added unless otherwise required.

----End

Example

Assume that an incoming third-party call will interrupt the inner standalone call after the communication between MG 0 and the MGC recovers. To configure MG 0 to support the inner standalone, and set the internal digitmap to 1234xxxx, do as follows:

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#mg-software parameter 11 1
huawei(config-if-h248-0)#display mg-software parameter 11
  -------------------------------------------------
  Interface Id:0          para index:11  value:1
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
   Interface software parameter name:
   11: Stand alone support
       0: None
       1: Inner
       2: Emergency
       3: Both
huawei(config-if-h248-0)#digitmap set inner 1234xxxx
huawei(config-if-h248-0)#display digitmap
  ----------------------------------------------------------------------------
  Inner digitmap                                        : 1234xxxx
  Emergency digitmap                                    : -
  Urgent digitmap (for overload or bandwidth restrict)   : -
  Dualdial digitmap for card service                     : -
  -----------------------------------------------------------------------------
```

To configure SIP interface 0 to support the inner standalone (so that the internal phones whose numbers belong to the number segment of 07552856xxxx can call each other, if the communication between SIP interface 0 and the softswitch is interrupted), do as follows:

```
huawei(config)#display local-digitmap name defaultnormal

  Command:
          display local-digitmap name defaultnormal
  ------------------------------------------
  Name: defaultnormal
  Type: normal
  Body: x.S|Exx.S       //can match any phone numbers
  ------------------------------------------
huawei(config)#interface sip 0
huawei(config-if-sip-0)#mg-software parameter 2 1
huawei(config-if-sip-0)#display mg-software parameter 2
  -------------------------------------------------
  MGID:0           para index:2   value:1
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
 Parameter Index:  Interface software parameter name:
    2 : SAL Support
        0: No
        1: Yes
```

10.8.3 Configuring the Dual Homing (Multi-Homing)

This topic describes how to configure the H.248-based, MGCP-based, and SIP-based dual homing (multi-homing). Dual homing (multi-homing) is a measure that protects the softswitch against a crash and a disaster recovery mechanism against accidents (such as a fire in the telecommunications room, disconnection of the cable connected to the telecommunications room, and abnormal power supply).

Context

The working principle of multi-homing is as follows: an MG interface (for H.248 and MGCP) or a SIP interface is homed to multiple registration servers. If the primary server malfunctions, the interface is switched to a secondary server and then continues to provide services.

Dual homing is one type of multi-homing configured with only primary/secondary servers without a disaster-recovery server.

Configuring H.248-based Dual Homing (Multi-homing)

In the case of H.248, the MA5600T/MA5603T supports homing of a media gateway (MG) interface to the primary/secondary media gateway controllers (MGCs) and disaster-recovery MGC. When the primary MGC malfunctions, the MG interface will register with the secondary MGC and then the disaster-recovery MGC cyclically.

Context

Technically speaking, dual homing is a configuration in which an MG is homed to the primary MGC and secondary MGC. Multi-homing is a configuration in which an MG is homed to the primary MGC, secondary MGC, and disaster-recovery MGC. Multi-homing is an enhancement of dual homing. In a broad sense, dual homing is one type of multi-homing.

The MA5600T/MA5603T provides different application policies for the dual homing (multi-homing) by configuring MG homing parameters and MG software parameters.

Procedure

Step 1 Create an MG interface and configure MG interface parameters.

1. In the global config mode, run the **interface h248** command to enter the MG interface mode.
2. Run the **if-h248 attribute** command to create an MG interface and then configure the primary/secondary MGCs and disaster-recovery MGC.

   When configuring an MG interface supporting dual homing, note that:

   - The MG is dual homed to the primary/secondary MGCs. The configurable parameters include **secondary-mgc-ip1** *secondary-mgc-ip1*, **secondary-mgc-ip2** *secondary-mgc-ip2*, **secondary-mgc-port** *secondary-mgc-port*, or **mgc-domain-name2** *mgcdomainname2*.
   - At least one secondary MGC (containing the IP address and port ID) is configured.

   When configuring an MG interface supporting multi-homing, note that:

   - A disaster-recovery MGC is configured based on the dual homing. The configurable parameters include **stand-alone-mgc-ip1** *stand-alone-mgc-ip1*, **stand-alone-mgc-ip2** *stand-alone-mgc-ip2*, and **stand-alone-mgc-port** *stand-alone-mgc-port*.
   - At least one disaster-recovery MGC (containing the IP address and port ID) is configured.

   For details about how to configure an MG interface, see **10.1.1 Configuring an MG Interface**.

Step 2 Configure the software parameters of an MG interface.

1. Run the **mg-software parameter 2** command to configure the MG interface supporting dual homing.

   The values of **mg-software parameter 2** are described as follows:

   - When the value of **mg-software parameter 2** is **0** (default value), multi-homing is not supported. Specifically, after an MG interface is unable to register with the primary MGC, the MG interface does no initiate registration with the secondary MGC or disaster-recovery MGC though it has been configured.
   - When the value of **mg-software parameter 2** is **1**, multi-homing is supported but auto-switching is not supported. Specifically,
     - An MG interface registering with the primary MGC will register with the secondary MGC and then the disaster-recovery MGC cyclically when the primary MGC malfunctions.
     - After the primary MGC recovers, the secondary MGC or disaster-recovery MGC will not automatically switch back to the primary MGC. Run the **mgc switch (h.248)** command to forcibly switch the MGC to the primary MGC.
   - When the value of **mg-software parameter 2** is **2**, multi-homing and auto-switching are supported. Specifically,
     - An MG interface registering with the secondary MGC will automatically switch to the primary MGC after the primary MGC recovers.

  - An MG interface registering with the disaster-recovery MGC will automatically switch to the primary or secondary MGC after the primary or secondary MGC recovers.

CAUTION

After an MG interface is manually or automatically switched, the MG interface will restart, causing services interrupted for a short time.

2. (Optional) Run the **mg-software parameter 36** command to configure the registration interval during MGC's multi-homing registration switchover.

   This parameter is used to configure the switch interval when an MGC (primary MGC, secondary MGC, or disaster-recovery MGC) malfunctions and switches to another MGC. It is defaulted to 40s.
3. Run the **display mg-software parameter** command to query the software parameters of the MG interface.

----End

Example

To configure dual homing on MG interface 0 with the following settings, do as follows:

- The IP address of the primary MGC is 192.168.0.10 and the port number for the transport layer protocol is 2944.
- The IP address of the secondary MGC is 192.168.0.20 and the port number for the transport layer protocol is 2944.
- Auto-switching is not supported.

```
huawei(config)#interface h248 0
huawei(config-if-h248-0)#if-h248 attribute primary-mgc-ip1 192.168.0.10 primary-
mgc-port 2944 secondary-mgc-ip1 192.168.0.20 secondary-mgc-port 2944
huawei(config-if-h248-0)#mg-software parameter 2 1
huawei(config-if-h248-0)#display mg-software parameter 2
  ------------------------------------------------
  Interface Id:0          para index:2   value:1
  ------------------------------------------------
 APPENDIX:
  ------------------------------------------------
   Interface software parameter name:
   2: Whether MG support multi-home function
      0: Do not support the multi-homing
      1: Support the multi-homing, but do not support the auto switchover
      2: Support the multi-homing and auto switchover
```

To configure dual homing on MG interface 1 with the following settings, do as follows:

- The IP address of the primary MGC is 192.168.0.10 and the port number for the transport layer protocol is 2944;
- The IP address of the secondary MGC is 192.168.0.20 and the port number for the transport layer protocol is 2944;
- The IP address of the disaster-recovery MGC is 192.168.0.30 and the port number for the transport layer protocol is 2945;
- Auto-switching is supported.

```
huawei(config)#interface h248 1
huawei(config-if-h248-1)#if-h248 attribute primary-mgc-ip1 192.168.0.10 primary-
```

```
mgc-port 2944 secondary-mgc-ip1 192.168.0.20 secondary-mgc-port 2944 stand-alone
-mgc-ip1 192.168.1.30 stand-alone-mgc-port 2945
huawei(config-if-h248-1)#mg-software parameter 2 2
huawei(config-if-h248-1)#display mg-software parameter 2
  -------------------------------------------------
  Interface Id:1          para index:2   value:2
  -------------------------------------------------
 APPENDIX:
  -------------------------------------------------
   Interface software parameter name:
   2: Whether MG support multi-home function
      0: Do not support the multi-homing
      1: Support the multi-homing, but do not support the auto switchover
      2: Support the multi-homing and auto switchover
```

Configuring MGCP-based Dual Homing

This topic describes how to configure the MGCP-based dual homing.

Context

The MA5600T/MA5603T supports registering with three MGCs (MGC1, MGC2, and MGC3) through the MG interface. MGC1 serves as the primary MGC. When MGC1 fails, the MG can switch to MGC2 and continue working. When MGC2 also fails, the MG can switch to MGC3 and continue working.

Prerequisite

- MGC1 and MGC2 must be configured in the attributes of the MG interface.
- On the MGCs, the data for interconnecting with the MG must be configured.

Procedure

Step 1 In the global config mode, run the **interface mgcp** command to enter the MG interface mode.

Step 2 Run the **mg-software parameter 3 1** command to enable the heartbeat message function.

Step 3 Run the **mg-software parameter 2 0** command to configure the MG interface to support dual homing.

----End

Example

To configure MG interface 0 to support dual homing and enable the heartbeat message function, do as follows:

```
huawei(config)#interface mgcp 0
huawei(config-if-mgcp-0)#mg-software parameter 3 1
huawei(config-if-mgcp-0)#mg-software parameter 2 0
```

Configuring the SIP-based Dual Homing

the MA5600T/MA5603T supports the 1+1 mutual assistance mode (the active/standby mode) of the upstream proxy devices. When either of the upstream active/standby devices is faulty, the MA5600T/MA5603T automatically switches the service to the other device. In this way, the disaster recovery solution is implemented through SIP to improve the access reliability of the device.

Context

The MA5600T/MA5603T supports the SIP interface homing to two proxy servers (Proxy1 and Proxy2), where Proxy1 functions as the primary proxy server. When Proxy1 fails, the MG can switch to Proxy2 to continue working.

Prerequisite

- The data for interconnecting with the SIP interface must be configured on the IMS.
- When configuring the IP address of the SIP interface, make sure that the IP address (signaling IP address or media IP address) exists in the corresponding IP address pool.

Procedure

Step 1 In the global config mode, run the **interface sip** command to enter the SIP interface mode.

Step 2 Run the **if-sip attribute basic** command to configure the basic attributes of the SIP interface.

To support dual homing, the information about the secondary proxy server must be specified here. A proxy server can be identified by its IP address or domain name.

Step 3 Run the **reset** command to reset the interface.

----End

Example

Assume that the SIP interface ID is 0, the media IP address is 10.10.10.13, signaling IP address is 10.10.10.13, transfer protocol is UDP, and UDP port number is 5000; IP address 1 of the primary proxy server is 10.10.10.14, and port number of the primary proxy server is 5060; IP address 1 of the secondary proxy server is 10.10.10.15, and port number of the secondary proxy server is 5060; the homing domain name **huawei.com**, and profile ID is 1. To configure the dual homing attributes of SIP interface 0, do as follows:

```
huawei(config)#interface sip 0
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.13
signal-ip 10.10.10.13 signal-port 5000 transfer udp primary-proxy-ip1
10.10.10.14 primary-proxy-port 5060 primary-proxy-domain proxy.domain
secondary-proxy-ip1 10.10.10.15 secondary-proxy-port 5060
huawei(config-if-sip-0)#if-sip attribute basic home-domain huawei.com sipprofile
-index 1
huawei(config-if-sip-0)#reset
```

11 Configuring the P2P Optical Fiber Access Service

About This Chapter

Point-to-point (P2P) optical access means the point-to-point FTTx access based on the combination between its P2P optical access board and the ONUs. So as to satisfy the users' requirements for the next generation access equipment which integrates video, voice, and data services.

Users connected to the OLT through an ONT, and are therefore provided with the Internet, VoIP, and IPTV service through a same port.

MDUs are subtended to an OLT through the OPGD board, thereby saving upstream optical fibers and simplifying the network and service configuration.

11.1 Configuring the FTTH P2P Optical Fiber Access Service (Single-Port for Multiple Services)

Users connected to the OLT through an ONT, and are therefore provided with the Internet, VoIP, and IPTV service through a same port.

Service Requirements

- ONT_1 and ONT_2 are provided with the triple play service through FTTH.
- The Internet access service is provided in the PPPoE access mode.
- The IPTV user connected to ONT_1 can watch all the programs, and the IPTV user connected to ONT_2 can watch only program BTV-1.
- The VoIP service and the IPTV service are provided in the DHCP mode and obtain IP addresses from the DHCP server in the DHCP option-60 mode.
- After receiving different traffic streams, the OLT provides different QoS guarantees to the traffic streams according to the priorities of the traffic streams.
- Traffic streams are differentiated on the OLT by the user-side VLAN (C-VLAN).

Figure 11-1 Example network of the optical fiber access service in the single-port for multiple services mode

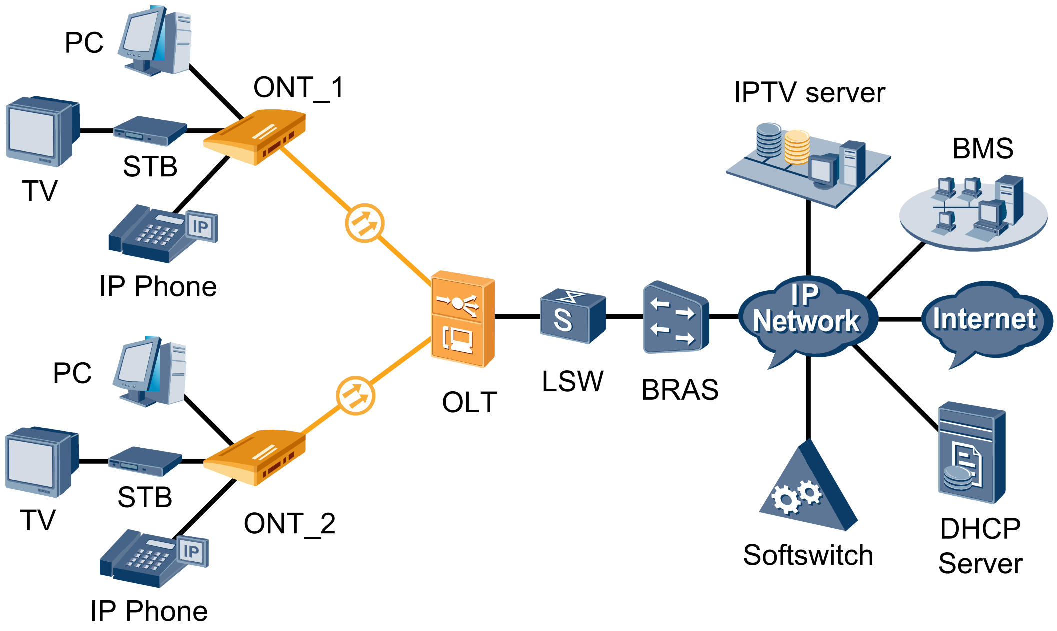


Table 11-1 Data plan for configuring the VLANs

Configuration Item	Data Item	Data
SVLAN	HSI service	SVLAN: 100 CVLAN: 2

Configuration Item	Data Item	Data
	IPTV service	SVLAN: 1000 CVLAN: 4
	VoIP service	SVLAN: 200 CVLAN: 3
IPTV service data	Multicast protocol	IGMP proxy
	Multicast version	IGMP V3
	Configuration mode of the multicast program	Static configuration mode
	IP address of the multicast server	10.10.10.10
	Multicast DHCP server group	20.2.2.2 20.2.2.3
	Multicast program	BTV-1: 224.1.1.10 BTV-2: 224.1.1.20
QoS (priority)	HSI service	Priority: 1; queue scheduling: WRR
	IPTV service	Priority: 4; queue scheduling: WRR
	VoIP service	Priority: 5; queue scheduling: PQ
VoIP service data	VoIP DHCP server group	20.1.1.2 20.1.1.3

Prerequisite

- The OLT is connected to the upper-layer devices such as the BRAS, multicast server, SoftX3000, and DHCP server.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The OLT uses the OPFA board or the OPGD board to connect to the ONT.

Procedure

- Configure the Internet access service on the OLT.
  1. Create a VLAN and add an upstream port to the VLAN.

     The VLAN ID is 100, and the VLAN is a smart VLAN. The upstream port is 0/19/0.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#port vlan 100 0/19 0
     ```

2. Configure a traffic profile.

   Because the VoIP, IPTV, and Internet access services are provided through the same port, you must set the 802.1p priority of each service. Generally, the priorities are in a descending order for the VoIP service, IPTV service, and Internet access service. In this example, set the traffic profile index to 7 and the priority of the Internet access service to 1.

   ```
   huawei(config)#traffic table ip index 7 cir 10240 priority 1 priority-
   policy
    local-Setting
   ```

3. Configure a service port.

   Add a service port to the VLAN and use traffic profile 7. The user-side VLAN ID is 2.

   ```
   huawei(config)#service-port vlan 100 eth 0/5/2 multi-service user-vlan 2
    rx-cttr 7 tx-cttr 7
   huawei(config)#service-port vlan 100 eth 0/5/3 multi-service user-vlan 2
   rx-cttr
    7 tx-cttr 7
   ```

4. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   NOTE

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6
   6
    cos7 7
   ```

   NOTE

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

5. Save the data.

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

- Configure the VoIP service on the OLT.

  1. Create a VLAN and add an upstream port to the VLAN.

     The VLAN ID is 200, and the VLAN is a smart VLAN. The upstream port is0/19/0.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. Configure a traffic profile.

     The traffic profile index is 8, and the 802.1p priority of the VoIP service is 6.

     ```
     huawei(config)#traffic table ip index 8 cir 10240 priority 6 priority-
     policy
      local-Setting
     ```

  3. Configure a service port.

     Add a service port to the VLAN and use traffic profile 8. The user-side VLAN ID is 3.

     ```
     huawei(config)#service-port vlan 200 eth 0/5/2 multi-service user-vlan 3
      rx-cttr 8 tx-cttr 8
     ```

```
huawei(config)#service-port vlan 200 eth 0/5/3 multi-service user-vlan 3
 rx-cttr 8 tx-cttr 8
```

4. Configure the DHCP relay.

   The VoIP service and the IPTV service are provided in the DHCP mode. The DHCP option 60 domain is used to differentiate service types.

   - The DHCP domain of the VoIP service is **voice**.
   - The IP addresses of VoIP DHCP server group 1 are 20.1.1.2 and 20.1.1.3.
   - The IP address of the Layer 3 interface of VLAN 200 is 10.1.1.1/24.
   - The gateway IP address of the DHCP domain is 10.1.1.1/24.

```
huawei(config)#dhcp mode layer-3 option-60
huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1.3
huawei(config)#dhcp domain voice
huawei(config-dhcp-domain-voice)#dhcp-server 1
huawei(config-dhcp-domain-voice)#quit
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 10.1.1.1 24
huawei(config-if-vlanif200)#dhcp domain voice gateway 10.1.1.1
huawei(config-if-vlanif200)#quit
```

   NOTE

   The DHCP option 60 domain of the Ethernet phone (Ephone) varies with the terminal type. In the actual configuration, see the operation instructions of the Ephone.

5. Save the data.

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

- Configure the IPTV service on the OLT.

1. Create a VLAN and add an upstream port to the VLAN.

   The VLAN ID is 1000, and the VLAN is a smart VLAN. The upstream port is0/19/0.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

2. Configure a traffic profile.

   The traffic profile index is 9, and the 802.1p priority of the IPTV service is 5.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-
policy
 local-Setting
```

3. Configure a service port.

   Add a service port to the VLAN and use traffic profile 9. The user-side VLAN ID is 4.

```
huawei(config)#service-port 200 vlan 1000 eth 0/5/2 multi-service user-
vlan 4
 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 300 vlan 1000 eth 0/5/3 multi-service user-
vlan 4
 rx-cttr 9 tx-cttr 9
```

4. Configure the DHCP relay.

   The VoIP service and the IPTV service are provided in the DHCP mode. The DHCP option 60 domain is used to differentiate service types.

   - The DHCP domain of the IPTV service is **video**.
   - The IP addresses of IPTV DHCP server group 2 are 20.2.2.2 and 20.2.2.3.
   - The IP address of the Layer 3 interface of VLAN 1000 is 10.2.2.1/24.
   - The gateway IP address of the DHCP domain is 10.2.2.1/24.

```
huawei(config)#dhcp mode layer-3 option-60
huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
huawei(config)#dhcp domain video
huawei(config-dhcp-domain-video)#dhcp-server 2
huawei(config-dhcp-domain-voice)#quit
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 10.2.2.1 24
huawei(config-if-vlanif1000)#dhcp domain video gateway 10.2.2.1
huawei(config-if-vlanif1000)#quit
```

NOTE

The DHCP option 60 domain of the set-top box (STB) varies with the terminal type. In the actual configuration, see the operation instructions of the STB.

5. Create a multicast VLAN and select the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

6. Set the IGMP version.

   Set the IGMP version of the multicast VLAN to IGMP v3.

```
huawei(config-mvlan1000)#igmp version v3
```

7. Add an IGMP upstream port.

   The IGMP upstream port is port 0/19/0 and works in the default mode, and protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

8. (Optional) Set the multicast global parameters.

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

9. Configure the program library.

   Configure the program names to BTV-1 and BTV-2, multicast IP addresses of the programs to 224.1.1.10 and 224.1.1.20, and source IP address of the programs to 10.10.10.10.

```
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp program add name BTV-1 ip 224.1.1.10
sourceip
 10.10.10.10
huawei(config-mvlan1000)#igmp program add name BTV-2 ip 224.1.1.20
sourceip
 10.10.10.10
```

10. Configure the right profile.

    Configure the profile name to profile0, with the right of watching program BTV-1.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
```

11. Configure the multicast users.

    Add service ports 200 and 300 as multicast users.

```
huawei(config-btv)#igmp user add service-port 200 no-auth
huawei(config-btv)#igmp user add service-port 300 auth
huawei(config-btv)#igmp user bind-profile service-port 300 profile-name
profile0
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 200
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 300
huawei(config-mvlan1000)#quit
```

12. Save the data.

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

----End

Result

After the related upstream device and downstream device are configured, the triple play service (Internet, VoIP, and IPTV services) is available.

- The Internet user can access the Internet in the PPPoE mode.
- The VoIP user can make and receive phone calls.
- The IPTV user connected to port 0/5/2 can watch all the programs, and the IPTV user connected to port 0/5/3 can watch only program BTV-1.

Configuration File

Internet service:

```
vlan 100 smart
port vlan 100 0/19 0
traffic table ip index 7 cir 10240 priority 1 priority-policy local-Setting
service-port vlan 100 eth 0/5/2 multi-service user-vlan 2 rx-cttr 7 tx-cttr 7
service-port vlan 100 eth 0/5/3 multi-service user-vlan 2 rx-cttr 7 tx-cttr 7
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

VoIP service:

```
vlan 200 smart
port vlan 200 0/19 0
traffic table ip index 8 cir 10240 priority 6 priority-policy local-Setting
service-port vlan 200 eth 0/5/2 multi-service user-vlan 3 rx-cttr 8 tx-cttr 8
service-port vlan 200 eth 0/5/3 multi-service user-vlan 3 rx-cttr 8 tx-cttr 8
dhcp mode layer-3 option-60
dhcp-server 1 ip 20.1.1.2 20.1.1.3
dhcp domain voice
dhcp-server 1
quit
interface vlanif 200
ip address 10.1.1.1 24
dhcp domain voice gateway 10.1.1.1
quit
save
```

IPTV service:

```
vlan 1000 smart
port vlan 1000 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 200 vlan 1000 eth 0/5/2 multi-service user-vlan 4 rx-cttr 9 tx-cttr 9
service-port 300 vlan 1000 eth 0/5/3 multi-service user-vlan 4 rx-cttr 9 tx-cttr 9
dhcp mode layer-3 option-60
dhcp-server 2 ip 20.2.2.2 20.2.2.3
dhcp domain video
dhcp-server 2
quit
interface vlanif 1000
ip address 10.2.2.1 24
dhcp domain video gateway 10.2.2.1
quit
multicast-vlan 1000
igmp mode proxy
y
igmp uplink-port
igmp program add name BTV-1 ip 224.1.1.10 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.20 sourceip 10.10.10.10
btv
igmp uplink-port-mode default
y
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name BTV-1 watch
igmp user add service-port 200 no-auth
igmp user add service-port 300 auth
igmp user bind-profile service-port 300 profile-name profile0
multicast-vlan 1000
igmp multicast-vlan member service-port 200
igmp multicast-vlan member service-port 300
quit
save
```

11.2 Configuring MDUs Subtended to an OLT

MDUs are subtended to an OLT through the OPGD board, thereby saving upstream optical fibers and simplifying the network and service configuration.

Service Requirements

- MDU_1 and MDU_2 are connected to an OLT through GE subtending, implementing the Internet access service.
- The Internet access service is provided in the PPPoE dialing mode.

Figure 11-2 Network of MDUs subtended to an OLT

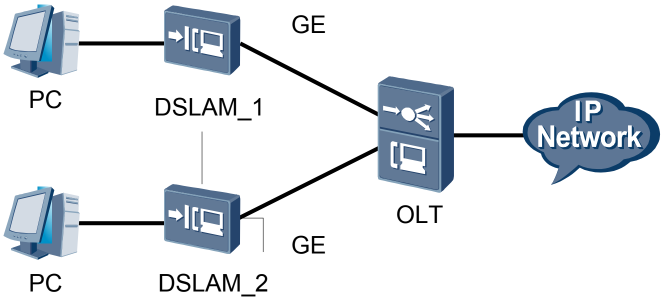


Table 11-2 Data plan

Item	Data
OLT	SVLAN ID: 100 SVLAN type: smart VLAN
	CVLAN ID: 200
	Upstream port: 0/19/0
MDU_1	SVLAN ID: 200 SVLAN type: smart VLAN
	Upstream port: 0/0/1 **NOTE** The upstream ports vary with MDU type.

Item	Data
MDU_2	SVLAN ID: 200 SVLAN type: smart VLAN
	Upstream port: 0/0/1

Procedure

- Configure the OLT.
  1. Configure the port role.

     Configure the port role of the OPGD board as a subtending port. The port roles of the OPGD board are user port and subtending port. By default, the port role is user port.

     ```
     huawei(config)#interface opg 0/2
     huawei(config-if-opg-0/2)#network-role cascade
     huawei(config-if-opg-0/2)#quit
     ```
  2. Create a VLAN and add an upstream port to the VLAN.

     Create smart SVLAN 100. The upstream port is port 0/19/0.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#port vlan 100 0/19 0
     ```
  3. Configure a service port.

     Add the service port to the SVLAN by using default traffic profile 6. The CVLAN ID is 200, the same as the upstream VLAN ID of the MDU. MDU_1 and MDU_2 are connected to ports 0/2/0 and 0/2/1 of the OLT respectively.

     ```
     huawei(config)#service-port vlan 100 eth 0/2/0 multi-service user-vlan
     200
      rx-cttr 6 tx-cttr 6
     huawei(config)#service-port vlan 100 eth 0/2/1 multi-service user-vlan
     200
      rx-cttr 6 tx-cttr 6
     ```
  4. Save the data.

     ```
     huawei(config)#save
     ```
- Configure the MDUs.

  The configurations of MDU_1 and MDU_2 are the same. The configuration of MDU_1 is used as an example.
  1. Create a VLAN and add an upstream port to the VLAN.

     Create smart SVLAN 200. The upstream port is port 0/0/1.

     NOTE

     The SVLAN of the MDU must be the same as the CVLAN of the OLT.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/0 1
     ```
  2. Configure a service port.

     According to actual conditions, an MDU supports multiple access modes. In this example, the ethernet port 0/3/1 is used. For other access modes, see the corresponding configuration guide of the MDU.

     ```
     huawei(config)#service-port vlan 200 eth 0/3/1 multi-service user-vlan
     untagged
      rx-cttr 6 tx-cttr 6
     ```
  3. Save the data.

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

----End

Result

On the PC, the Internet access service is provided in the PPPoE dialing mode.

Configuration File

Configure the OLT:

```
interface opg 0/2
network-role cascade
quit
vlan 100 smart
port vlan 100 0/19 0
service-port vlan 100 eth 0/2/0 multi-service user-vlan 200 rx-cttr 6 tx-cttr 6
service-port vlan 100 eth 0/2/1 multi-service user-vlan 200 rx-cttr 6 tx-cttr 6
save
```

Configure the MDU:

```
vlan 200 smart
port vlan 200 0/0 1
service-port vlan 200 eth 0/3/1 multi-service user-vlan untagged rx-cttr 6 tx-cttr
6
save
```

12 Configuring MPLS and PWE3

About This Chapter

The Multi-protocol Label Switching (MPLS) network adopts the standard packet switching mode to forward Layer 3 packets and the label switching mode to exchange Layer 2 packets. Pseudo Wire Emulation Edge to Edge (PWE3) uses MPLS to carry Layer 2 services so that packets can smoothly traverse the MPLS area and users or services can be differentiated.

Context

MPLS resides between the data link layer and the network layer in the TCP/IP protocol stack. The label in a short fixed length is used to encapsulate IP packets. On the data plane, fast label forwarding is implemented. On the control plane, MPLS can meet the requirements on the network from various new applications with the help of the powerful and flexible routing functions of the IP network.

The MPLS feature includes the following sub-features:

- Basic MPLS functions.
- MPLS RSVP-TE.
- MPLS OAM.

PWE3 is a technology used to emulate ATM, frame relay, Ethernet and SONET/SDH services in packet switched network (PSN). After processing various services from the access layer, the provider edge (PE) creates the PWE3 service, which can be carried on the IP or MPLS network in a unified manner.

According to the emulation service type, MA5600T/MA5603T supports the following types of PWE3:

- TDM PWE3.

  TDM PWE3 is a mechanism that emulates the basic behaviors and characteristics of the TDM circuit service in the PSN to enable the PSN to carry the TDM service.
- ETH PWE3

  ETH PWE3 uses user Ethernet frames as payload, encapsulates the frames through PWE3, and sends them to the PSN. In the downstream direction, ETH PWE3 terminates the PW encapsulation of Ethernet frames and forwards them to the user device.

- ATM PWE3

  ATM PWE3 uses user ATM cells as payload, encapsulates the frames through PWE3, and sends them to the PSN. In the downstream direction, ETH PWE3 terminates the PW encapsulation of ATM cells and forwards them to the user device.

12.1 Configuring the MPLS Service
This topic describes the MPLS technology and how to configure the MPLS service on the MA5600T/MA5603T.

12.2 Configuring the PWE3 Private Line Service
Pseudo wire emulation edge-to-edge (PWE3) uses LDP or RSVP-TE as the signaling protocol and carries various Layer 2 services of the customer edge (CE) over the MPLS LSP or TE tunnel, transparently transmitting the Layer 2 data of the CE.

12.1 Configuring the MPLS Service

This topic describes the MPLS technology and how to configure the MPLS service on the MA5600T/MA5603T.

Basic concept

- The path that an FEC traverses in an MPLS network is called LSP. The LSP, whose function is the same as the virtual circuit in ATM and frame relay, is a unidirectional path from the ingress to the egress. Each node on the LSP is an LSR.
- The static LSP is the label forwarding path manually set up for label distribution to each FEC.
- The dynamic LSP is the label forwarding path dynamically established through the label distribution protocol (LDP or RSVP-TE).

Configuration logic

In the MPLS configuration, the core is to configure the LSP and the second is to configure fault detection and protection for the LSP. At the same time, According to the protocol for creating LSPs, LSPs are categorized as static LSP, LDP LSP, and RSVP-TE LSP.

Therefore, configure MPLS as follows:

1. Configure LSPs.
   - Configure a static LSP.
   - Configure an LDP LSP.
   - Configure an RSVP-TE LSP.
2. Configure LSP protection. Configure the MPLS OAM.

12.1.1 Configuring the Static LSP

Static LSP is configured manually. A static LSP can work in the normal state only when all the LSRs along the static LSP are configured.

Prerequisites

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The global MPLS, VLAN MPLS, and VLAN interface MPLS must be enabled.
4. A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).

Context

The administrator needs to manually distribute labels to each LSR when configuring the static lsp. Principle: The out label value of a node must be equal to the in label value of its next node. LSRs on a static LSP cannot perceive the entire LSP. Therefore, static LSP is a local concept.

The MA5600T/MA5603T can function as a label switching edge router (LER) or a label switching router (LSR). According to the position of the LER or LSR in a network, the configuration of the static LSP involves the ingress configuration, transit node configuration, and egress configuration.

An LSP corresponds to a unidirectional forwarding path. To ensure bidirectional communication of the MPLS service, two static LSPs are required. The two LSPs have opposite directions. Their ingress and egress are reverse. Their transit nodes can be the same or different according to the networking requirements, or even free of being configured.

Procedure

- When the MA5600T/MA5603T functions as an LER, configure the static LSP as follows:
  1. Run the **static-lsp ingress** command to configure the ingress parameters of a static LSP.

     An LER is generally located at the edge of an MPLS network. The PE or PTN device can be considered an LER.

     Format:

     static-lsp ingress { *lsp-name* | **tunnel-interface tunnel** *tunnel-id* } **destination** *ip-addr* **nexthop** *ip-addr* **out-label** *out-label*

     – You can create a static LSP by using the LSP name or the tunnel. To create a static LSP by using the tunnel, you must run the **interface tunnel** command to create a tunnel interface and then configure its attributes.

     – **destination** *ip-addr*: Indicates the destination IP address of the LSP, that is, the loopback interface IP address of the PE or PTN device.

     – **nexthop** *ip-addr*: Indicates the next hop IP address, that is, the VLAN interface IP address of the adjacent LSR.

     – **out-label** *out-label*: Indicates the out label value, which must be the same as the in label value of the downstream LSR.
  2. Run the **static-lsp egress** command to configure the egress parameters of a static LSP.

     Format:

     static-lsp egress *lsp-name* **incoming-interface vlanif** *vlanid* **in-label** *in-label*[**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*]

     – In the egress configuration of a static LSP, only a VLAN interface can be used as the ingress interface.

     – **in-label** *in-label*: Indicates the in label value of the egress, which must be the same as the out label value of the upstream LSR.
  3. Run the **display mpls static-lsp** command to query the configuration of a static LSP.
- When the MA5600T/MA5603T functions as an LSR, configure the static LSP as follows:
  1. Run the **static-lsp transit** command to configure the transit node parameters of a static LSP.

     An LSR is generally located in the middle of an MPLS network. The P device can be considered an LSR that forwards MPLS labels.

     Format:

     static-lsp transit *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* **nexthop** *next-hop-address* **out-label** *out-label*

- The ingress interface of the transit node on a static LSP can only be the VLAN interface, that is, the VLAN interface of the upstream egress.
- **in-label** *in-label*: Indicates the in label value of the transit node, which must be the same as the out label value of the upstream ingress.
- **nexthop** *next-hop-address*: Indicates the next hop IP address, that is, the VLAN interface IP address of the adjacent LSR.
- **out-label** *out-label*: Indicates the out label value of the transit node, which must be the same as the in label value of the downstream LSR.

⚠ **CAUTION**

Because the LSP is unidirectional, you must configure the transit node parameters twice with opposite directions to ensure bidirectional communication of the MPLS service.

2. Run the **display mpls static-lsp** command to query the configuration of a static LSP.

----End

Example

When the MA5600T/MA5603T functions as an LER, to configure the ingress and egress of a static LSP, set the parameters as follows:

- Ingress node name of the static LSP: lsp1; egress name of the static LSP: lsp2
- IP address of local VLAN interface 100: 100.1.1.2/24
- Destination IP address of the LSP: 3.3.3.3/32
- Out label: 8200; in label: 8300
- Next hop IP address: 100.1.1.3

```
huawei(config)#static-lsp ingress lsp1 destination 3.3.3.3 32 nexthop 100.1.1.3
out-label 8200
huawei(config)#static-lsp egress lsp2 incoming-interface vlanif 100 in-label 8300
huawei(config)#display mpls static-lsp
{ <cr>|exclude<K>|include<K>|string<S><Length 1-19>|verbose<K> }:

  Command:
          display mpls static-lsp
TOTAL          :        2       STATIC LSP(S)
UP             :        0       STATIC LSP(S)
DOWN           :        2       STATIC LSP(S)
Name                FEC                I/O Label    I/O If                Status
lsp1                3.3.3.3/32         NULL/8200    -/-                   Down
lsp2                -/-                8300/NULL    vlanif100/-           Down
```

When the MA5600T/MA5603T functions as an LSR, to configure the transit node parameters of a static LSP, set the parameters as follows:

- LSP name of the transit node in the positive direction: lsp1; LSP name of the transit node in the negative direction: lsp2
- IP address of local VLAN interface 100: 100.1.1.2/24
- IP address of local VLAN interface 200: 200.1.1.2/24
- Out label in the positive direction: 8200; in label in the positive direction: 8300
- Out label in the negative direction: 8200; in label in the negative direction: 8300

- Next hop IP address in the positive direction: 200.1.1.3
- Next hop IP address in the negative direction: 100.1.1.3

```
huawei(config)#static-lsp transit lsp1 incoming-interface vlanif 100 in-label 82
00 nexthop 200.1.1.3 out-label 8300
huawei(config)#static-lsp transit lsp2 incoming-interface vlanif 200 in-label 83
00 nexthop 100.1.1.2 out-label 8200
huawei(config)#display mpls static-lsp
{ <cr>|exclude<K>|include<K>|string<S><Length 1-19>|verbose<K> }:

  Command:
          display mpls static-lsp
TOTAL          :        2       STATIC LSP(S)
UP             :        0       STATIC LSP(S)
DOWN           :        2       STATIC LSP(S)
Name                FEC                I/O Label    I/O If                Status
lsp1                -/-                8200/8300    vlanif100/-           Down
lsp2                -/-                8300/8200    vlanif200/-           Down
```

12.1.2 Configuring the LDP LSP

Set up an MPLS LDP session between LSRs along the LSP. After the MPLS LDP session is set up, the LDP LSP is automatically created.

Prerequisites

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The VLAN for MPLS label forwarding must be created.
4. Global MPLS must be enabled.
5. A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).

Context

- The MA5600T/MA5603T supports LDP and RSVP-TE, both of which generate dynamic LSPs.
- LDP is a standard MPLS label distribution protocol defined by IETF. LDP, which is mainly used to distribute labels for the negotiation between LSRs to set up label switching paths (LSPs), regulates various types of information for the label distribution process, and the related processing. The LSRs form an LSP that crosses the entire MPLS domain according to the local forwarding table, which correlates the in label, network hop node, and out label of each specific FEC.

Procedure

Step 1 Configure the MPLS LDP session.

The MPLS-LDP session is used for information exchange such as label mapping and release between LSRs. The MPLS-LDP session is classified into two types:

- Local LDP session: Two LSRs between which a session is set up are connected directly.
- Remote LDP session: Two LSRs between which a session is set up are not connected directly. Remote LDP sessions are mainly set up between nonadjacent LSRs. They can also be set up between adjacent LSRs.

NOTE

If local adjacency with the specified remote peer exists, remote adjacency cannot be set up; if remote adjacency exists and local adjacency is set up for the remote peer, the remote peer will be deleted. In other words, only one session can exist between two LSRs and a local LDP session takes priority over a remote LDP session.

- Configure the local LDP session.
  1. In the global config mode, run the **mpls ldp** command to enable global MPLS LDP.
  2. In the global config mode, run the **mpls vlan** command to enable the MPLS function of the VLAN.

     NOTE

     The VLAN 1 is the system default VLAN. All the upstream ports have been added to this VLAN by default. Do not use this VLAN as the MPLS VLAN or enable the MPLS function on this VLAN.
  3. Run the **interface vlanif** command to enter the VLAN interface mode.
  4. In the VLAN interface mode, run the **mpls** command to enable the MPLS function of the VLAN interface and run the **mpls ldp** command to enable the MPLS LDP function of the VLAN interface.
  5. Run the **quit** command to quit the VLAN interface mode.
- Configure the remote LDP session.
  1. In the global config mode, run the **mpls ldp** command to enable global MPLS LDP.
  2. Run the **mpls ldp remote-peer** command to create an LDP remote peer and then enter the remote peer mode.
  3. Run the **remote-ip** command to configure the IP address of the LDP remote peer.

     NOTE

     The IP address of the remote LDP peer should be the LSR ID of the remote LSR. When the LSR ID is used as the transmission address of a remote peer, two remote peers set up a TCP connection between them using the LSR ID as the transmission address.
  4. (Optional) Run the **mpls ldp advertisement** command to set the label distribution mode to DoD (downstream on demand) or DU (downstream unsolicited, default).

     In a network with a large scale, it is recommended to set the mode to DoD to reduce unnecessary MPLS forwarding entries.
  5. (Optional) Run the **remote-peer auto-dod-request** command to automatically use the DoD label distribution mode to request the label mapping information about the LSR IDs of all downstream remote peers.

     When the network has a large scale and many LDP remote peers, perform this configuration to maximally save system resources.

Step 2 (Optional) Configure the LDP MTU signaling function.

Run the **mtu-signalling** command to enable the sending of the MTU type, length, and value (TLV). This enables the LDP to automatically calculate and negotiate the minimum MTU value for all ports on each LSP. In this way, the MPLS determines the size of the MPLS forwarding packet at the ingress according to the minimum MTU, thereby avoiding the forwarding failure on transit nodes caused by oversize packets at the ingress.

By default, the LDP MTU signaling is enabled.

Step 3 (Optional) Configure the route trigger policy for setting up an LSP.

Run the **lsp-trigger host** command to configure the route trigger policy for setting up an LSP. The default route trigger policy is used to set up an LSP by triggering the LDP through the host address. To modify the default route trigger policy, run this command.

NOTE

It is recommended that you configure the route trigger policy for setting up an LSP to host (default), that is, the host route triggers the LDP to set up an LSP. In this way, the setup of useless LSPs can be prevented.

Step 4 (Optional) Configure the trigger policy set up by the transit LSP.

Run the **propagate mapping** command to filter certain routes received by the LDP by using the IP prefix table. Only the route that matches the specified IP prefix table is used by the local LDP for creating the transit LSP. By default, the LDP does not filter the received routes when creating the transit LSP.

Step 5 (Optional) Configure the LDP inter-domain extension function.

By default, LDP uses the full match mode to search for a route and set up an LSP; however, when the network scale is large and the LDP spans multiple IGP areas, the longest match mode must be used to search the routing table and set up an LSP accordingly. Run the **longest-match** command to configure the LDP inter-domain extension function.

Step 6 Query the relevant information about the LDP LSP configuration.

- Run the **display mpls ldp lsp** command to query the relevant information about the created LDP LSP.
- Run the **display mpls ldp session** command to check whether the created remote MPLS LDP session is in the normal (operational) state.
- Run the **display mpls interface** command to check whether the MPLS interface is in the normal (up) state.

----End

Example

To configure an LDP LSP between two adjacent LSRs by using VLAN interface 200 as the MPLS forwarding interface and using default values for other parameters, do as follows:

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
huawei(config)#mpls vlan 200
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#mpls ldp
huawei(config-if-vlanif200)#quit
huawei(config)#display mpls interface vlanif 200
{ <cr>|verbose<K> }:

  Command:
          display mpls interface vlanif 200
Interface             Status    TE Attr   LSP Count  CRLSP Count Effective MTU
vlanif200             Down      Dis       0          0           1500
```

To configure an LDP LSP between two nonadjacent LSRs by configuring the local lsr-id to 3.3.3.3, configuring the remote lsr-id to 5.5.5.5, and using default values for other parameters, do as follows:

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
huawei(config)#mpls ldp remote-peer session1
huawei(config-mpls-ldp-remote-session1)#remote-ip 5.5.5.5
huawei(config-mpls-ldp-remote-session1)#quit
huawei(config)#display mpls ldp remote-peer
{ <cr>|peer-id<K>|string<S><Length 1-32>||<K> }:

  Command:
        display mpls ldp remote-peer
```

```
                        LDP Remote Entity Information
------------------------------------------------------------------------------
Remote Peer Name  : session1
Remote Peer IP    : 5.5.5.5            LDP ID        : 1.1.1.1:0
Transport Address : 1.1.1.1            Entity Status : Active

Configured Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : ---
Configured Hello Hold Timer     : 45 Sec
Negotiated Hello Hold Timer     : 45 Sec
Configured Hello Send Timer     : ---
Configured Delay Timer          : 10 Sec
Hello Packet sent/received      : 0/0
Label Advertisement Mode        : Downstream Unsolicited
Remote Peer Deletion Status     : No
Auto-config                     : ---
------------------------------------------------------------------------------
TOTAL: 1 Peer(s) Found.
```

12.1.3 Configure an RSVP-TE LSP

MPLS TE is a technology that integrates TE with MPLS. Through the MPLS TE technology, you can create an LSP tunnel to a specified path, to reserve resources and implement re-optimization.

Prerequisites

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The VLAN for MPLS label forwarding must be created.
4. Global MPLS and VLAN MPLS must be enabled.
5. The OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

Context

- To create constraint-based LSPs in MPLS TE, RSVP is extended. The extended RSVP signaling protocol is called the RSVP-TE signaling protocol.
- MPLS TE creates the LSP tunnel along a specified path through RSVP-TE and reserves resources. Thus, carriers can accurately control the path that traffic traverses to avoid the node where congestion occurs. This solves the problem that certain paths are overloaded and other paths are idle, utilizing the current bandwidth resources sufficiently. In addition, MPLS TE can reserve resources during the creation of LSP tunnels to ensure the QoS.

Procedure

Step 1 Enable MPLS TE and RSVP-TE.

1. In the global config mode, run the **mpls** command to enter the MPLS mode.
2. In the MPLS mode, run the **mpls te** command to enable global MPLS TE, run the **mpls rsvp-te** command to enable global RSVP-TE, and run the **mpls te cspf** command to enable Constraint Shortest Path First (CSPF).
3. Run the **quit** command to quit the MPLS mode and run the **interface vlanif** command to enter the VLAN interface mode.

4. In the VLAN interface mode, run the **mpls** command to enable the VLAN interface MPLS, run the **mpls te** command to enable the VLAN interface MPLS TE, and run the **mpls rsvp-te** command to enable the VLAN interface RSVP-TE.

   NOTE

   - CSPF provides a way to select the path in an MPLS area. Enable CSPF before configuring other CSPF functions.
   - It is recommended that you configure CSPF on all transit nodes lest the ingress cannot calculate the entire path.

Step 2 (Optional) Configure the line bandwidth.

To guarantee the bandwidth of the service transmitted on the MPLS TE tunnel, perform this operation.

1. In the VLAN interface mode, run the **mpls te bandwidth max-reservable-bandwidth** command to configure the maximum reservable bandwidth for the MPLS TE tunnel on the VLAN interface.
2. In the VLAN interface mode, run the **mpls te bandwidth** { **bc0** *bandwidth* | **bc1** *bandwidth* } command to configure the bandwidth that can be obtained from BC0 and BC1 of the VLAN interface when an MPLS TE tunnel is created.

   NOTE

   - BC0: Indicates the global pool bandwidth of an MPLS TE tunnel.
   - BC1: Indicates the sub-pool bandwidth type of an MPLS TE tunnel. It is used to transmit services with higher priority and higher performance requirements.
   - The bandwidth values must meet the following requirement: maximum reservable bandwidth ≥ BC0 bandwidth ≥ BC1 bandwidth.

Step 3 Enable MPLS TE for the OSPF area.

The MA5600T/MA5603T enables the MPLS TE to know the relevant dynamic TE attributes of each link by extending the OSPF protocol. The extended OSPF enables the link status entry to add TE attributes, such as link bandwidth and affinity attribute. Each router in the network collects all the TE information in OSPF area and generates traffic engineering database (TEDB).

1. In the global config mode, run the **ospf** command to start the OSPF process and enter the OSPF mode.
2. Run the **opaque-capability enable** command to enable the OSPF opaque capability.

   After the opaque capability of the MA5600T/MA5603T is enabled, it can export TEDB information to neighbor devices.
3. Run the **area** command to enter the OSPF area mode and run the **mpls-te enable** command to enable the OSPF area TE.

Step 4 (Optional) Configure an MPLS TE explicit path.

An explicit path consists of a series of nodes, which constitute a vector path according to the configured sequence. The IP address in an explicit path is the IP address of the interface on the node. Generally, the loopback interface IP address on the egress is used as the destination IP address of the explicit path.

To specify a known path for a special traffic stream in the MPLS network, you can run the **explicit-path** command in the global config mode to configure an explicit path, and then run the **mpls te path explicit-path** command in the tunnel mode to specify the explicit path for the tunnel.

After an explicit path is created, you can run the **next hop**, **modify hop**, and **delete hop** command to add a next hop node, modify a node, and delete a node respectively for the explicit path.

Step 5 Configure an MPLS TE tunnel interface.

1. In global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
2. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE.
3. Run the **destination** *ip-address* command to configure the destination IP address of the tunnel. Generally, the egress LSR ID is used.
4. Run the **mpls te tunnel-id** command to configure the tunnel ID.
5. Run the **mpls te signal-protocol rsvp-te** command to configure the signaling protocol of the tunnel to RSVP-TE.
6. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface that meets this bandwidth value can be selected as the node traversed by the MPLS TE tunnel path when the MPLS TE tunnel is created.

   If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the tunnel bandwidth.
7. (Optional) Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.

   If only the bandwidth used by the MPLS TE tunnel is limited but the transmission path is not limited, you may not configure the explicit path used by the MPLS TE tunnel.
8. Run the **mpls te commit** command to commit the current configuration of the tunnel.

Step 6 Check the configuration.

1. Run the **display mpls te cspf tedb** command to query the CSPF TEDB information.
2. Run the **display mpls te link-administration admission-control** command to check the CR LSP information allowed on the link, including the bandwidth and priority.
3. Run the **display mpls te tunnel** command to query details about a specified tunnel.
4. Run the **display mpls te tunnel path** command to query the path information about a tunnel on a local node.
5. Run the **display mpls te tunnel-interface** command to query the tunnel interface information about a local node.

----End

Example

To configure the RSVP-TE LSP from the MA5600T/MA5603T to the PTN, set the parameters as follows.

- Set the parameters on the MA5600T/MA5603T.
  - LSR-ID: 3.3.3.3
  - Layer 3 interface IP address of VLAN 20 for MPLS forwarding: 10.1.1.3/24
  - Maximum reservable bandwidth of the VLAN interface: 20480 kbit/s; BC0 bandwidth: 10240 kbit/s
  - OSPF process ID: 100; OSPF area ID: 1
  - MPLS TE tunnel ID: 10; tunnel interface ID: 10
  - Required BC0 bandwidth when an MPLS TE tunnel is created: 5120 kbit/s

  - Other parameters: default settings

- Set the LSR ID of the PTN to 5.5.5.5.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 3.3.3.3 32
huawei(config-if-loopback0)#quit
huawei(config)#mpls lsr-id 3.3.3.3
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsvp-te
   //Configure the MPLS TE to use CSPF to calculate the shortest path to a node.
huawei(config-mpls)#mpls te cspf
huawei(config-mpls)#quit
huawei(config)#mpls vlan 20
huawei(config)#interface vlanif 20
   //Configure the IP address of the VLAN Layer 3 interface.
huawei(config-if-vlanif20)#ip address 10.1.1.3 24
   //Enable MPLS for the VLAN interface.
huawei(config-if-vlanif20)#mpls
   //Enable MPLS TE for the VLAN interface.
huawei(config-if-vlanif20)#mpls te
   //Enable MPLS RSVP-TE for the VLAN interface.
huawei(config-if-vlanif20)#mpls rsvp-te
huawei(config-if-vlanif20)#quit
huawei(config)#ospf 100
   //Enable the opaque capability to send the engineering data base information
     to peripheral devices.
huawei(config-ospf-100)#opaque-capability enable
huawei(config-ospf-100)#area 1
   //Enable MPLS TE for the OSPF area.
huawei(config-ospf-100-area-0.0.0.1)#mpls-te enable standard-complying
huawei(config-ospf-100-area-0.0.0.1)#quit
huawei(config-ospf-100)#quit
huawei(config)#interface vlanif 20
   //Configure the maximum reservable bandwidth of the Layer 3 interface.
huawei(config-if-vlanif20)#mpls te bandwidth max-reservable-bandwidth 20480
   //Configure the obtainable maximum bandwidth of the Layer 3 interface from BC0
     when the MPLS TE tunnel is created.
huawei(config-if-vlanif20)#mpls te bandwidth bc0 10240
huawei(config-if-vlanif20)#quit
huawei(config)#interface tunnel 10
   //Configure the link layer encapsulation protocol to MPLS TE for the tunnel
interface,
     that is, configure the tunnel interface to work in the CR-LSP tunnel mode.
huawei(config-if-tunnel10)#tunnel-protocol mpls te
   //Configure the destination IP address of the MPLS TE tunnel.
huawei(config-if-tunnel10)#destination 3.3.3.3
   //Configure the MPLS TE tunnel ID, which, along with the LSR-ID,
     uniquely indicates an MPLS TE tunnel.
huawei(config-if-tunnel10)#mpls te tunnel-id 10
   //Configure the protocol of the MPLS TE tunnel to RSVP-TE.
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
   //Configure the global pool bandwidth required by the MPLS TE tunnel.
huawei(config-if-tunnel10)#mpls te bandwidth ct0 5120
   //Allow the MPLS TE tunnel to be bound to a VPN instance, that is, the MPLS TE
tunnel
     can function as the outer tunnel of the PWE3 service.
huawei(config-if-tunnel10)#mpls te reserved-for-binding
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

12.1.4 Configuring the MPLS OAM

The MPLS OAM function uses an effective OAM mechanism to detect whether an LSP is normal and report an alarm in time when an LSP fault occurs. In addition, the MPLS OAM function features a complete protection switching mechanism, which triggers a switchover when a defect at the MPLS layer is detected to minimize the user data loss.

Context

Through the MPLS OAM mechanism, the MA5600T/MA5603T can effectively detect, confirm, and locate internal defects at the MPLS layer of a network. Then, the system reports and handles the defects. In addition, the system provides a mechanism for triggering 1:1 protection switching when a fault occurs.

The basic process of the MPLS OAM connectivity check and protection switching is as follows:

1. The source transmits the CV/FFD packets to the destination through the detected LSP.
2. The destination checks the correctness of the type and frequency carried in the received detection packets and measures the number of correct and errored packets that are received within the detection period to monitor the connectivity of the LSP in real time.
3. After detecting a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward path.
4. The source learns about the status of the defect, and triggers the corresponding protection switching when the protect group is correctly configured.

Configure the MPLS OAM as follows:

1. Configure the active LSP at the source end (ingress).
2. Configure the standby LSP at the source end.
3. Create a tunnel protect group.
4. Enable the MPLS OAM function at the source end.
5. Configure the backward LSP at the destination end (egress).
6. Enable the MPLS OAM function at the destination end.

NOTE

If only the MPLS OAM connectivity check needs to be enabled and 1:1 protection is not required for the LSP, you need not configure the standby LSP or the tunnel protect group at the source end.

Configuration Example for Detection of MPLS OAM for Static LSP Connectivity

This topic describes how to configure the function of MPLS OAM to detect the static LSP connectivity.

Prerequisites

Before the configuration, make sure that:

- Set the IP addresses and the masks of the ports based on the example network. After that, LSRs can ping the peer LSRs.
- A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).

Networking

Figure 12-1 shows an example network of configuring MPLS OAM to detect the static LSP connectivity.

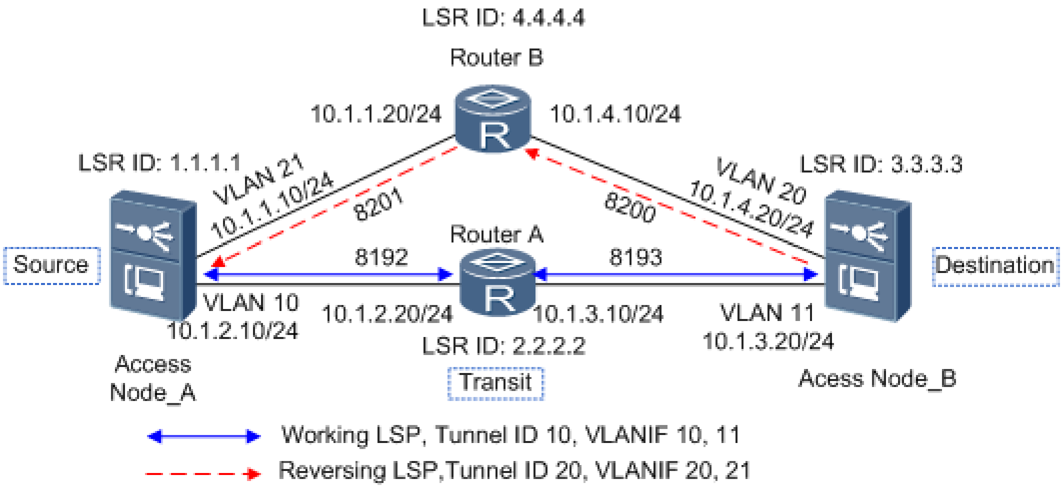
1. Source end MA5600T/MA5603T_A sends CV/FFD detection packets to the destination end through the detected LSP (MA5600T/MA5603T_A->Router A->MA5600T/MA5603T_B).

2. After detecting a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward LSP (MA5600T/MA5603T_B->Router B->MA5600T/MA5603T_A). This enables the source end to obtain the defect status in time.

NOTE

To facilitate description of the MPLS OAM application, the MA5600T/MA5603T is used at both the source end and destination end as an example. In the actual application, the MA5600T/MA5603T at one end may be replaced by a device that supports MPLS OAM such as a PTN device, but their implementation principles are the same.

Figure 12-1 Example network of detection of MPLS OAM for static LSP connectivity



Data Plan

Table 12-1 provides the data plan for detection of MPLS OAM for static LSP connectivity.

Table 12-1 Data plan for detection of MPLS OAM for static LSP connectivity

Item	Data
MA5600T/ MA5603T_A	LSR ID: 1.1.1.1
	Port: 0/19/0 IP address of VLAN interface 10 connected to Router A: 10.1.2.10/24 Tunnel ID: 10; tunnel interface ID: 10 Out label value of the LSP ingress: 8192 In label value of the LSP egress: 8193
	Port: 0/19/1 IP address of VLAN interface 21 connected to Router B: 10.1.1.10/24
	Static LSP: Router A to MA5600T/MA5603T_B
MA5600T/ MA5603T_B	LSR ID: 3.3.3.3

Item	Data
	Port: 0/19/0 IP address of VLAN interface 11 connected to Router A: 10.1.3.20/24
	Port: 0/19/1 IP address of VLAN interface 20 connected to Router B: 10.1.4.20/24 Tunnel ID: 20; tunnel interface ID: 20 Out label value of the LSP ingress: 8200 In label value of the LSP egress: 8201
	Static LSP: Router B to MA5600T/MA5603T_A
Router A	LSR ID: 2.2.2.2
	IP address of the interface connected to the MA5600T/MA5603T_A: 10.1.2.20/24
	IP address of the interface connected to the MA5600T/MA5603T_B: 10.1.3.10/24
Router B	LSR ID: 4.4.4.4
	IP address of the interface connected to the MA5600T/MA5603T_A: 10.1.1.20/24
	IP address of the interface connected to the MA5600T/MA5603T_B: 10.1.4.10/24

Procedure

- **Configure source end MA5600T/MA5603T_A.**

  1. Configure the loopback interface.

     ```
     huawei(config)#interface loopback 0
     huawei(config-if-loopback0)#ip address 1.1.1.1 32
     huawei(config-if-loopback0)#quit
     ```

  2. Enable the basic MPLS and MPLS TE.

     a. Enable the basic MPLS and MPLS TE globally.

     ```
     huawei(config)#mpls lsr-id 1.1.1.1
     huawei(config)#mpls
     huawei(config-mpls)#mpls te
     huawei(config-mpls)#quit
     ```

     b. Enable the basic MPLS and MPLS TE on the interface.

     ```
     huawei(config)#vlan 10 standard
     huawei(config)#mpls vlan 10
     huawei(config)#port vlan 10 0/19 0
     huawei(config)#interface vlanif 10
     huawei(config-if-vlanif10)#ip address 10.1.2.10 24
     huawei(config-if-vlanif10)#mpls
     huawei(config-if-vlanif10)#mpls te
     huawei(config-if-vlanif10)#quit
     huawei(config)#vlan 21 standard
     huawei(config)#mpls vlan 21
     huawei(config)#port vlan 21 0/19 1
     huawei(config)#interface vlanif 21
     huawei(config-if-vlanif21)#ip address 10.1.1.10 24
     ```

```
huawei(config-if-vlanif21)#mpls
huawei(config-if-vlanif21)#mpls te
huawei(config-if-vlanif21)#quit
```

3. Configure the MPLS TE tunnel from the source end to the destination end.

   Configure the MPLS TE tunnel bound to the detected LSP.

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
huawei(config-if-tunnel10)#destination 3.3.3.3
huawei(config-if-tunnel10)#mpls te tunnel-id 20
huawei(config-if-tunnel10)#mpls te signal-protocol static
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

4. Configure the static LSP bound to the MPLS TE tunnel.

   Source end MA5600T/MA5603T functions as the ingress of the detected static LSP.

```
huawei(config)#static-lsp ingress tunnel-interface tunnel 10
destination 3.3.3.3 nexthop 10.1.2.20 out-label 8192
```

   Source end MA5600T/MA5603T functions as the egress of the detected static LSP.

```
huawei(config)#static-lsp egress LSP1 incoming-interface vlanif 10 in-
label 8193
```

   Source end MA5600T/MA5603T functions as the egress of the backward static LSP.

```
huawei(config)#static-lsp egress LSP2 incoming-interface vlanif 20 in-
label 8201
```

5. Enable MPLS OAM at source end MA5600T/MA5603T_A.

```
huawei(config)#mpls
huawei(config-mpls)#mpls oam
huawei(config-mpls)#quit
huawei(config)#mpls oam ingress tunnel 10 type ffd frequency 100
backward-lsp lsr-id 3.3.3.3 tunnel-id 20
...//Configure the MPLS OAM source end. Configure the tunnel ID of the
detected LSP to 10, detection packet type to FFD, Tx frequency to 100 ms,
LSR-ID of the backward LSP to 3.3.3.3,
...//and backward LSP tunnel ID to 20.
huawei(config)#mpls oam ingress enable all
```

6. Save the data.

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

- **Configure Router A or Router B.**

  When functioning as the transit node, Router A or Router B mainly forwards MPLS labels. The ingress interface, in label, next hop IP address, and out label must be configured bi-directionally. For detailed configuration, see the configuration guide of the specific router.

- **Configure destination end MA5600T/MA5603T_B.**

1. Configure the loopback interface.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 3.3.3.3 32
huawei(config-if-loopback0)#quit
```

2. Enable the basic MPLS and MPLS TE.

   a. Enable the basic MPLS and MPLS TE globally.

```
huawei(config)#mpls lsr-id 3.3.3.3
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#quit
```

   b. Enable the basic MPLS and MPLS TE on the interface.

```
huawei(config)#vlan 11 standard
huawei(config)#mpls vlan 11
huawei(config)#port vlan 11 0/19 0
huawei(config)#interface vlanif 11
```

```
    huawei(config-if-vlanif11)#ip address 10.1.3.20 24
    huawei(config-if-vlanif11)#mpls
    huawei(config-if-vlanif11)#mpls te
    huawei(config-if-vlanif11)#quit
    huawei(config)#vlan 20 standard
    huawei(config)#mpls vlan 20
    huawei(config)#port vlan 20 0/19 1
    huawei(config)#interface vlanif 20
    huawei(config-if-vlanif20)#ip address 10.1.4.20 24
    huawei(config-if-vlanif20)#mpls
    huawei(config-if-vlanif20)#mpls te
    huawei(config-if-vlanif20)#quit
```

3. Configure the MPLS TE tunnel from the destination end to the source end.

   Configure the MPLS TE tunnel bound to the detected LSP.

   ```
   huawei(config)#interface tunnel 10
   huawei(config-if-tunnel10)#tunnel-protocol mpls te
   huawei(config-if-tunnel10)#destination 1.1.1.1
   huawei(config-if-tunnel10)#mpls te tunnel-id 10
   huawei(config-if-tunnel10)#mpls te signal-protocol static
   huawei(config-if-tunnel10)#mpls te commit
   huawei(config-if-tunnel10)#quit
   ```

   Configure the MPLS TE tunnel bound to the backward LSP.

   ```
   huawei(config)#interface tunnel 20
   huawei(config-if-tunnel20)#tunnel-protocol mpls te
   huawei(config-if-tunnel20)#destination 1.1.1.1
   huawei(config-if-tunnel20)#mpls te tunnel-id 20
   huawei(config-if-tunnel20)#mpls te signal-protocol static
   huawei(config-if-tunnel20)#mpls te commit
   huawei(config-if-tunnel20)#quit
   ```

4. Configure the static LSP bound to the tunnel.

   Destination end MA5600T/MA5603T functions as the egress of the detected static LSP.

   ```
   huawei(config)#static-lsp egress LSP2 incoming-interface vlanif 10 in-
   label 8192
   ```

   Destination end MA5600T/MA5603T functions as the ingress of the detected static LSP.

   ```
   huawei(config)#static-lsp ingress tunnel-interface tunnel 10
   destination 1.1.1.1 nexthop 10.1.3.10 out-label 8193
   ```

   Destination end MA5600T/MA5603T functions as the ingress of the backward static LSP.

   ```
   huawei(config)#static-lsp ingress tunnel-interface tunnel 20
   destination 1.1.1.1 nexthop 10.1.4.10 out-label 8200
   ```

5. Enable MPLS OAM at destination end MA5600T/MA5603T.

   ```
   huawei(config)#mpls
   huawei(config-mpls)#mpls oam
   huawei(config-mpls)#quit
   huawei(config)#mpls oam egress lsr-id 1.1.1.1 tunnel-id 10 type ffd
   frequency 100 backward-lsp t
   unnel 20 private
   ...//Configure the MPLS OAM destination end. Configure the ingress LSR-ID
   of the detected LSP to 1.1.1.1, tunnel ID to 10, detection packet type to
   FFD, Tx frequency to 100 ms,
   ...//backward LSP tunnel ID to 20, and tunnel to exclusive mode.
   huawei(config)#mpls oam egress enable all
   ```

6. Save the data.

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

----End

Result

After the configuration, shut down the interface of VLAN 10 by running the **shutdown** command on MA5600T/MA5603T_A to simulate the link fault:

- On MA5600T/MA5603T_B, run the **display mpls oam egress** command and you can see the following defect state: dLocv detected (dLocv).
- On MA5600T/MA5603T_A, run the **display mpls oam ingress** command and you can see the following defect state: in defect (In-defect).

Perform similar operations on MA5600T/MA5603T_B and you can obtain similar results.

Configuration Example of the MPLS OAM Protection Switching Function

This topic describes how to configure MPLS OAM to implement the protection switching function.

Service Requirements

- The OAM mechanism is used to detect in real time whether the MPLS link is normal and generates an alarm in time when a link fault is detected.
- The end-to-end tunnel protection technology is provided to recover the interrupted service.
- RSVP-TE is used to create an LSP tunnel for the specified path and reserve resources so that the existing bandwidth resources can be fully used and QoS can be improved for specific services.

Prerequisite

- The OSPF protocol must be successfully configured on each LSR in the network (the host route of each port must be successfully advertised).
- The interface IP address and mask, loopback interface, and LSR-ID must be configured on each LSR.
- The global and physical interface MPLS and MPLS TE functions must be enabled on each node of the LSR.

Networking

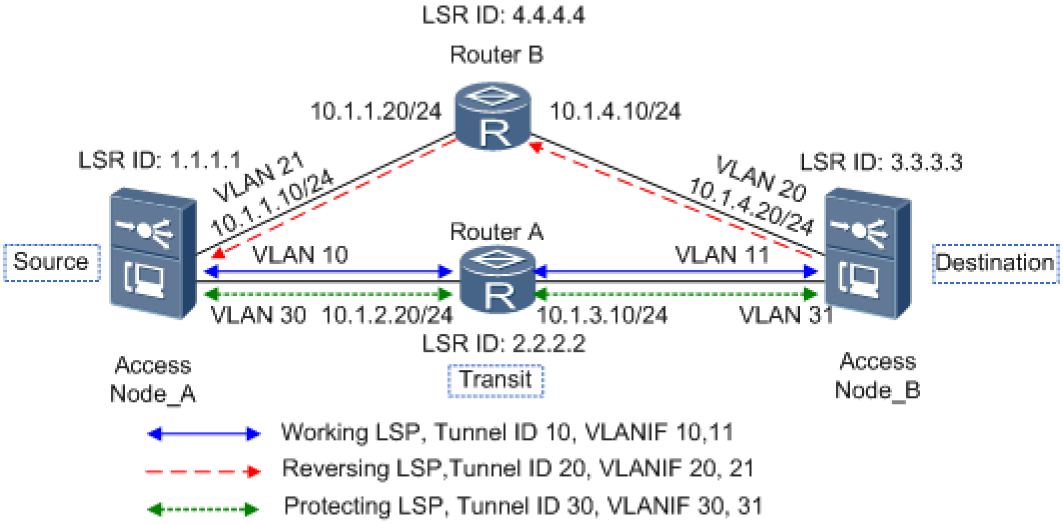
Figure 12-2 shows an example network for configuring the MPLS OAM protection switching function.

Configure two LSP tunnels on source end MA5600T/MA5603T_A and destination end MA5600T/MA5603T_B functioning primary and secondary LSPs. Enable the MPLS OAM protection switching function for the LSPs. When the primary LSP is faulty, the traffic is switched to the secondary LSP. Configure the backward LSP for reporting a fault to source end MA5600T/MA5603T_A.

NOTE

To prevent a fault from occurring on a transit node (for example, router A), it is recommended that you specify different transit nodes when creating a secondary LSP.

Figure 12-2 Configuring the MPLS OAM protection switching function



Data Plan

Table 12-2 provides the data plan for the MPLS OAM protection switching.

Table 12-2 Data plan for the MPLS OAM protection switching

Item	Data
MA5600T/ MA5603T_A	LSR ID: 1.1.1.1
	Port: 0/19/0 IP address of VLAN interface 10 connected to Router A: 10.1.2.10/24
	Port: 0/19/1 IP address of VLAN interface 30 connected to Router A: 10.1.5.10/24 IP address of VLAN interface 21 connected to Router B: 10.1.1.10/24
MA5600T/ MA5603T_B	LSR ID: 3.3.3.3
	Port: 0/19/0 IP address of VLAN interface 11 connected to Router A: 10.1.3.20/24
	Port: 0/19/1 IP address of VLAN interface 20 connected to Router B: 10.1.4.20/24 IP address of VLAN interface 31 connected to Router A: 10.1.6.20/24
	Backward tunnel: Router B to MA5600T/MA5603T_A
Router A	LSR ID: 2.2.2.2
Router B	LSR ID: 4.4.4.4

Procedure

- **Configure source end MA5600T/MA5603T_A.**

1. Configure the loopback interface.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 1.1.1.1 32
huawei(config-if-loopback0)#quit
```

2. Enable the basic MPLS, MPLS TE, and RSVP-TE functions.

   a. Enable the global basic MPLS, MPLS TE, and RSVP-TE functions.

```
huawei(config)#mpls lsr-id 1.1.1.1
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsvp-te
huawei(config-mpls)#mpls te cspf
huawei(config-mpls)#quit
```

   b. Enable the interface basic MPLS, MPLS TE, and RSVP-TE functions.

```
   //Configure the attributes of VLAN interface 10 and configure the
IP address of VLAN interface10 to 10.1.2.10/24.
huawei(config)#vlan 10 standard
huawei(config)#mpls vlan 10
huawei(config)#port vlan 10 0/19 0
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.1.2.10 24
huawei(config-if-vlanif10)#mpls
huawei(config-if-vlanif10)#mpls te
huawei(config-if-vlanif10)#mpls rsvp-te
huawei(config-if-vlanif10)#mpls te bandwidth max-reservable-bandwidth
10240
   //(Optional) Configure VLAN interface 10 to provide a reservable
bandwidth of 10240 kbit/s for all tunnels.
huawei(config-if-vlanif10)#quit
   //Configure the attributes of VLAN interface 30 and configure the
IP address of VLAN interface 30 to 10.1.5.10/24.
huawei(config)#vlan 30 standard
huawei(config)#mpls vlan 30
huawei(config)#port vlan 30 0/19 1
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.1.1.10 24
huawei(config-if-vlanif30)#mpls
huawei(config-if-vlanif30)#mpls te
huawei(config-if-vlanif30)#mpls rsvp-te
huawei(config-if-vlanif30)#mpls te bandwidth max-reservable-bandwidth
10240
   //(Optional) Configure VLAN interface 30 to provide a reservable
bandwidth of 10240 kbit/s for all tunnels.
huawei(config-if-vlanif30)#quit
   //Configure the attributes of VLAN interface 21 and configure the
IP address of VLAN interface 21 to 10.1.1.10/24.
huawei(config)#vlan 21 standard
huawei(config)#mpls vlan 21
huawei(config)#port vlan 21 0/19 1
huawei(config)#interface vlanif 21
huawei(config-if-vlanif21)#ip address 10.1.1.10 24
huawei(config-if-vlanif21)#mpls
huawei(config-if-vlanif21)#mpls te
huawei(config-if-vlanif21)#mpls rsvp-te
huawei(config-if-vlanif21)#mpls te bandwidth max-reservable-bandwidth
10240
   //(Optional) Configure VLAN interface 21 to provide a reservable
bandwidth of 10240 kbit/s for all tunnels.
huawei(config-if-vlanif21)#quit
```

3. Enable MPLS TE for the OSPF area.

```
huawei(config)#ospf 100
huawei(config-ospf-100)#opaque-capability enable
huawei(config-ospf-100)#area 0
huawei(config-ospf-100-area-0.0.0.0)#mpls-te enable standard-complying
huawei(config-ospf-100-area-0.0.0.0)#quit
huawei(config-ospf-100)#quit
```

4. Configure the MPLS TE tunnel from the source end to the destination end.

   Configure the attributes of the working MPLS TE tunnel from the source end to the destination end.

   ```
   huawei(config)#interface tunnel 10
   huawei(config-if-tunnel10)#tunnel-protocol mpls te
   huawei(config-if-tunnel10)#destination 3.3.3.3
   huawei(config-if-tunnel10)#mpls te tunnel-id 10
   huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
   huawei(config-if-tunnel10)#mpls te bandwidth ct0 5120   //(Optional)
   Configure the global bandwidth of tunnel 10 to 5210 kbit/s.
   huawei(config-if-tunnel10)#mpls te commit
   huawei(config-if-tunnel10)#quit
   ```

   Configure the attributes of the protection MPLS TE tunnel from the source end to the destination end.

   ```
   huawei(config)#interface tunnel 30
   huawei(config-if-tunnel30)#tunnel-protocol mpls te
   huawei(config-if-tunnel30)#destination 3.3.3.3
   huawei(config-if-tunnel30)#mpls te tunnel-id 30
   huawei(config-if-tunnel30)#mpls te signal-protocol rsvp-te
   huawei(config-if-tunnel30)#mpls te bandwidth ct0 5120   //(Optional)
   Configure the global bandwidth of tunnel 30 to 5210 kbit/s.
   huawei(config-if-tunnel30)#mpls te commit
   huawei(config-if-tunnel30)#quit
   ```

5. Configure a tunnel protect group.

   Configure tunnel 30 as the protect tunnel for tunnel 10, switching mode to revertive, and automatic WTR time to 900s (the corresponding WTR is 30 with step 30s).

   ```
   huawei(config)#interface tunnel 10
   huawei(config-if-tunnel10)#mpls te protection tunnel 30 mode revertive wtr
   30
   huawei(config-if-tunnel10)#mpls te commit
   huawei(config-if-tunnel10)#quit
   ```

6. Enable MPLS OAM at source end MA5600T/MA5603T_A.

   ```
   huawei(config)#mpls
   huawei(config-mpls)#mpls oam
   huawei(config-mpls)#quit
   huawei(config)#mpls oam ingress tunnel 10 type ffd frequency 100
   backward-lsp lsr-id 3.3.3.3 tunnel-id 20
      //Configure the MPLS OAM source end. Configure the tunnel ID of the
   detected LSP to 10, detection packet type to FFD, Tx frequency to 100 ms,
   LSR-ID of the backward LSP to 3.3.3.3,
      //and backward LSP tunnel ID to 20.
   huawei(config)#mpls oam ingress enable all
   ```

7. Save the data.

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

- **Configure Router A or Router B.**

When functioning as the transit node, Router A or Router B mainly forwards MPLS labels. The ingress interface, in label, next hop IP address, and out label must be configured bi-directionally. For detailed configuration, see the configuration guide of the specific router.

- **Configure destination end MA5600T/MA5603T_B.**

1. Configure the loopback interface.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 3.3.3.3 32
   huawei(config-if-loopback0)#quit
   ```

2. Enable the basic MPLS, MPLS TE, and RSVP-TE functions.

   a. Enable the global basic MPLS, MPLS TE, and RSVP-TE functions.

```
huawei(config)#mpls lsr-id 3.3.3.3
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsvp-te
huawei(config-mpls)#mpls te cspf
huawei(config-mpls)#quit
```

   b. Enable the interface basic MPLS, MPLS TE, and RSVP-TE functions.

```
   //Configure the attributes of VLAN interface 11 and configure the
IP address of VLAN interface 11 to 10.1.3.20/24.
huawei(config)#vlan 11 standard
huawei(config)#mpls vlan 11
huawei(config)#port vlan 11 0/19 0
huawei(config)#interface vlanif 11
huawei(config-if-vlanif11)#ip address 10.1.3.20 24
huawei(config-if-vlanif11)#mpls
huawei(config-if-vlanif11)#mpls te
huawei(config-if-vlanif11)#mpls rsvp-te
huawei(config-if-vlanif10)#quit
   //Configure the attributes of VLAN interface 20 and configure the
IP address of VLAN interface 20 to 10.1.4.20/24.
huawei(config)#vlan 20 standard
huawei(config)#mpls vlan 20
huawei(config)#port vlan 20 0/19 1
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.1.4.20 24
huawei(config-if-vlanif20)#mpls
huawei(config-if-vlanif20)#mpls te
huawei(config-if-vlanif20)#mpls rsvp-te
huawei(config-if-vlanif20)#quit
   //Configure the attributes of VLAN interface 31 and configure the
IP address of VLAN interface 31 to 10.1.6.20/24.
huawei(config)#vlan 31 standard
huawei(config)#mpls vlan 31
huawei(config)#port vlan 31 0/19 1
huawei(config)#interface vlanif 31
huawei(config-if-vlanif31)#ip address 10.1.6.20 24
huawei(config-if-vlanif31)#mpls
huawei(config-if-vlanif31)#mpls te
huawei(config-if-vlanif31)#mpls rsvp-te
huawei(config-if-vlanif31)#quit
```

3. Configure the MPLS TE tunnel bound to the backward LSP.

   Configure the tunnel ID to 20, destination IP address to 1.1.1.1, and global bandwidth for the tunnel to 5120 kbit/s.

```
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls te
huawei(config-if-tunnel20)#destination 1.1.1.1
huawei(config-if-tunnel20)#mpls te tunnel-id 20
huawei(config-if-tunnel20)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel20)#mpls te bandwidth ct0 5120
huawei(config-if-tunnel20)#mpls te reserved-for-binding
huawei(config-if-tunnel20)#mpls te commit
huawei(config-if-tunnel20)#quit
```

4. Enable MPLS OAM at destination end MA5600T/MA5603T_B.

```
huawei(config)#mpls
huawei(config-mpls)#mpls oam
huawei(config-mpls)#quit
huawei(config)#mpls oam egress lsr-id 1.1.1.1 tunnel-id 10 type ffd
frequency 100
 backward-lsp tunnel 20 private
   //Configure the MPLS OAM destination end. Configure the ingress LSR-ID
of the detected LSP to 1.1.1.1, tunnel ID to 10, detection packet type to
FFD, Tx frequency to 100 ms,
   //backward LSP tunnel ID to 20, and tunnel to exclusive mode.
huawei(config)#mpls oam egress enable all
```

5. Save the data.

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

----End

Result

After the configuration, you can shut down the interface of VLAN 10 by running the **shutdown** command on MA5600T/MA5603T_A to simulate the link fault. Then, you can query the information about the primary tunnel (with ID 10) that is configured on MA5600T/MA5603T_A by running the **display mpls te protection tunnel** command on MA5600T/MA5603T_A. The information is as follows:

- Status of the working tunnel (work-tunnel defect state): in defect.
- Status of the protection tunnel (protect-tunnel defect state): non-defect.
- Switch result: The traffic is switched to protection tunnel 30.

12.2 Configuring the PWE3 Private Line Service

Pseudo wire emulation edge-to-edge (PWE3) uses LDP or RSVP-TE as the signaling protocol and carries various Layer 2 services of the customer edge (CE) over the MPLS LSP or TE tunnel, transparently transmitting the Layer 2 data of the CE.

PWE3 Service Model

According to the PWE3 service model, PWE3 is indicated by the outer packet switch network (PSN) tunnel label and the inner label (PW demultiplexer).

The PSN layer can select the MPLS or IP technology and the PW demultiplexer can select the MPLS, UDP, or layer-2 tunneling protocol (L2TP) technology. The PWE3 outer label and inner label support the following combinations: MPLS over MPLS, MPLS over IP, UDP over IP, and L2TP over IP. The MA5600T/MA5603T supports the first three.

Network Application

Figure 12-3 shows the network application of the MPLS PWE3.

As shown in the figure, the mainstream applications of the MPLS PWE3 supported by the MA5600T/MA5603T are as follows:

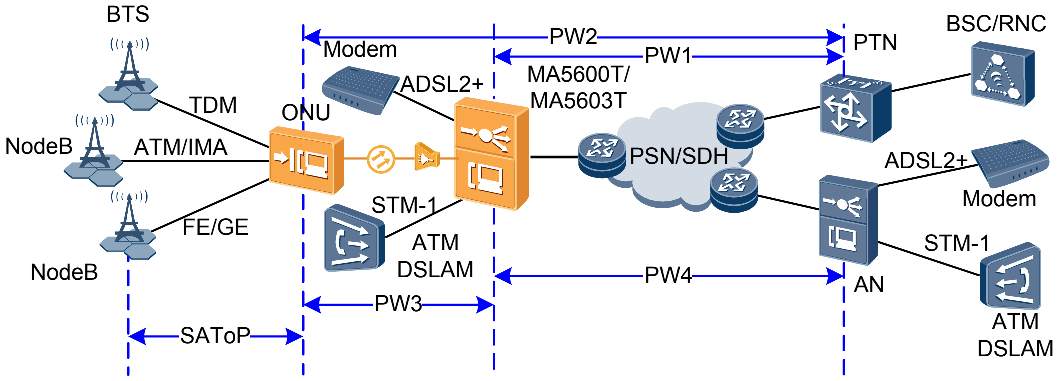
- TDM PWE3: A mobile 2G base station is connected to the ONU through the TDM E1 port. The ONU implements the TDM PWE3, transmitting traffic streams to the peer TDM PWE3 device through the PSN. The MA5600T/MA5603T functions as a Layer 2 transparent transmission device, PE device, or P device.
- ATM PWE3: The IMA service data of a 3G base station is connected to the ONU through the E1 port. The ONU restores the IMA service to the ATM service and encapsulates the ATM service on the ATM PWE3 private line for connecting to the peer ATM PWE3 device (PTN device in the figure). The MA5600T/MA5603T functions as a Layer 2 transparent transmission device or P device.
- ETH PWE3: A 3G base station is connected to the ONU through the FE/GE port. The ONU performs the ETH PWE3 encapsulation for interconnecting with the peer ETH PWE3

device. The MA5600T/MA5603T functions as a Layer 2 transparent transmission device or P device.

NOTE

- The MA5600T/MA5603T can function as a Layer 2 transparent transmission device or PE/P device, determined by the service requirement.
- As shown in the following figure, in PW1, PW3, and PW4, the MA5600T/MA5603T functions as a PE device that initiates or terminates the PW; in PW2, the MA5600T/MA5603T functions as a Layer 2 transparent transmission device or P device.

Figure 12-3 MPLS PWE3 network application when the MA5600T/MA5603T functions as a Layer 2 transparent transmission device, PE device, or P device



Procedure

According to the PWE3 service model, PWE3 configurations include the outer tunnel configuration, inner PW configuration, and tunnel protection. Therefore, the configuration procedure is as follows.

12.2.1 Configuring the PWE3 Outer Tunnel

To provide services across the IP network or MPLS network, the MA5600T/MA5603T supports PW over the IP tunnel or MPLS tunnel to transparently transmit services in the IP network.

Prerequisites

1. The loopback interface IP address must be configured.
2. The LSR ID must be configured.
3. The global MPLS and MPLS TE functions must be enabled.
4. The OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

Context

According to the upper-layer PSN type, namely MPLS network or IP network, the PWE3 outer tunnel is categorized as MPLS tunnel and IP tunnel.

Different PWE3s support different tunnel encapsulation formats. Pay attention to the following points during the configuration:

- TDM PWE3 supports the following PWE3 tunnel encapsulation formats: MPLS over MPLS and MPLS over IP
- ATM PWE3 supports the following PWE3 tunnel encapsulation formats: MPLS over MPLS and MPLS over IP.
- ETH PWE3 supports only the MPLS over MPLS encapsulation format.

Procedure

- Configure the MPLS TE tunnel.
  1. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
  2. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE, that is, configure the tunnel interface to work in the TE tunnel mode.
  3. Run the **destination** *ip-address* command to configure the destination IP address of the tunnel. Generally, the LSR ID of the ingress is used.
  4. Run the **mpls te tunnel-id** command to configure the tunnel ID.
  5. Run the **mpls te signal-protocol** { **rsvp-te** | **static** } command to configure the signaling protocol for the MPLS TE tunnel.

     According to whether the MPLS TE tunnel uses the dynamic signaling protocol, the tunnel is categorized as static MPLS TE tunnel and MPLS RSVP-TE tunnel.

     - Static MPLS TE tunnel: The forwarding information and resource information are configured manually, and the signaling protocol and path calculation are not involved. Because the MPLS-related control packets are not exchanged, fewer resources are used. The static tunnel, however, cannot be dynamically adjusted according to network changes. Therefore, the actual application is limited.
     - MPLS RSVP-TE tunnel: MPLS TE creates the LSP tunnel along a specified path through RSVP-TE and reserves resources. Thus, carriers can accurately control the path that traffic traverses to avoid the node where congestion occurs. This solves the problem that certain paths are overloaded and other paths are idle, utilizing the current bandwidth resources sufficiently.
  6. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth of the tunnel. After the configuration is completed, only the VLAN interface meeting this bandwidth requirement is selected as the node traversed by an MPLS TE tunnel when the MPLS TE tunnel is created.

     If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the bandwidth of the tunnel.
  7. (Optional) Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.

     To limit only the bandwidth of the MPLS TE tunnel but not the transmission path, you may not configure the explicit path of the tunnel.
  8. Run the **mpls te commit** command to commit the current tunnel configuration.

     NOTE

     Each time the MPLS TE parameters on the tunnel interface are changed, you need to run the **mpls te commit** command to commit the configuration.
  9. Run the **display interface tunnel** command to query the configuration of the tunnel.
- Configure the MPLS IP tunnel.

1. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
2. Run the **tunnel-protocol mpls ip** command to configure the tunnel protocol to MPLS IP, that is, configure the tunnel interface to work in the IP tunnel mode.
3. Run the **source** *ip_addr* command to configure the source IP address of the tunnel. Generally, the LSR ID of the ingress is used.
4. Run the **destination** *ip-address* command to configure the destination IP address of the tunnel. Generally, the LSR ID of the egress is used.
5. Run the **display interface tunnel** command to query the configuration of the tunnel.

----End

12.2.2 Configuring the Tunnel Policy

Configure the tunnel selection sequence for load balancing or the tunnel binding policy in the tunnel. After the configuration is successful, packets in the tunnel are processed according to tunnel policy.

Prerequisites

The PWE3 outer tunnel must be created.

Context

The tunnel selection sequence and the tunnel binding policy are mutually exclusive. This means that you can configure only one of them.

- The IP tunnel supports the configuration of only the tunnel selection sequence.
- The MPLS TE tunnel supports the configuration of only the tunnel binding policy.

Procedure

Step 1 Run the **tunnel-policy** command to create a tunnel policy name and enter the tunnel policy mode.

Step 2 For IP tunnel, run the **tunnel select-seq** command to configure the selection sequence of tunnels for load balancing.

To configure different tunnel types for load balancing according to priorities, run this command. The more the tunnel type close to keyword **select-seq**, the higher priority for load balancing.

The MA5600T/MA5603T does not support load balancing between different tunnels. In other words, tunnels for load balancing must be of the same type. The tunnels are selected according to the tunnel configuration.

Step 3 For MPLS TE tunnel, run the **tunnel binding** command to configure the tunnel binding policy.

To bind to a specified tunnel ID and configure the system to switch another tunnel according to the configured sequence when a tunnel is not available, run this command. After the tunnel binding policy is configured, run the **mpls te reserved-for-binding** command in the tunnel mode to allow the MPLS TE tunnel to be bound to the VPN instance.

destination *ip-addr* indicates the destination IP address of the tunnel, which must be the same as the destination IP address configured in the MPLS TE tunnel.

Step 4 In the global config mode, run the **display tunnel-policy** command to query the information about the tunnel policy.

----End

Example

To configure a tunnel policy named te_policy and bind to tunnels with the destination IP address 5.5.5.5 and IDs 10 and 20, do as follows:

```
huawei(config)#tunnel-policy te_policy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-te_policy)#tunnel binding destination 5.5.5.5 te 
tunnel
 10 tunnel 20
huawei(config)#display tunnel-policy
{ <cr>|string<S><Length 1-19> }:

  Command:
          display tunnel-policy
Total   tunnel policy num:              1
Sel-Seq tunnel policy num:              0
Binding tunnel policy num:              1
Invalid tunnel policy num:              0

Tunnel Policy Name  Destination     Tunnel Intf                   Down switch
-----------------------------------------------------------------------------
te_policy           5.5.5.5         tunnel10                      Disable
                                    tunnel20
```

12.2.3 Configuring the PWE3 Inner PW

Configure the attribute of PW and use the PW parameters for PW binding.

Prerequisites

- MPLS L2VPN must be enabled.
- The tunnel policy must be configured.

Context

PW parameters include the following parameters: control word, jitter buffer (only for TDM PWs), maximum transmission unit (MTU), loopback IP address of the peer device, PW type, RTP control header, virtual circuit connectivity verification (VCCV), used tunnel policy, flow label classification, and TDM load time (only for TDM PWs).

Different services have different configurations when the services are bound to a PW.

Procedure

Step 1 Run the **pw-para** command to create PW parameter.

PW parameters and the PW have a one-to-one mapping. One PW parameter can be used by only one PW.

Step 2 Run the **peer-address** command to configure the IP address of the peer device.

peer-address indicates the peer IP address in the PW for creating communication. In the actual transmission, data packets are automatically transmitted to the peer device according to this IP address.

Step 3 Run the **pw-type** command to configure the PW type.

The MA5600T/MA5603T supports TDM, ATM and ETH PWs.

The ATM PW is categorized as ATM NTo1 VCC and ATM SDU types.

- ATM NTo1 VCC: One or more ATM VCCs are transmitted on a PW.
- ATM SDU: Only the AAL5 CPCS-SDU payload is transmitted.

ETH PWs are categorized as raw and tagged modes.

- Raw mode: The PW VLAN tag is not carried in the upstream direction, but the PW payload can carry the SVLAN.
- Tagged mode: The payload of an upstream packet carries the PW VLAN tag, and the PW VLAN tag is removed in the downstream direction.

For the same PW, the PW types at both ends must be the same. In this way, the PW can be available.

⚠ **CAUTION**

Among PW parameters, the IP address and PW type of the peer device cannot be changed after they are configured. To change these two parameters, run the **undo pw-para** command to delete them first, and then configure them again. Make sure that the two parameters are correctly configured the first time, so as to prevent repeated operations.

Step 4 Run the **control-word** command to enable the control word mode.

When VCCV ping works in the control word mode, you need to enable the control word. It is recommended that you enable the control word mode.

Step 5 (Optional) Run the **pri-mapping-profile** command to bind an MPLS priority mapping profile to the PW.

The MPLS priority mapping profile can be configured by running the **mpls qos pri-mapping-profile** command. The profile includes the mapping from EXP to COS and the mapping from COS to EXP. To use different QoS policies based on different services for flexible mapping in the upstream and downstream directions, use this configuration.

By default, the MPLS priority mapping profile named default-profile-0 is bound to the ETH PW; the MPLS priority mapping profile named default-profile-1 is bound to the ATM PW; the MPLS priority mapping profile named default-profile-2 is bound to the TDM PW.

Step 6 (Optional) Run the **jitter-buffer** command to configure the jitter buffer.

The jitter buffer can effectively prevent jitter and delay. By default, the jitter buffer size is 2000 μs.

NOTE

- Only a TDM PW supports setting of the jitter buffer size.
- The jitter buffer size must be an integer multiple of 125.

Step 7 (Optional) Run the **mtu** command to configure the MTU.

Due to the limit in the system, the configurable MTU ranges for different PW types are different:

- MTU values set on the two devices at the ends of an ETH PW must be the same. If MTU values are different, an ETH PW can never be available.

- By default, the MTU is 1500 bytes. Do not modify this value unless there is a special requirement.

Step 8 Run the **rtp-header** command to configure the RTP control header.

NOTE

This command is applicable to only TDM PWs.

The length of the RTP header is 12 bytes, including the version number, padding flag, and timestamp fields. The timestamp field, whose length is 32 bits, is used for clock synchronization. For format of the RTP header, see RFC3550.

After RTP is enabled, PW packets of the TDM type carry the RTP control header. Otherwise, the RTP control header is not carried.

The RTP configuration must be the same as that on the peer PW device. By default, the MA5600T/MA5603T disables the RTP control header.

Step 9 Run the **vccv** command to enable VCCV, so as to notify the peer device of the VCCV types supported by the local device. After a successful negotiation between both devices, a virtual circuit connectivity verification is performed by using LSP ping according to the priority of the VCCV type.

VCCV is an end-to-end PW fault detection and diagnosis mechanism. Simply, VCCV is a control channel for the PW to send verification messages between the ingress and egress.

Enable the LSP ping function for alter, CW, and TTL channels or any of the three channels according to the VCCV types supported by the system. By default, VCCV is disabled.

Step 10 (Optional) Run the **tdm-load-time** command to configure the TDM load time.

NOTE

Only a TDM PW supports the setting of the load time.

Because each TDM frame is 125 μs, the load time must be an integer multiple of 125. If the entered number is not an integer multiple of 125, the system rounds it down to the nearest integer multiple of 125 μs. The jitter buffer must be greater than the load time.

The default jitter buffer is 1000 μs. Do not modify this value unless there is a special requirement.

Step 11 (Optional) Run the **tnl-policy** command to configure the tunnel policy used by the PW.

NOTE

The tunnel policy and the PW flow label classification are mutually exclusive. Configure either of them.

After the tunnel policy used by the PW is configured, the PW can perform load balancing or path selection according to the tunnel policy.

Step 12 (Optional) Run the **flow-label** command to enable flow classification.

NOTE

- The tunnel policy and the PW flow label classification are mutually exclusive. Configure either of them.
- Only the ETH PW supports flow label.
- Before configuring the flow label capability, make sure that the status of the flow label function on the local end is same as that on the peer end, and it is recommended that you adopt the same classification rules. If the flow label function is enabled on the local end but is disabled on the peer end, the packets carrying a flow label sent by the local end will be dropped after they arrive at the peer end, and the packet carrying no flow label will also be dropped after they arrive at the local end. As a result, services will be interrupted.
- After flow classification is enabled, you need to run the **mpls ecmp** command in the global config mode to enable the MPLS ECMP function. Then, the flow classification function takes effect.

To implement PWE3 load balancing, at the start point of the PW (ingress PE), the PW data is classified into different flows and each flow is allocated with a flow label. The downstream P node of the PW performs load balancing according to the flow labels.

The flow label supports the following flow classification by the source IP address, destination IP address, source MAC address, destination MAC and address, and any combination of the previous four IP addresses.

Step 13 (Optional) Run the **max-atm-cells** command to configure the maximum number of ATM cells that can be subtended.

Only the PW bound to a PW of the NTo1 VCC type requires the configuration of the maximum number of ATM cells that can be subtended. After the configuration, the number of ATM cells in the packet sent from the peer end cannot exceed this value. The default value is 1.

Step 14 (Optional) Run the **max-encapcell-delay** command to configure the packet delay of the ATM cell maximum group.

Only the PW of the NTo1 VCC type requires the configuration of the packet delay of the ATM cell maximum group. After the configuration, the maximum waiting time of subtended ATM cells encapsulated in a packet is the packet delay of the ATM cell maximum group. The default value is 0 ms.

CAUTION

If a PW is already set up and its adminstatus queried by running the **display pw** command is displayed as up, the attributes of the PW cannot be changed. Before changing the attributes, run the **manual-set pw-ac-fault** command to set the adminstatus of the PW to down. After the attributes are changed, run the **undo manual-set pw-ac-fault** command to set the adminstatus of the PW back to up. Then, the new configurations of the PW take effect.

Step 15 In the privilege mode or global config mode, run the **display pw-para** command to query the configuration of the PW.

----End

Example

To configure PW 10 with the following attributes, do as follows:

- IP address of the peer PW device: 10.10.10.20
- PW type: TDM SAToP E1
- Name of the tunnel policy used by the PW: **tdm-policy**
- Enable the RTP control header and the control word mode
- Enable the connectivity verification function of the alter, CW and TTL channels
- Other parameters: default settings

```
huawei(config)#pw-para 10
huawei(config-pw-para-10)#peer-address 10.10.10.20
huawei(config-pw-para-10)#pw-type tdm satop e1
huawei(config-pw-para-10)#tnl-policy tdm-policy
huawei(config-pw-para-10)#rtp-header
huawei(config-pw-para-10)#control-word
huawei(config-pw-para-10)#vccv cc cw alert ttl cv lsp-ping
huawei(config-pw-para-10)#quit
huawei(config)#display pw-para 10
  PW ID             : 10
  PeerIP            : 10.10.10.20
  Tnl Policy Name   : tdm-policy
  PW Type           : tdm satop e1
  CtrlWord          : enable
  VCCV Capability   : cw alert ttl/lsp-ping
  MTU               : 1500
  Statistic switch  : disable
  MaxAtmCells       : --
  MaxEncapDelay     : --
  RTP               : enable
  JitterBuffer      : 2000
  LoadTime(us)      : 1000
  TimeSlotNum       : 32
  PayLoadSize(bytes): 256
  FlowLabel Transmit            : --
  FlowLabel Classification-rule : --
  FlowLabel Receive             : --
  Priority mapping profile name : default-profile-2
```

To configure PW 20 with the following attributes, do as follows:

- IP address of the peer PW device: 10.20.30.40
- PW type: ETH Tagged
- Name of the tunnel policy used by the PW: **eth-policy**
- Other parameters: default settings

```
huawei(config)#pw-para 20
huawei(config-pw-para-20)#peer-address 10.20.30.40
huawei(config-pw-para-20)#pw-type ethernet tagged

huawei(config-pw-para-20)#tnl-policy eth-policy
huawei(config-pw-para-20)#quit
huawei(config)#display pw-para 20
  PW ID             : 20
  PeerIP            : 10.20.30.40
  Tnl Policy Name   : eth-policy
  PW Type           : ethernet tagged
  CtrlWord          : disable
  VCCV Capability   : disable
  MTU               : 1500
  Statistic switch  : disable
  MaxAtmCells       : --
  MaxEncapDelay     : --
  RTP               : --
  JitterBuffer      : --
  LoadTime(us)      : --
  TimeSlotNum       : --
  PayLoadSize(bytes): --
  FlowLabel transmit            : disable
  FlowLabel classification-rule : --
  FlowLabel receive             : disable
  Priority mapping profile name : default-profile-0
```

12.2.4 Binding the Service to the PW

Bind various PWE3 services to a PW. After the binding, user packets are encapsulated and forwarded according to the modes defined in the PW parameters.

Prerequisites

- The PW must be configured.
- For TDM PWE3, the TDM connection must be created.

- For ATM PWE3, the ATM-based service port must be created.
- For ETH PWE3, the ETH-based service port must be created.

Context

Different PWE3 services have different configurations when the services are bound to a PW.

- TDM PWE3 supports dynamic PW and static PW.
- ATM PWE3 supports dynamic PW and static PW.
- ETH PWE3 supports dynamic PW and static PW.

The parameters of a static PW are not negotiated using the signaling protocol, the relevant information is configured manfully through the command line interface (CLI), and the data is transmitted through tunnels between PEs.

Procedure

- Bind the TDM service to a PW.

  Run the **pw-ac-binding tdm** command to use a PW to create the TDM PW service.

  Pay attention to the following points during the configuration:

  - To specify a PW as a static PW, you need to configure the in label and out label of the PW. The out label value must be an unallocated and idle value at the peer end and the in label value must be an unallocated value at the local end.
  - To specify a PW and an UDP PW, you need to configure the destination port ID and source port ID of the PW. The destination port ID must be the same as the source port ID at the peer PW device and the source port ID must be the same as the destination port ID at the peer PW device.
- Bind the ATM service to a PW.

  Run the **pw-ac-binding pvc** command to use a PW to create the ATM PW service.

  The PVC and the PW can be bound in two modes: NTo1 mode and SDU mode. Pay attention to the following points during the configuration:

  - In the SDU mode, a PW is bound to only one PVC. Therefore, you need not change the VPI or VCI.
  - In the NTo1 mode, a PW can be bound to multiple PVCs. To differentiate between PVCs, you must change the out VPI and VCI of the PW, that is, you must specify **outvpi** and **outvci**. Operation procedure is as follows:

    1. Run the **pw-ac-binding pvc** command to bind a PW to a PVC.
    2. Run the **pw-ac-append pvc** command to bind the PW to another PVC.
- Bind the ETH service to a PW.

  Run the **pw-ac-binding vlan** command to use a PW to create the ETH PW service.

  Note: To specify a PW as a static PW, you need to configure the in label and out label of the PW. The out label value must be an unallocated and idle value at the peer end and the in label value must be an unallocated value at the local end.

----End

Example

To create a static binding between TDM connection 0 and PW 20 (outgoing label/incoming label: 16/8448), do as follows:

```
huawei(config)#pw-ac-binding tdm 0 pw 20 static transmit-label 16 receive-label 8448
```

To bind the ATM service to a PW with the following settings, PW type to ATM sdu, do as follows. Settings: ATM access port 0/3/0, VPI/VCI 0/35, and PW ID 20.

```
huawei(config)#pw-ac-binding pvc 0/3/0 vpi 0 vci 35 pw 20
```

To bind the ETH service to a PW with the following settings, do as follows. Settings: VLAN ID 100, PW ID 30, PW out label 8500, and PW in label 8600.

```
huawei(config)#pw-ac-binding vlan 100 pw 30 static transmit-label 8500 receive-
label 8600
```

12.2.5 Configuring PW Protection

Create a standby PW for a PW. When the active PW is faulty, the system quickly switches to the standby PW to ensure the service reliability.

Prerequisites

- The active PW must be created.
- The basic parameters are configured. For the configuration method, see **12.2.3 Configuring the PWE3 Inner PW**.

Context

PW protection: When a PW is faulty (such as an LDP session is down, a tunnel is deleted, the protocol communication is faulty, the route status changes, or VCCV has no response), the system can quickly switch to the standby PW. Then, the standby PW functions as the active PW.

The MA5600T/MA5603T supports PW 1:1 redundancy.

Procedure

Step 1 Run the **pw-protect** command to configure the standby PW.

Pay attention to the following points during the configuration:

- The standby PW ID cannot exist.
- The PW parameters of the active and standby PWs must be the same.
- Both active PW and the standby PW are not static PW.

Step 2 (Optional) Enable the PW protection group to support dual-sending and dual-receiving for the multicast service.

When the PW protection group supports dual-sending, both active and standby PWs can forward IGMP packets so that the multicast forwarding entry can also be created on the device corresponding to the standby PW. After the active/standby PW switchover, the multicast service can be smoothly switched. This configuration is recommended when the multicast service is carried by the active and standby PWs.

When the PW protection group supports dual-receiving, both active and standby PWs can receive packets to avoid packet loss caused by signaling delay when switchback is performed after the faulty active PW recovers. This configuration is recommended when the multicast service is carried by the active and standby PWs.

1. Run the **igmp_send_dual-pw** command to set whether IGMP packets can be sent by both active and standby PWs.
2. Run the **pw-redundancy_stream-dual-receiving** command to set the PW protection group to work in the dual-receiving mode.

Step 3 Run the **pw-revertive-mode** command to configure the switchback policy for the PW protection group.

Switchback: When both active and standby PWs are available, if the original service traffic is carried on the standby PW, the service can be switched back to the active PW according to actual requirements. Set the switchback policy according to actual network conditions (such as whether the network topology often changes and whether the traffic should be carried on the active PW).

The switchback policy of a PW protection group can be immediate automatic switchback, automatic switchback after a period of time, and no automatic switchback.

Step 4 Run the **display pw-ps** command to query the configuration of the PW protection group.

----End

Example

To configure a PW protection group, set the parameters as follows: active PW ID to 10, standby PW ID to 20, and switchback policy to allowing automatic switchback for the PW protection group in 30 seconds.

```
huawei(config)#pw-protect primary-pw 10 secondary-pw 20
huawei(config)#pw-revertive-mode 10 revertive wtr 30
huawei(config)#display pw-ps 10
  ----------------------------------------------------------------------------
  Primary-PW-ID     Primary-PW-state     Secondary-PW-ID     Secondary-PW-state
  ----------------------------------------------------------------------------
             10            up/active                  20                   down
  ----------------------------------------------------------------------------
  revertive-mode: revertive, in 30 seconds
```

12.2.6 Configuring MPLS Tunnel Protection

Create a protection tunnel for the MPLS TE tunnel. When the working tunnel is faulty, the system quickly switches to the protection tunnel to ensure the service reliability.

Prerequisites

- The forward LSP must be created.
- The backward LSP must be created.
- MPLS OAM must be enabled.

Context

MPLS tunnel protection is a part of the MPLS OAM connectivity detection mechanism.

The basic process of the MPLS OAM connectivity check and protection switching is as follows:

1. The source transmits the CV/FFD packets to the destination through the detected LSP.

2. The destination checks the correctness of the type and frequency carried in the received detection packets and measures the number of correct and errored packets that are received within the detection period to monitor the connectivity of the LSP in real time.
3. After detecting a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward path.
4. The source learns about the status of the defect, and triggers the corresponding protection switching when the protect group is correctly configured.

Procedure

Step 1 Configure working MPLS TE tunnel.

1. In global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
2. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE.
3. Run the **destination** *ip-address* command to configure the destination IP address of the tunnel. Generally, the egress LSR ID is used.
4. Run the **mpls te tunnel-id** command to configure the tunnel ID.
5. Run the **mpls te signal-protocol rsvp-te** command to configure the signaling protocol of the tunnel to RSVP-TE.
6. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface that meets this bandwidth value can be selected as the node traversed by the MPLS TE tunnel path when the MPLS TE tunnel is created.

   If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the tunnel bandwidth.
7. (Optional) Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.

   If only the bandwidth used by the MPLS TE tunnel is limited but the transmission path is not limited, you may not configure the explicit path used by the MPLS TE tunnel.
8. Run the **mpls te commit** command to commit the current configuration of the tunnel.

Step 2 Configure protection MPLS TE tunnel.

The working mode of MPLS OAM protection switching is 1:1 protection. Normally, each working tunnel has a protection tunnel.

The configuration of the protection tunnel is the same as that of the working tunnel.

Step 3 Configure a tunnel protect group.

Configure the working tunnel and the protection tunnel as a tunnel protect group. When the source end finds the active LSP is defective through the MPLS OAM detection mechanism, and the protection switching is required, the system can switch the data to the protection tunnel for continuous transmission.

1. In the global config mode, run the **interface tunnel** command to enter the working tunnel interface mode.
2. Run the **mpls te protection tunnel** command to create a tunnel protect group and set the switchback mode of the protect group.

   The switchback policy of a PW protect group can be immediate automatic switchback, automatic switchback after a period of time, and no automatic switchback.

Step 4 (Optional) Run the **mpls te protect-switch** command forcibly switch over the tunnel protect group.

To manually switch data streams between working and protection tunnels, run this command.

There are for forcible switching modes:

- **clear**: clears all external switching commands that are already executed in the system.
- **lock**: lock switching, which locks data streams on the working tunnel.
- **force**: forcible switching, which forcibly switch data streams to the protect tunnel.
- **manual work-lsp**: manually switches data streams on the working tunnel to the protection tunnel.
- **manual protect-lsp**: manually switches data streams on the protection tunnel to the working tunnel.

Keywords **clear**, **lock**, **force**, and **manual** corresponds to switching priorities in descending order. If a command with a higher priority is executed, a command with a lower priority cannot be executed.

Step 5 In the global config mode, run the **display mpls te protection tunnel** command to query the configuration of the tunnel protect group.

----End

Example

To configure RSVP-TE tunnel IDs to 10 and 30, destination IP address of the tunnels to 3.3.3.3, tunnel 30 as the protection tunnel of tunnel 10, switchback mode to revertive, and WTR time to 900s, do as follows:

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
huawei(config-if-tunnel10)#destination 3.3.3.3
huawei(config-if-tunnel10)#mpls te tunnel-id 10
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel10)#mpls te bandwidth ct0 5120   //(Optional) Configure the 
global bandwidth of tunnel 10 to 5210 kbit/s.
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
huawei(config)#interface tunnel 30
huawei(config-if-tunnel30)#tunnel-protocol mpls te
huawei(config-if-tunnel30)#destination 3.3.3.3
huawei(config-if-tunnel30)#mpls te tunnel-id 30
huawei(config-if-tunnel30)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel30)#mpls te bandwidth ct0 5120   //(Optional) Configure the 
global bandwidth of tunnel 30 to 5210 kbit/s.
huawei(config-if-tunnel30)#mpls te commit
huawei(config-if-tunnel30)#quit
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#mpls te protection tunnel 30 mode revertive wtr 30
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

12.2.7 Configuring PW-based trTCM by CoS Remarking

In an asynchronous transfer mode (ATM) multi-protocol label switch (MPLS) network, quality of service (QoS) is required for the user ATM cells carried in ATM pseudo wire emulation edge to edge (PWE3) over the packet switched network (PSN) network. Due to mechanism differences, two rate three color marker (trTCM) by class of service (CoS) remarking is implemented on the ingress PE (MA5600T/MA5603T) to map ATM traffic policing mechanism to the MPLS traffic policing mechanism, and CoS-based early drop is implemented on the egress PE.

Prerequisite

The specified PW is configured.

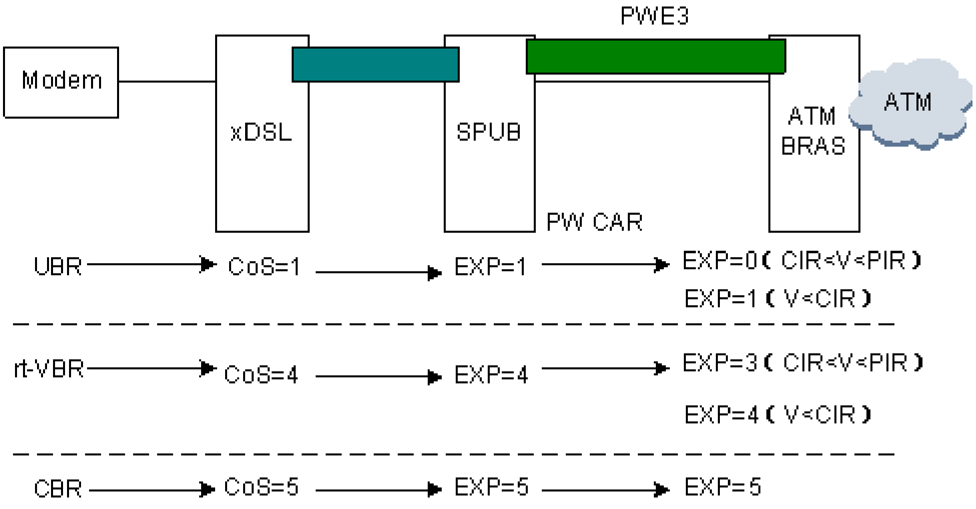
Context

In the ATM MPLS network, certain upper-layer ATM devices fail to identify the DEI bit in the VLAN Tag field and therefore fail to implement trTCM by the DEI bit for ATM private line user. In this case, in the upstream direction of an ingress PE (MA5600T/MA5603T), trTCM by CoS remarking is performed according to PW committed access rate (CAR). With this mechanism, MPLS packets whose rate is lower than committed information rate (CIR) are green packets. They are marked with the default CoS value, and MPLS packets who rate is higher than CIR and lower than peak information rate (PIR) are yellow packets. Their CoS values are remarked by the system by running the **cos-remark** command. while MPLS packets who rate are red packets. They are directly discarded by the system. When a PW packet is being encapsulated, the CoS of the MPLS packet is mapped to the EXP field of the outer MPLS label (the EXP field of the inner PW label is also processed in this way). Then, traffic management is performed in the PSN network based on the EXP field of the MPLS label.

In the downstream direction of an egress PE, if the color policy of the traffic profile is **cos**, packets are discarded based on CoS values in the EXP field. The packets carrying the default CoS value and remarking low-priority CoS values are mapped to the same queue. Then, different early-drop thresholds are configured for packets with different colors in the queue to ensure that packets whose rate is lower than CIR have a higher priority when congestion occurs.

In the upstream direction, the MA5600T/MA5603T implements PW-based trTCM for CIR and PIR by CoS remarking on the SPUB board, as shown in **Figure 12-4**. In the downstream direction, the MA5600T/MA5603T does not perform CAR or CoS-based early drop on the SPUB board, but implements queue-based early drop on the xDSL board according to the CoS early drop threshold.

Figure 12-4 PW-based trTCM on the upstream SPUB board



NOTE

- V indicates the rate of the MPLS packet.
- In the downstream direction, the CoS value processing on theMA5600T/MA5603T is reverse to that in the upstream direction.

Procedure

- Configure trTCM by CoS remarking in the upstream direction.
  1. Run the **mpls car-pw** command to configure PW-based rate limitation.

     In the upstream direction of an ingress PE, the system remarks packets with different rates with different colors based on the CIR and PIR parameters and discards the red packets.

     - Only the upstream packets on the SPUB board are remarked.
     - The CAR parameters of a PW can be configured only after the MPLS L2 VPN function is enabled by running the **mpls l2vpn** command.
     - CIR is mandatory, and the other three parameters are optional. If you configure only the CIR, the system calculates the other three parameters based on the formula. It is recommended to configure only the CIR. The relationships between these parameters are as follows:
       - CBS = (CIR+8191)/8192+1
       - PIR = 2*CIR
       - PBS = MAX(((PIR+8191)/8192+1), CBS)
  2. Run the **cos-remark** command to configure the priority remarking policy of trTCM.

     The system remarks the priorities of yellow packets with a low-priority CoS value. In the downstream direction of an egress PE, if the color policy of the traffic profile used by the traffic stream is **cos**, priority-based early drop is implemented.

     - By default, the CoS value remarked is the same as the original value.
     - The CoS value remarked is low-priority CoS value while the other CoS value is the high-priority CoS value. The high-priority CoS value can be remarked as the low-priority CoS value while the low-priority CoS value can only be remarked as itself. For example, when priority A is remarked as priority B, A is the high-priority CoS value and B is the low-priority CoS value. Priority B can only be remarked as priority B.
- Configure CoS-based early drop in the downstream direction.
  1. Run the **traffic table ip** command to create an IP traffic profile for AoE streams. To implement CoS-based early drop for AoE streams, the color policy must be set to **cos**.
     - Only the ADSL and SHDSL boards support early drop for the downstream packets.
     - The default color policy is **dei**.
     - The color policy in the upstream and downstream traffic profiles used by the traffic stream must be the same.
     - **traffic table ip** indicates traffic stream-based rate limitation and **mpls car-pw** indicates PW-based rate limitation. If more than one rate limitation modes are configured in the system, the minimum rate is used.

   - CIR is mandatory, and the other three parameters are optional. If you configure only the CIR, the system calculates the other three parameters based on the formula. It is recommended to configure only the CIR. The relationships between these parameters are as follows:
      - CBS = min(2000+CIR*32, 10240000)
      - PIR = min(2*CIR, 10240000)
      - PBS = min(2000+32*PIR, 10240000)

2. Run the **cos-queue-map** command to configure the mapping between queues and CoS values (802.1p priority) so that packets with different priorities are mapped to the specified queues based on the configured mapping. This enhances the flexibility of mapping packets to the queue.
   - The larger the queue ID, the higher the priority for forwarding packets.
   - The default mapping between priorities and queue IDs is: Priority 0 maps to queue 0; priority 1 maps to queue 1; the same rule applies to other priorities.
   - A PVC may have two different CoS values: a default CoS value and a remarked CoS value. To ensure that packets with these two CoS values are in correct sequence during AoE encapsulation, the packets are mapped to the same queue.
   - It is recommended that the same type of permanent virtual paths (PVCs) be encapsulated into the same PW. Otherwise, different types of PVCs have the same EXP value and service-based queue scheduling cannot be implemented.
3. Run the **wred-profile** command to add a weighted random early detection (WRED) profile. Configure the early-drop thresholds and drop ratios for the green and yellow packets.
4. Run the **queue-wred** command to bind the WRED profile to queues. After the WRED profile is bound, the system performs color-based early drop according to the parameters configured in the WRED profile.

----End

Example

Assume that in the upstream direction of the MA5600T/MA5603T, CIR of PW 10 is 1 Mbit/s and yellow packets are remarked with CoS 0; in the down stream direction, green packets are not dropped, low drop threshold for yellow packets is 50, high drop threshold 80, and drop ratio 100. In an ATM MPLS network, to create the AoE service port (no CAR for the service port) by referencing traffic profile 8 (in which the VLAN priority is set to 1) to provision 1 Mbit/s service the ATM private line user, do as follows:

```
huawei(config)#mpls car-pw 10 cir 1024
huawei(config)#cos-queue-map cos1 0 cos4 3
huawei(config)#traffic table ip index 8 name "CBR" cir off color-policy cos
priority 1 priority-policy tag-in-package
huawei(config)#service-port 2 vlan aoe adsl 0/2/0 vpi 0 vci 35 single-service
inbound traffic-table index 8 outbound traffic-table index 8
huawei(config)#cos-queue-map cos0 0 cos1 0 cos3 1 cos4 1 cos5 5 cos2 3 cos6 3 cos7
3
huawei(config)#wred-profile index 6 green low-limit 100 high-limit 100
discard-probability 0 yellow low-limit 50 high-limit 80 discard-probability
100
huawei(config)#queue-wred queue0 6 queue1 6 queue2 6 queue3 6
```

nx

13 Configuring VPLS MP2MP Intercommunication

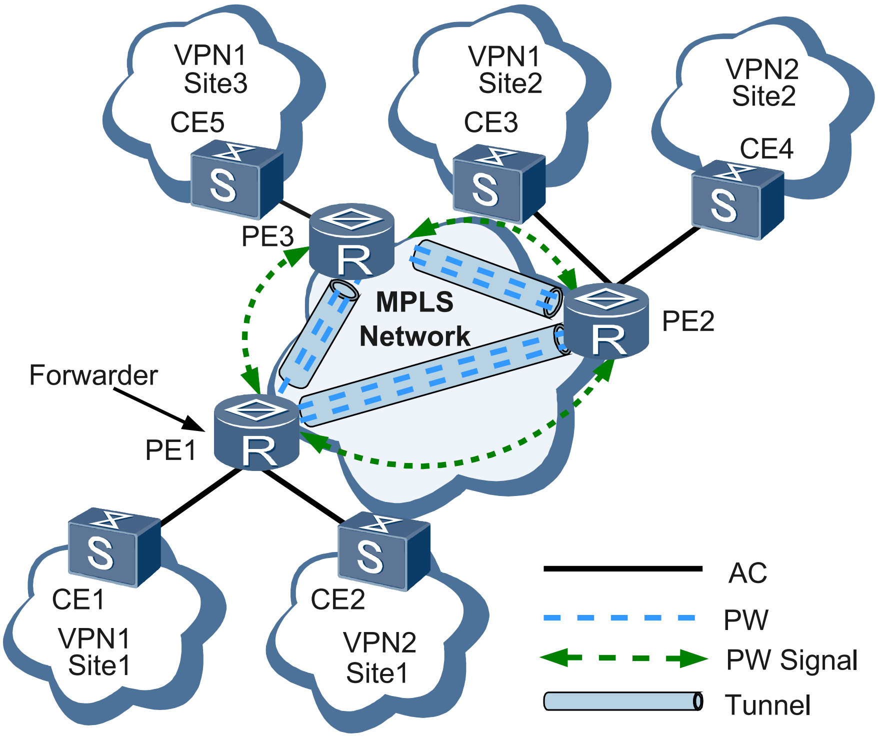
VPLS can implement the multipoint-to-multipoint (MP2MP) VPN networking; therefore, by using the VPLS technology, service providers (SPs) can provide the Ethernet-based multipoint services through MPLS backbone networks.

Application Context

A lot of private line services in carriers' network use the virtual private network (VPN) virtual private wire service (VPWS) technology, which can provide point-to-point (P2P) communication services on Layer 2 or Layer 3 network. With the development of Ethernet and MPLS technologies, carriers hope to provide not only P2P services on the private network, but Ethernet-like point-to-multipoint (P2MP) services on the metropolitan area network (MAN) and wide area network (WAN). By deploying virtual private LAN service (VPLS) technology on the provider edge (PE), carriers can provide Ethernet-based MP2MP services for users through MPLS backbone networks, achieving the local area network (LAN) simulation.

Figure 13-1 shows the basic VPLS transmission process. Full-meshed PWs are created through signaling transmission by PE routers. Transmission of packets between CEs relies on VSIs configured on PEs, and PWs established between the VSIs.

Figure 13-1 Basic VPLS transmission process



Prerequisite

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The VLAN for MPLS label forwarding must be created.
4. The global MPLS, VLAN MPLS, and VLAN interface MPLS must be enabled.
5. MPLS L2VPN must be enabled.
6. A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).
7. The global LDP function is enabled and remote LDP sessions are configured.
8. The vlan-based traffic stream must be created.

Data Plan

Before configuring the VPLS P2MP intercommunication services, plan the data items as listed in **Table 13-1**.

Table 13-1 Plan of VPLS P2MP intercommunication service data items

Item	Data	Remarks
MA5600T/ MA5603T	VSI	VLANs are mapped to the VPLS domain after a VSI is bound to the VLAN and PW. VLAN mapping allows service packets to be broadcast in the VPLS domain.
	VPLS PW	-

Procedure

Step 1 Configure a VSI.

VSIs are the core of VPLS services. With VSIs, actual links carrying VPLS services can be mapped into PWs.

1. In global config mode, run the **vsi** command to create a VSI and enter the VSI mode.
2. Run the **pwsignal ldp** command to configure the signaling type for VSI as LDP.

   Currently, you can only configure the signaling type for VSI as LDP.
3. Run the **vsi-id** command to configure the VSI ID.

   Once the VSI ID is successfully set, it cannot be changed or deleted. If you need to change it, delete the VSI.

Step 2 (Optional) Configure VSI attributes.

In VSI mode, configure VSI basic attributes based on actual requirements. VSI basic attributes include the VSI description information, encapsulation type, control words, maximum transmission unit (MTU), and traffic suppression.

- Run the **description** command to configure the description of a VSI.
- Run the **encapsulation** command to configure the encapsulation type of a VSI.
- Run the **control-word** command to enable the control word of a VSI. After the control word is enabled, control information will be added to packets.

  NOTE

  If you use the **control-word** command in VSI mode and the **control-word** command in PW-para-index mode to configure the control word concurrently, the one set by the **control-word** command in PW-para-index mode takes effect.
- Run the **mtu** command to set the MTU of a VSI.
- Run the **traffic-suppress** command to set the suppression level of the broadcast, unknown multicast, and unknown unicast traffic for a VSI.

  Before configuring the multicast service carried in VPLS, you must disable the VSI unknown multicast supression. Otherwise, packet loss will occur in the multicast services.

Step 3 Configure PWs.

1. In global config mode, run the **pw-para pwindex** *pwindex* command to create a PW and enter the PW-para-index mode.

   For a VPLS PW, you must first create the PW-para-index mode and then perform the PW binding.

2. Run the **service-type vpls** command to configure the service type of a PW as VPLS.
3. Run the **pwid** command to configure the ID of a PW.
4. Run the **peer-address** command to set the IP address of the peer device of a PW.
5. Run the **pw-type ethernet** command to configure the type of a PW as Ethernet.

   When the service type is VPLS, you can set the PW type only to **Ethernet**. The PW type must be identical to the VSI encapsulation type.
6. (Optional) Run the **control-word** command to enable the control word of a PW.
7. Run the **dyn-receive-label** command to specify the incoming label of a dynamic PW.

Step 4 In VSI mode, run the **vsi-pw-binding** command to bind the VSI to the PW to create a VPLS PW service.

Step 5 In VSI mode, run the **vsi-ac-binding vlan** command to bind a VLAN to the VSI.

After the above configurations are complete, VLAN service packets can be forwarded within a VSI.

----End

Example

Assume that VLAN 100 is used for MPLS forwarding, a VSI and a PW are created, and the PW and VLAN 100 are bound to the VSI respectively. To configure VSI and PW parameters as follows:

- To set the VSI ID to **1**, the VSI name to **hsi**, and the signaling mode to **LDP**, and retain the default values for other parameters, do as follows:
- To set the PW index to **1**, the service type to **VPLS**, the PW ID to **1**, the IP address of the peer device to **1.1.1.1**, the encapsulation type to **Ethernet tagged**, and the dynamic PW incoming label to **10240**, do as follows:

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#pwsignal ldp
huawei(config-vsi-hsi)#vsi-id 1
huawei(config-vsi-hsi)#quit
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 1.1.1.1
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#vsi-pw-binding pwindex 1
huawei(config-vsi-hsi)#vsi-ac-binding vlan 100
```

14 Configuring Network Protection

About This Chapter

The MA5600T/MA5603T provides a powerful redundancy backup mechanism. The redundancy or backup implements the high reliability and self-healing capability of the system. In this way, when an exception occurs, the stability of the services and customer network provided by the carrier can be optimally ensured and the loss is reduced to the minimum.

Context

In the carrier-class operation, to ensure that the system to work normally in case of an accident or disaster, generally, redundancy (backup) devices or parts are added to increase the reliability of the entire system.

14.1 Configuring Ethernet Link Aggregation
Configure Ethernet link aggregation to increase link bandwidth and improve link reliability, without performing a hardware upgrade.

14.2 Configuring an Ethernet Port Protection Group
The MA5600T/MA5603T allows two Ethernet ports to be bound together to provide protection. If the working port is faulty, the system switches services to the protection port. This ensures uninterrupted service forwarding and improves the reliability of links.

14.3 Configuring the Smart Link Redundancy Backup
The smart link is a solution that is applied in the network with dual uplinks and provides reliable and efficient backup and quick switching for the dual uplinks. The solution provides high reliability for carriers' network.

14.4 Configuring ARP Detection (for Accelerating Protection Switching)
Address Resolution Protocol (ARP) probe enables faster protection switching by detecting status of end-to-end links. ARP detection can be configured for a network scenario in which a link protection group is configured for the upstream Ethernet ports on the access device, and there are other types of devices deployed, such as switches and transmission devices, between the access device and the aggregation devices.

14.5 Configuring the MSTP
The MA5600T/MA5603T supports the application of the Multiple Spanning Tree Protocol (MSTP), Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP). The

MA5600T/MA5603T supports the MSTP ring network, which can meet various networking requirements.

14.6 Configuring VRRP Transparent Transmission in the S+C Forwarding Mode
In the S+C forwarding mode, after VRRP snooping is enabled, VRRP packets can be forwarded between two isolated upstream ports.

14.7 Configuring RRPP
Rapid Ring Protection Protocol (RRPP) is a data link layer protocol specially applied to the Ethernet ring. When the Ethernet ring is complete, RRPP can prevent broadcast storms caused by a data loop. When a link on the Ethernet ring is disconnected, RRPP can quickly recover the communication channels between nodes on the Ethernet ring, increasing the network reliability.

14.8 Configuring the BFD
This topic describes how to configure the BFD on the MA5600T/MA5603T.

14.9 Configuring ETH OAM
In a broad sense, operation, administration, and maintenance (OAM) means a set of methods for monitoring and diagnosing network faults. The Ethernet OAM feature includes two sub-features: Ethernet CFM OAM and Ethernet EFM OAM.

14.10 Configuring GPON Protection
The MA5600T/MA5603T supports Type B, Type C protection. This topic describes the configuration of each type of protection.

14.1 Configuring Ethernet Link Aggregation

Configure Ethernet link aggregation to increase link bandwidth and improve link reliability, without performing a hardware upgrade.

Prerequisites

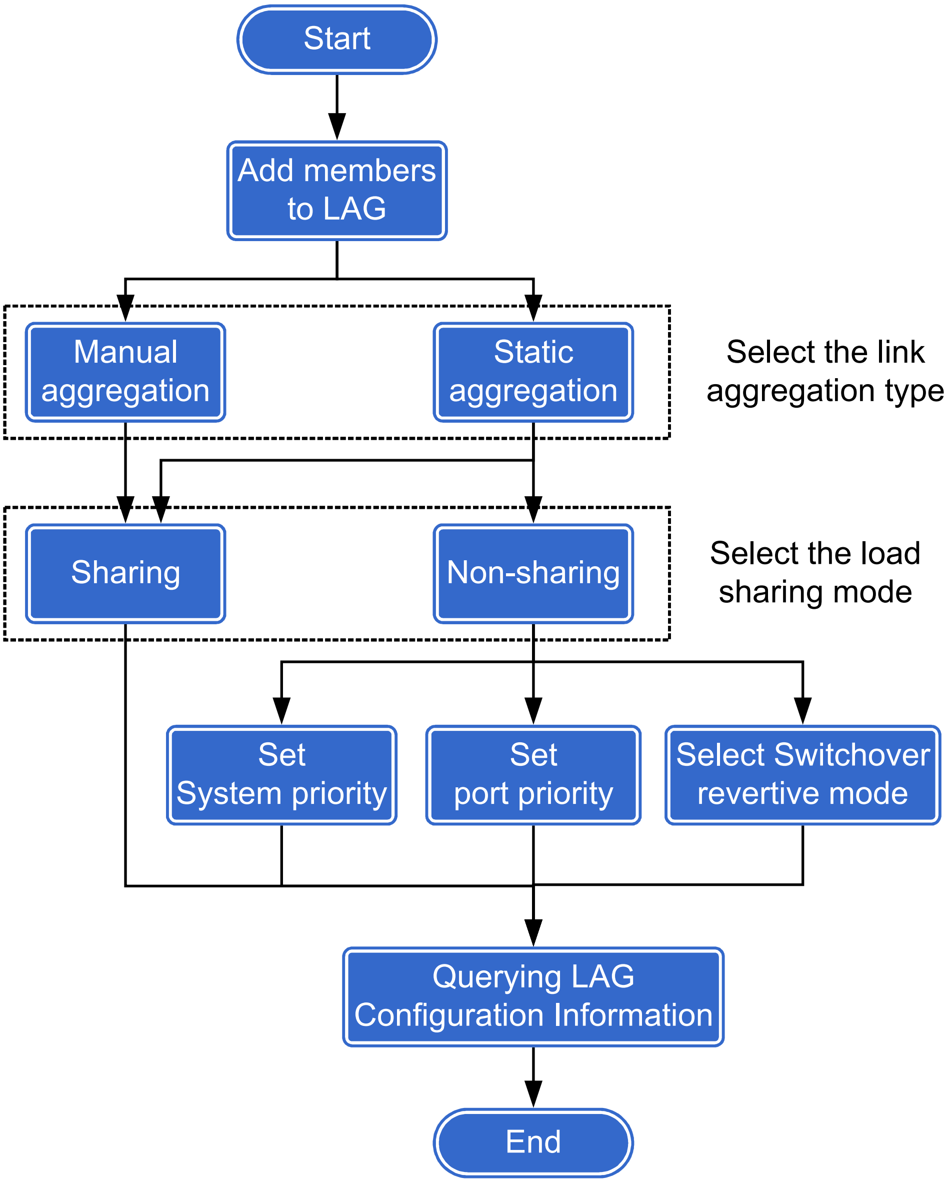
- Interconnected devices, hardware, and port attributes must support LAGs. For details, see Feature Dependency and Limitation in *Ethernet Link Aggregation* of the Feature Description.
- The two aggregated ports do not have static MAC addresses. You can run the **display mac-address** command to query whether an aggregated port has static MAC address.

Context

For details about Ethernet link aggregation, see *Ethernet Link Aggregation* in the **Feature Description**.

Figure 14-1 shows the flowchart for configuring a LAG.

Figure 14-1 Configuration flowchart


Start
Add members to LAG
Manual aggregation
Static aggregation
Select the link aggregation type
Sharing
Non-sharing
Select the load sharing mode
Set System priority
Set port priority
Select Switchover revertive mode
Querying LAG Configuration Information
End

Procedure

Step 1 (Mandatory) Create a LAG and select the aggregation type.

Run the **link-aggregation** command to add multiple upstream Ethernet ports to the same LAG to implement protection and load sharing between ports.

NOTE

If the device is interconnected with the device that supports LACP, static aggregation is recommended. If the device is interconnected with the device that does not support LACP, only manual aggregation can be used.

Step 2 (Optional) Add a LAG member port.

Perform this step when the LAG bandwidth or link reliability needs to be improved further. Run the **link-aggregation add-member** command to add an Ethernet port to an existing LAG to increase the LAG bandwidth and improve the link reliability.

NOTE

If the port to be added to or deleted from a LAG is connected to the peer device, run the **shutdown(Ethernet)** command to deactivate the Ethernet port or remove the optical fiber to prevent loops.

Step 3 (Optional) Select the load carrying type.

NOTE

If the load sharing type is not configured, a LAG works in load sharing mode by default.

This step is required only when a static LAG is configured. Configuring the maximum selected links in a LAG implements traffic allocation in load non-sharing mode. For example, M+N links are configured in a LAG. Then, run the **link-aggregation max-link-number** command to specify N selected links. The remaining M links are standby ones. If a selected link is disconnected, a standby link automatically changes to the selected one.

Step 4 (Optional) Set the system priority and port priority.

This step is required only when a static LAG is configured.

- LACP system priority: If the access device is dual homed to two convergence devices, the access device determines the selected and standby LAGs. Run the **lacp priority system** command to set the LACP system priority of the access device to be higher than that of the peer device.
- LACP port priority: LACP port priority must be used together with the maximum number of links. If a port is required preferentially for carrying services, set its priority higher. Run the **lacp priority port** command to change the link priority so that the standby link and the selected link can be switched over.

Step 5 (Optional) Selected the link revertive mode.

This step is required only when a static LAG in load non-sharing mode is configured. Run the **lacp preempt** command to set whether traffic is switched back to the original link if the link failure is rectified.

Step 6 (Optional) Query LAG information.

Run the **display link-aggregation** command to query the LAG information, including primary port, number of links, aggregation type (manual or static), and maximum number of links.

----End

Example

Assume the following configurations: The MA5600T/MA5603T transmits services upstream using the GIU board, upstream ports 0/19/0 and 0/19/1 on the same GIU board are configured in an upstream port LAG, packets are distributed to the LAG member ports according to the source MAC address, and the working mode is LACP static aggregation. To perform these configurations, run the following commands:

NOTE

The network topology is shown in "Upstream Transmission of Intra-Board Link Aggregation" in Applications of the Feature Description.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
huawei(config)#display link-aggregation all
  -------------------------------------------------------------------------
  Master port  Link aggregation mode  Port NUM  Work mode  Max link number
  -------------------------------------------------------------------------
  0/19/0       ingress                       2  lacp-static               -
  -------------------------------------------------------------------------
  Total: 1 link aggregation(s)
```

Assume the following configurations: The MA5600T/MA5603T transmits services upstream using the GIU board, upstream ports 0/19/0 and 0/20/0 on the active and standby GIU control boards are configured in an inter-board LAG, packets are distributed to the LAG member ports according to the source MAC address and destination MAC address, and the working mode is LACP static aggregation. To perform these configurations, run the following commands:

NOTE

The network topology is shown in "Upstream Transmission of Inter-Board Link Aggregation (Single Homing)" in Applications of the Feature Description.

```
huawei(config)#link-aggregation 0/19 0 0/20/0 0 egress-ingress workmode lacp-
static


huawei(config)#display link-aggregation all
  -------------------------------------------------------------------------
  Master port  Link aggregation mode  Port NUM  Work mode  Max link number
  -------------------------------------------------------------------------
  0/19/0       egress-ingress                2  lacp-static              -
  -------------------------------------------------------------------------
  Total: 1 link aggregation(s)
```

Assume the following configurations: The MA5600T/MA5603T is configured with only one control board, the SCUN control board and the GIU board are configured in an inter-board LAG, packets are distributed to the LAG member ports according to the source MAC address, and the working mode is LACP static aggregation. To perform these configurations, run the following commands:

```
huawei(config)#link-aggregation 0/9 0-3 0/19 0-1 ingress workmode lacp-static

huawei(config)#display link-aggregation all
  -------------------------------------------------------------------------
  Master port  Link aggregation mode  Port NUM  Work mode  Max link number
  -------------------------------------------------------------------------
  0/9 /0       ingress                       6  lacp-static              -
  -------------------------------------------------------------------------
  Total: 1 link aggregation(s)
```

14.2 Configuring an Ethernet Port Protection Group

The MA5600T/MA5603T allows two Ethernet ports to be bound together to provide protection. If the working port is faulty, the system switches services to the protection port. This ensures uninterrupted service forwarding and improves the reliability of links.

The MA5600T/MA5603T supports two types of Ethernet port protection groups:

- Portstate protection group: Applies to a network scenario in which the control board provides upstream ports, and protection is available at link level, link aggregation group (LAG) level, or board level. In the upstream direction, the access device is usually single-homed to a transmission device.
- Timedelay protection group: Applies to a network scenario in which the system control board or upstream board provides upstream ports, and protection is available only at link level. In the upstream direction, the access device can either be single-homed or dual-homed to aggregation devices.

14.2.1 Configuring a Link-Level Portstate Protection Group on the Control Board

A link-level Portstate protection group applies to the following scenario: The active and standby control boards on an access device each provide an upstream Ethernet port, and users want the upstream Ethernet port (working port) on the active control board to carry services and the upstream Ethernet port (protection port) on the standby control board to back up. If the working port is faulty, the system switches services to the protection port to implement uninterrupted forwarding.

Prerequisites

- The boards and ports on the access device support Ethernet port protection groups. For details, see Feature Dependency and Limitation in "Ethernet Port Protection Group" of Feature Description.
- In the protection group, a static MAC address is configured only on the working port. You can run the **display mac-address** command to query the static MAC address.
- The two ports on the interconnected device have the same data configurations and allow MAC address transfer (the same MAC address learned on different ports).

Context

For details on a Portstate protection group, see Ethernet Port Protection Group in Feature Description.

Procedure

Step 1 Configure a link-level Portstate protection group on the control board.

Run the **protect-group** command to create a protection group (select **as-mainboard-port** as the protection level and **Portstate** as the protection type).

Step 2 Add a working port and a protection port to the protection group.

Run the **protect-group member** command to add a port on the control board as the working port and a port on the standby control board as the protection port in the protection group.

Step 3 Enable the protection group.

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

Step 4 Query configurations about the protection group.

Run the **display protect-group** command to query configurations about the protection group. The configurations include the protection level, member ports, protection type, and reversion mode.

----End

Example

This example assumes a scenario in which two control boards on the MA5600T/MA5603T each provide an upstream port: 0/9/0 on the active control board and 0/10/0 on the standby control board. The two upstream ports form a link-level Portstate protection group.

NOTE

For details on the application diagram, see Application in "Ethernet Port Protection Group" of Feature Description.

To configure a link-level Portstate protection group in such a network scenario, do as follows:

NOTE

```
huawei(config)#protect-group 0 protect-target as-mainboard-port workmode portstate
huawei(protect-group-0)#protect-group member port 0/9/0 role work
huawei(protect-group-0)#protect-group member port 0/10/0 role protect
huawei(protect-group-0)#protect-group enable
huawei(protect-group-0)#display protect-group 0
  -----------------------------------------------------------------------
  Group ID         : 0
  Protect Target   : Port of active main board and standby main board
  Work Mode        : portstate
  Description      :
  Admin State      : enable
  Operation        : none
  Reversion        : disable
  Reversion Time(s): 720
  -----------------------------------------------------------------------
  Member       Role         Operation         State         PeerMember
  -----------------------------------------------------------------------
  0/9/0        work         none              active        none
  0/10/0       protect      none              standby       none
  -----------------------------------------------------------------------
```

14.2.2 Configuring an LAG-Level Portstate Protection Group on the Control Board

A link aggregation group (LAG)-level Portstate protection group applies to the following network scenario: The active and standby control boards on an access device each provide multiple upstream Ethernet ports, and users want the upstream Ethernet ports (working ports) on the active control board to carry services and those (protection ports) on the standby control board to back up. If a working port is faulty, and the LAG on the active control board has fewer properly-functioning ports than the LAG on the standby control board, the system switches services to the protection ports to implement uninterrupted forwarding.

Prerequisites

- The boards and ports on the access device support Ethernet port protection groups. For details, see Feature Dependency and Limitation in "Ethernet Port Protection Group" of Feature Description.
- In the protection group, a static MAC address is configured only on the working port. You can run the **display mac-address** command to query the static MAC address.
- The LAG ports on the interconnected device have the same data configurations and allow MAC address transfer.

Context

For details on a Portstate protection group, see Ethernet Port Protection Group in Feature Description.

The combination of a Portstate protection group and an Ethernet Link Aggregation Group ensures faster protection switching. The following options are available for configuring LAGs on the MA5600T/MA5603T:

- You can configure multiple ports in one LAG. Select multiple ports on the active control board to form one LAG, and select multiple ports on the standby control board to form another LAG.
- You can also configure only one port in one LAG. Select one port on the active control board to form one LAG, and select one port on the standby control board to form another LAG.

Note the following restrictions when you configure an LAG-level Portstate protection group on the control board:

- You need to configure an LAG first, and then add the master port of the LAG to the protection group.
- A port that is included in a protection group cannot be added to an LAG.

Procedure

Step 1 Create an LAG on the active control board.

Run the **link-aggregation** command to create an LAG on the active control board. The LAG on the standby control board will be automatically created.

Step 2 Configure an LAG-level Portstate protection group on the control board.

Run the **protect-group** command to create a protection group (select **as-mainboard-lag** as the protection level and **Portstate** as the protection type).

Step 3 Add a working port and a protection port to the protection group.

Run the **protect-group member** command to add the master port in the LAG on the control board as the working port of the protection group, and the master port in the LAG on the standby control board as the protection port.

Step 4 Enable the protection group.

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

Step 5 Query configurations about the protection group.

Run the **display protect-group** command to query configurations about the protection group. The configurations include the protection level, member ports, protection type, and reversion mode.

----End

Example

This example assumes a scenario in which two control boards on the MA5600T/MA5603T each provide two upstream ports to form LAGs: 0/9/0 and 0/9/1 on the active control board form one LAG, and 0/10/0 and 0/10/1 on the standby control board form the other LAG. The four upstream ports form one LAG-level Portstate protection group.

NOTE

For details on the application diagram, see Application in "Ethernet Port Protection Group" of Feature Description.

To configure an LAG-level Portstate protection group in such a network scenario, do as follows:

```
huawei(config)#link-aggregation 0/9 0-1 egress-ingress
huawei(config)#protect-group 0 protect-target as-mainboard-lag workmode
portstate
huawei(protect-group-0)#protect-group member port 0/9/0 role work
huawei(protect-group-0)#protect-group member port 0/10/0 role protect
huawei(protect-group-0)#protect-group enable
huawei(protect-group-0)#display protect-group 0
  -----------------------------------------------------------------------
  Group ID         : 0
  Protect Target   : LAG of active main board and standby main board
  Work Mode        : portstate
  Description      :
  Admin State      : enable
  Operation        : none
  Reversion        : disable
  Reversion Time(s): 720
```

```
-----------------------------------------------------------------------
Member        Role         Operation          State         PeerMember
-----------------------------------------------------------------------
0/9/0         work         none               active        none
0/10/0        protect      none               standby       none
-----------------------------------------------------------------------
```

14.2.3 Configuring a Board-Level Portstate Protection Group on the Control Board

A board-level Portstate protection group applies to the following network scenario: The active and standby control boards on the access device provide upstream ports, and users want the active control board (working board) to carry services and the standby one (protection board) to back up. If the working board is faulty, and the active control board has fewer properly-functioning ports than the standby control board, the system switches services to the protection board to implement uninterrupted forwarding.

Prerequisites

- The boards and ports on the access device support Ethernet port protection groups. For details, see Feature Dependency and Limitation in "Ethernet Port Protection Group" of Feature Description.
- In the protection group, a static MAC address is configured only on the working port. You can run the **display mac-address** command to query the static MAC address.
- The ports on the interconnected device have the same data configurations and allow MAC address transfer.

Context

For details on a Portstate protection group, see Ethernet Port Protection Group in Feature Description.

Procedure

Step 1 Configure a board-level Portstate protection group on the control board.

Run the **protect-group** command to create a protection group (select **as-mainboard** as the protection level and **Portstate** as the protection type).

Step 2 Add the working and protection boards to the protection group.

Run the **protect-group member** command to add the active control board as the working board of the protection group, and the standby control board as the protection board.

Step 3 Enable the protection group.

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

Step 4 Query configurations about the protection group.

Run the **display protect-group** command to query configurations about the protection group. The configurations include the protection level, member ports, protection type, and reversion mode.

----End

Example

This example assumes a scenario in which the MA5600T/MA5603T connects to the upstream network through two control boards. The active control board 0/9 and the standby control board form a board-level Portstate protection group.

NOTE

For details on the application diagram, see Application in "Ethernet Port Protection Group" of Feature Description.

To configure a board-level Portstate protection group in such a network scenario, do as follows:

```
huawei(config)#protect-group 0 protect-target as-mainboard workmode portstate
huawei(protect-group-0)#protect-group member board 0/9 role work
huawei(protect-group-0)#protect-group member board 0/10 role protect
huawei(protect-group-0)#protect-group enable
huawei(protect-group-0)#display protect-group 0
  -----------------------------------------------------------------------
  Group ID          : 0
  Protect Target    : Active main board and standby main board
  Work Mode         : portstate
  Description       :
  Admin State       : enable
  Operation         : none
  Reversion         : disable
  Reversion Time(s): 720
  -----------------------------------------------------------------------
  Member        Role         Operation          State         PeerMember
  -----------------------------------------------------------------------
  0/9           work         none               active        none
  0/10          protect      none               standby       none
  -----------------------------------------------------------------------
```

14.2.4 Configuring a Timedelay Protection Group

A Timedelay protection group applies to the following scenario: The active and standby control boards or upstream service boards on an access device each provide an upstream Ethernet port, and users want port to carry services and the other port to back up. If the working port is faulty, the system switches services to the protection port to implement uninterrupted forwarding.

Prerequisites

- The boards and ports on the access device support Ethernet port protection groups. For details, see Feature Dependency and Limitation in "Ethernet Port Protection Group" of Feature Description.
- In the protection group, a static MAC address is configured only on the working port. You can run the **display mac-address** command to query the static MAC address.
- In a protection group, the two interconnected ports have the same data configurations and allow MAC address transfer.

Context

For details on a Timedelay protection group, see Ethernet Port Protection Group in Feature Description.

Procedure

Step 1 (Optional) Configure the optical port shutdown function.

Run the **offline-tx-off-time** command to specify the time for keeping an optical port shut down in the case of a Linkdown. The optical port shutdown function helps improve protection switching performance.

Step 2 Create a Timedelay protection group.

Run the **protect-group** command to create a protection group (select **eth-nni-port** as the protection level and **Timedelay** as the protection type).

Step 3 Add a working port and a protection port to the protection group.

Run the **protect-group member** command to add one port on the control board or on the upstream board as the working port, and the other port on the board as the protection port in the protection group.

Step 4 Enable the protection group.

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

Step 5 Query configurations about the protection group.

Run the **display protect-group** command to query configurations about the protection group. The configurations include the protection level, member ports, protection type, and reversion mode.

----End

Example

This example assumes a scenario in which the MA5600T/MA5603T connects to the upstream network through the GIU upstream service board. Two upstream ports 0/19/0 and 0/20/0 on the GIU board form a Timedelay protection group.

NOTE

For details on the application diagram, see Application in "Ethernet Port Protection Group" of Feature Description.

To configure a Timedelay protection group in such a network scenario, do as follows:

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#offline-tx-off-time 0 500
huawei(config)#quit
huawei(config)#interface giu 0/20
huawei(config-if-giu-0/20)#offline-tx-off-time 0 500
huawei(config)#quit
huawei(config)#protect-group 0 protect-target eth-nni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/19/0 role work
huawei(protect-group-0)#protect-group member port 0/20/0 role protect
huawei(protect-group-0)#protect-group enable
huawei(protect-group-0)#display protect-group 0
  -----------------------------------------------------------------------
  Group ID         : 0
  Protect Target   : Port of Ethernet nni
  Work Mode        : timedelay
  Description      :
  Admin State      : enable
  Operation        : none
  Reversion        : disable
  Reversion Time(s): 720
  -----------------------------------------------------------------------
  Member        Role         Operation         State         PeerMember
  -----------------------------------------------------------------------
  0/19/0        work         none              active        none
  0/20/0        protect      none              standby       none
  -----------------------------------------------------------------------
```

14.3 Configuring the Smart Link Redundancy Backup

The smart link is a solution that is applied in the network with dual uplinks and provides reliable and efficient backup and quick switching for the dual uplinks. The solution provides high reliability for carriers' network.

Context

Therefore, the smart link solution is applied to the access network. With this solution, redundancy backup for active and standby links and quick switching are implemented for a dual homing network. This ensures high reliability and quick convergence. Meanwhile, as a supplementary to the smart link solution, the monitor link solution is introduced to monitor uplinks. This improves the backup function of the smart link solution.

The smart link and monitor link feature, which is applied to the scenario of a network with dual uplinks (the network is connected to the upstream IP network through dual uplinks), is related to the OLT and the upstream network device. The upstream network device such as the router must support the smart link and monitor link feature.

NOTE

The smart link and monitor link feature is put forth by Huawei. Currently, only Huawei devices support this technology.

Smart link-related concepts:

- Smart link protection group

  A smart link group contains up to two ports, namely one master port and one slave port. In normal conditions, only one port is in the active state, and the other port is blocked and in the standby state. When the port in the active state fails, the smart link group automatically blocks the port, and switches the previously standby port to the active state.

- Master port

  The master port, which is also called the work port, is a port role in a smart link group. When both ports are in the standby state, the master port takes priority to switch to the active state.

- Slave port

  The slave port, which is also called the protection port, is a port role in the smart link group. When both ports are in the standby state, the master is prevailed upon to switch to the active state, and the slave port remains in the standby state.

- Flush packet

  After link switching occurs on the smart link group, the original forwarding entry is not applicable to the network with new topology, and the upstream convergence device needs to update the MAC and ARP entries. In this case, the smart link group notifies the other devices in the network of updating the address table through sending the notification packet. This notification packet is the flush packet.

Monitor link-related concepts:

- Monitor link group

  A monitor link group is composed of one uplink and several downlinks.

- Uplink

When the uplink in a monitor link group fails, the monitor link group fails. In this case, the downlinks in the monitor link group will be blocked by force.

- Downlink

  When a downlink in a monitor link group fails, it does not affect the uplink or the other downlinks.

A smart link can work in either the active/standby mode or the load balancing mode. The differences are as follows:

- In the active/standby mode, both ports are enabled. Only the master port is in the active state and can forward data. The slave port is blocked and is in the standby state.
- In the load balancing mode, both ports are enabled. If both ports work in the normal state, the data is forwarded through both ports, implementing load balancing.

Procedure

Step 1 Configure a smart link protection group.

1. Run the **protect-group** command to create a smart link protection group. The protection group works in either the active/standby mode or the load balancing mode.

   NOTE

   - When configuring a smart link protection group, set the protected object to **eth-nni-port**. Working modes of other types do not support the smart link feature.
   - Keyword **smart-link**: Indicates the smart-link active and standby mode. In this mode, both members in the PG are enabled, but only the active member forwards data.
   - Keyword **smart-link load-balance**: Indicates the smart-link load balancing mode. In this mode, both links are enabled to share load to improve the usage ratio of the line.

2. Run the **protect-group member** command to add members to a smart link protection group.

   When adding members to the protection group, add a working member, and then add a protection member.

3. Run the **protect-group enable** command to enable the smart link protection group.

   After a protection group is created, the protection group is in the disabled state by default. You should enable the protection group to make the configuration take effect.

4. Query the information about the protection group.

   Run the **display protect-group** command to query the information about the protection group and all the members in the protection group.

Step 2 Configure the flush packet sending mode.

After service switching occurs on a protection group, the original forwarding entry is not applicable to the new network, and the entire network needs to update the MAC and ARP entries. In this case, the protection group sends flush packets to other devices to notify them of updating the MAC and ARP entries.

1. Run the **flush send** command to configure the flush packet sending parameters of the protection group, including the control VLAN and the password.

   a. If the flush packet sending parameters are not configured, no flush packet is sent when switching occurs on the protection group.

   b. If the protection group is not in the control VLAN, no flush packet is sent.

   c. The peer device must support receiving flush packets, and the flush packet receiving function of the corresponding port must be enabled.

2. Run the **display flush receive** command to query the port that receives flush packets and the flush packet receiving parameters.

Step 3 (Optional) Run the **load-balance instance** command to configure the load balancing parameters of a protection group.

Load balancing parameters determine that the working member and protection member carry different STP instances. Because VLANs are mapped to STP instances, the load balancing parameters in practice determine through which port (working member or protection member) the packets with different VLAN tags are transmitted.

NOTE

Configure the load balancing parameters only when the specified smart link protection group works in the load balancing mode.

- This command is used to configure STP instances that are carried by the protection member. The instances that are unconfigured are carried by the working member.
- The load balancing parameters of a protection group are based on STP instances pre-configured. You can run the **instance vlan** command to map VLANs to STP instances.

Step 4 (Optional) Configure a monitor link group.

The monitor link group and the smart link protect group are generally used together for monitoring the uplink and completing the smart link redundancy.

NOTE

1. Generally, the monitor link group is configured on the upper-layer device (such as a router) that is interconnected with the OLT, subtended to the smart link protection group.
2. You need to configure the monitor link on the MA5600T/MA5603T for monitoring the uplink of the subtended OLT only when the MA5600T/MA5603T functions as an upper-layer device interconnecting with the OLT. Otherwise, the configuration is meaningless.

1. Run the **monitor-link group** command to create a monitor link group, and enter the monitor link group mode.

   A monitor link group consists of one upstream port and multiple downstream ports. When the upstream port is faulty, the downstream ports are disabled. Therefore, the downstream devices can detect the link fault and switch the services to a normal link.
2. Run the **member port** command to add members to a monitor link group.
   - The uplink of a monitor link group can be a common Ethernet port, the master port of a protection group, or the master port of an aggregation group.
   - The downlink of a monitor link group can be only a common Ethernet port.
3. Run the **display monitor-link group** command to query the information about the monitor link group.

----End

Example

Assume the following configurations: The MA5600T/MA5603T implements dual uplinks through the GIU board, upstream ports 0/19/0 and 0/19/1 on the GIU board are added as members of smart link protection group 2, port 0/19/0 functions as the working port, port 0/19/1 functions as the protection port, the working mode is the load balancing mode, where,

- The STP instance 1 (mapping to VLAN 100-110) is carried by the working member.
- The STP instance 2 (mapping to VLAN 120-130) is carried by the protection member.
- The control VLAN of flush packets is VLAN 10, and the password is **abc**.

To perform these configurations and enable the protection group function, do as follows:

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#instance 1 vlan 100 to 110
huawei(stp-region-configuration)#instance 2 vlan 120 to 130
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration,it may take several minutes,are you sure to
active region configuration? [Y/N][N]y
huawei(stp-region-configuration)#quit
huawei(config)#protect-group 2 protect-target eth-nni-port workmode smart-link
load-balance
huawei(config-protect-group-2)#protect-group member port 0/19/0 role work
huawei(config-protect-group-2)#protect-group member port 0/19/1 role protect
huawei(config-protect-group-2)#load-balance instance 2
huawei(config-protect-group-2)#flush send control-vlan 10 password simple abc
huawei(config-protect-group-2)#protect-group enable
huawei(config-protect-group-2)#quit
```

14.4 Configuring ARP Detection (for Accelerating Protection Switching)

Address Resolution Protocol (ARP) probe enables faster protection switching by detecting status of end-to-end links. ARP detection can be configured for a network scenario in which a link protection group is configured for the upstream Ethernet ports on the access device, and there are other types of devices deployed, such as switches and transmission devices, between the access device and the aggregation devices.

Prerequisites

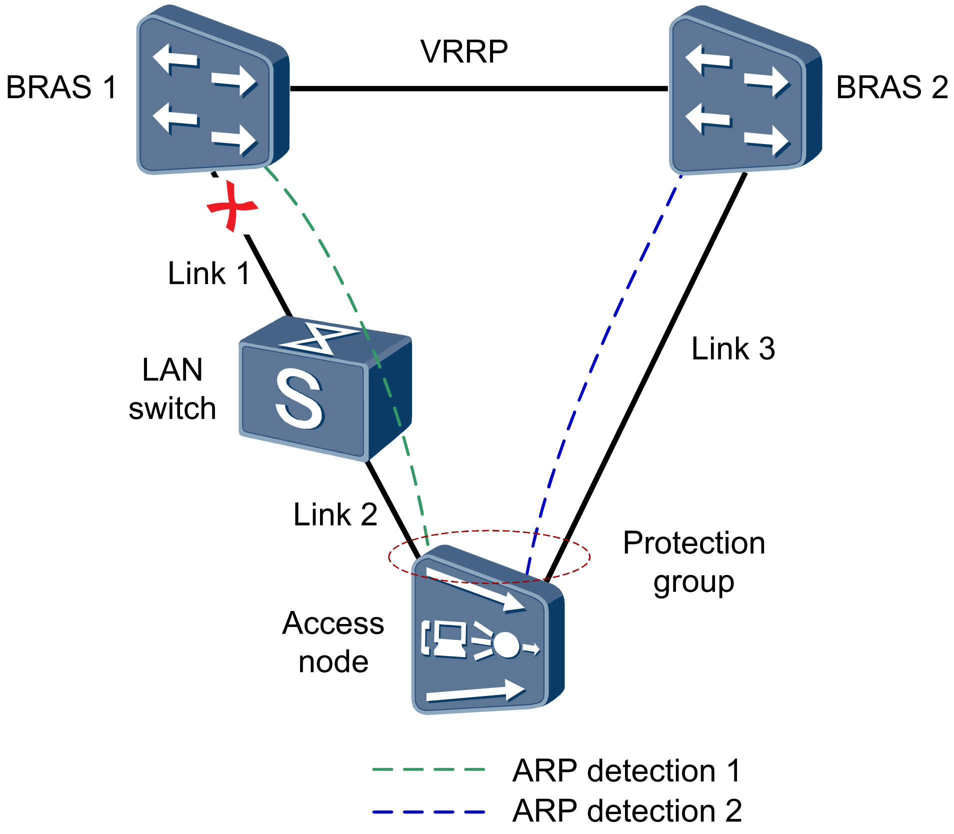
The access device provides upstream ports through the upstream boards. ARP detection is not supported if the access device provides upstream ports through the control board.

A Timedelay protection group is configured on the upstream boards. For configuration details, see **Configuring an Ethernet Port Protection Group**.

Context

Figure 14-2 shows an Ethernet port protection example in which the access device (MA5600T/MA5603T) is dual-homed to BRASs.

Figure 14-2 Ethernet port protection with the access device dual-homed to BRASs



The MA5600T/MA5603T is dual-homed to BRAS 1 and BRAS 2. The working links are Link1 and Link2, and the protection link is Link3. If Link1 is faulty and Link2 is normal, the MA5600T/MA5603T can switch services to Link3 by using ARP detection even though the upstream port on the MA5600T/MA5603T is functioning properly. This ensures uninterrupted service transmission.

Procedure

Step 1 Configure VLAN and Layer 3 port IP address for ARP detection.

1. Create a VLAN.

   Run the **vlan** command to create a smart VLAN for ARP detection.

2. Add an upstream port to the VLAN.

   Run the **port vlan** command to add the working upstream Ethernet port in the protection group to the VLAN. The protection port in the protection group cannot be added to the VLAN.

3. Create a Layer 3 interface for the VLAN.

   Run the **interface vlanif** command to create a Layer 3 interface for the VLAN and enter the VLAN interface mode.

4. Configure an IP address for the Layer 3 interface in the VLAN.

Run the **ip address** command to configure an IP address for the Layer 3 interface in the VLAN. Ensure that this IP address is in the same subnet as the IP address of the remote device.

Step 2 Configure ARP detection for the working port in the protection group.

1. Configure ARP detection for the working port in the protection group.

   Run the **arp-detect** command to configure ARP detection for the working port in the protection group.

2. (Optional) Configure the times for sending ARP detection packets.

   Run the **detect-multiplier** command to configure the times for sending ARP packets. If the remote device does not respond to the ARP detection packets sent by the local device (here, the access device) for the specified times, the local device considers ARP detection has timed out.

   The waiting time for ARP detection is derived from the following formula: Waiting time = Interval for sending ARP request packets x Times for sending ARP packets. The ARP detection waiting time is also the time taken for triggering a protection switching. The minimum waiting time is 3s (1s x 3). Because the interconnected devices have to process ARP packets, the device CPU load will increase. The more frequent the packets are sent, the heavier the CPU load.

3. (Optional) Configure the interval for sending ARP detection packets.

   Run the **min-tx-interval** command to configure the interval for sending ARP detection packets.

4. Enable the ARP detection function.

   Run the **detect enable** command to enable the ARP detection function.

Step 3 Configure ARP detection for the protection port in the protection group.

Repeat **Step 2**(but change the working port to the protection port) to configure ARP detection for the protection port in the protection group.

Step 4 Verify ARP detection configurations at the two ports in the protection group.

Run the **display arp-detect** command to verify ARP detection configurations, such as the remote IP address and enable/disable status of ARP detection, at the two ports in the protection group.

----End

Example

Table 14-1 Data plan

Item	Value
Positions of ports in the protection group	Ports on the GIU board: 0/19/0 and 0/19/1
VLAN for ARP detection	VLAN 20
IP address of the Layer 3 interface in the VLAN	Working port: 1.1.1.2/24 Protection port: 2.2.2.2/24

Item	Value
Remote IP address	1.1.1.1/24 2.2.2.1/24
ARP detection times	Three times (default)
Interval for sending ARP detection packets	1s (default)

This example assumes a scenario in which the MA5600T/MA5603T is dual-homed to BRAS 1 and BRAS 2 through the GIU upstream board, and the "Value" column in **Table 14-1** lists the data plan. When ARP detection times out, the system considers the working link interrupted and switches services to BRAS 2, ensuring uninterrupted service transmission.

To configure ARP detection in such a network scenario, do as follows:

```
//Configure the VLAN and Layer 3 interface IP address used for ARP detection of the
local device.
huawei(config)#vlan 20 smart
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 1.1.1.2 24
huawei(config-if-vlanif20)#ip address 2.2.2.2 24
huawei(config-if-vlanif20)#quit
//Configure ARP detection for the working port.
huawei(config)#arp-detect arp_test1 bind peer-ip 1.1.1.1 vlan 20 port 0/19/0
huawei(config-arp-detect-arp_test1)# detect-multiplier 3
huawei(config-arp-detect-arp_test1)# min-tx-interval 2
huawei(config-arp-detect-arp_test1)#detect enable
huawei(config-arp-detect-arp_test1)#quit
//Configure ARP detection for the protection port.
huawei(config)#arp-detect arp_test2 bind peer-ip 2.2.2.1 vlan 20 port 0/19/1
huawei(config-arp-detect-arp_test2)#detect-multiplier 3
huawei(config-arp-detect-arp_test2)#min-tx-interval 2
huawei(config-arp-detect-arp_test2)#detect enable
huawei(config-arp-detect-arp_test2)#quit
//Query configurations of the working port.
huawei(config)#display arp-detect arp_test1
 ---------------------------------------------------------------------------
  Name       : arp-test2                         Admin State : Enable
  Peerip     : 1.1.1.1                            Interval    : 2(s)
  Vlan       : 20                                 Multiplier  : 3
  F/S/P      : 0/19/0                             State       : Down
 ---------------------------------------------------------------------------
//Query configurations of the protection port.
huawei(config)#display arp-detect arp_test2
 ---------------------------------------------------------------------------
  Name       : arp_test2                         Admin State : Enable
  Peerip     : 2.2.2.1                            Interval    : 2(s)
  Vlan       : 20                                 Multiplier  : 3
  F/S/P      : 0/19/1                             State       : Down
 ---------------------------------------------------------------------------
```

14.5 Configuring the MSTP

The MA5600T/MA5603T supports the application of the Multiple Spanning Tree Protocol (MSTP), Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP). The MA5600T/MA5603T supports the MSTP ring network, which can meet various networking requirements.

Context

- MSTP applies to a redundant network. It makes up for the drawback of STP and RSTP. MSTP makes the network converge fast and the traffic of different VLANs distributed along their respective paths, which provides a better load-sharing mechanism.
- MSTP trims a loop network into a loop-free tree network. It prevents the proliferation and infinite cycling of the packets in the loop network. In addition, MSTP supports load sharing by VLAN during data transmission.

Procedure

Step 1 Enabling the MSTP function.

- By default, the MSTP function is disabled.
- After the MSTP function is enabled, the device determines whether it works in STP compatible mode or MSTP mode based on the configured protocol.
- After the MSTP function is enabled, MSTP maintains dynamically the spanning tree of the VLAN based on the received BPDU packets. After the MSTP function is disabled, the MA5600T/MA5603T becomes a transparent bridge and does not maintain the spanning tree.

1. Run the **stp enable** command to enable the MSTP function of the bridge.
2. Run the **stp port enable** command to enable the MSTP function of the port.
3. Run the **display stp** command or the **display stp port** command to query the MPLS state of the bridge or the port.

Step 2 Configuring the MST region name.

1. Run the **stp region-configuration** command to enter MST region mode.
2. Run the **region-name** command to configure the name of the MST region.

   By default, the MST region name is the bridge MAC address of the device.

Step 3 Configuring the MSTP instance.

The MSTP protocol configures the VLAN mapping table (mapping between the VLAN and the spanning tree), which maps the VLAN to the spanning tree.

1. Run the **stp region-configuration** command to switch over to MST region mode.
2. Run the **instance vlan** command to map the specified VLAN to the specified MSTP instance.
   - By default, all VLANs are mapped to CIST, that is, instance 0.
   - One VLAN can be mapped to only one instance. If you re-map a VLAN to another instance, the original mapping is disabled.
   - A maximum of 10 VLAN sections can be configured for an MSTP instance.

   NOTE

   A VLAN section refers to the consecutive VLAN IDs from the start VLAN ID to the end VLAN ID.
3. Run the **check region-configuration** command to query the parameters of the current MST region.

Step 4 Activating the configuration of the MST region.

1. Run the **stp region-configuration** command to switch over to MST region mode.
2. Run the **active region-configuration** command to activate the configuration of the MST region.

3. Run the **display stp region-configuration** command to query the effective configuration of the MST region.

Step 5 Setting the priority of the device in the specified spanning tree instance.

1. Run the **stp priority** command to set the priority of the device in the specified spanning tree instance.
2. Run the **display stp** command to query the MSTP configuration of the device.

Step 6 Other optional configurations.

- Setting the MST region parameters.
  - Run the **stp md5-key** command to set the MD5-Key for the MD5 encryption algorithm configured on the MST region.
  - In the MSTP region mode, run the **vlan-mapping module** command to map all VLANs to the MSTP instances by modular arithmetic.
  - In the MSTP region mode, run the **revision-level** command to set the MSTP revision level of the device.
  - Run the **reset stp region-configuration** command to restore the default settings to all parameters of the MST region.
- Specifying the device as a root bridge or a backup root bridge.
  - Run the **stp root** command to specify the device as a root bridge or a backup root bridge.
- Setting the time parameters of the specified network bridge.
  - Run the **stp timer forward-delay** command to set the Forward Delay of the specified network bridge.
  - Run the **stp timer hello** command to set the Hello Time of the specified network bridge.
  - Run the **stp timer max-age** command to set the Max Age of the specified network bridge.
  - Run the **stp time-factor** command to set the timeout time factor of the specified network bridge.
- Setting the parameters of the specified port.
  - Run the **stp port transmit-limit** command to set the number of packets transmitted by the port within the Hello Time.
  - Run the **stp port edged-port enable** command to set the port as an edge port.
  - Run the **stp port cost** command to set the path cost of a specified port.
  - Run the **stp port port-priority** command to set the priority of the specified port.
  - Run the **stp port point-to-point** command to set whether the link that is connected to the port is a point-to-point link.
- Configuring the device protection function.
  - Run the **stp bpdu-protection enable** command to enable the BPDU protection function of the device.
  - Run the **stp port loop-protection enable** command to enable the loop protection function of the port.
  - Run the **stp port root-protection enable** command to enable the root protection function of the port.
- Setting the maximum number of hops of the MST region.
  - Run the **stp max-hops** command to set the maximum number of hops of the MST region.
- Setting the diameter of the switching fabric.

  - Run the **stp bridge-diameter** command to set the diameter of the switching fabric.
- Setting the calculation standard for the path cost.
  - Run the **stp pathcost-standard** command to set the calculation standard for the path cost.
- Clear the MSTP protocol statistics.
  - Run the **reset stp statistics** command to clear the MSTP protocol statistics.

----End

Example

Configure the MSTP parameters as follows:

- Enable the MSTP function.
- Enable the MSTP function on port 0/19/0.
- Set the MSTP running mode to MSTP compatible mode.
- Configure MST region parameters:
  - Configure the MD5-Key for the MD5 encryption algorithm to 0x11ed224466.
  - Configure the MST region name to huawei-mstp-bridge.
  - Map VLAN2-VLAN10 and VLAN12-VLAN16 to MSTP instance 3.
  - Map all the VLANs to the specified MSTP instances.
  - Configure the MSTP revision level of the device to 100.
- Configure the maximum hops for the MST region to 10.
- Activate the configuration of the MST region manually.
- Configure the priority of the device in spanning tree instance 2 to 4096.
- Configure the current device as the root bridge of MSTP instance 2.
- Configure the diameter of the switching network to 6.
- Configure the calculation standard for the path cost to IEEE 802.1t.
- Configure the time parameters of a specified bridge:
  - Configure the forward delay to 2000 centiseconds.
  - Configure the hello time to 1000 centiseconds.
  - Configure the max age to 3000 centiseconds.
  - Configure the timeout time factor to 6.
- Configure the parameters of a specified port:
  - Configure the maximum number of packets transmitted in a hello time period to 16.
  - Configure port 0/19/0 to be an edge port.
  - Configure the path cost of the port in a specified spanning tree instance to 1024.
  - Configure the priority of the port to 64.
  - The link connected to port 0/19/0 is a point-to-point link.
- Enable the BPDU protection function on the device.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take several
minutes,are you sure to change global stp state? [Y/N][N]y
huawei(config)#stp port 0/19/0 enable
huawei(config)#stp mode mstp
huawei(config)#stp md5-key 11ed224466
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name huawei-mstp-bridge
huawei(stp-region-configuration)#instance 3 vlan 2 to 10 12 to 16
huawei(stp-region-configuration)#vlan-mapping module 16
huawei(stp-region-configuration)#revision-level 100
huawei(stp-region-configuration)#active region-configuration
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 2 priority 4096
huawei(config)#stp instance 2 root primary
huawei(config)#stp max-hops 10
huawei(config)#stp bridge-diameter 6
huawei(config)#stp pathcost-standard dot1t
huawei(config)#stp timer forward-delay 2000
huawei(config)#stp timer hello 1000
huawei(config)#stp timer max-age 3000
huawei(config)#stp time-factor 6
huawei(config)#stp port 0/19/0 transmit-limit 16
huawei(config)#stp port 0/19/0 edged-port enable
huawei(config)#stp port 0/19/0 instance 0 cost 1024
huawei(config)#stp port 0/19/0 instance 0 port-priority 64
huawei(config)#stp port 0/19/0 point-to-point force-true
huawei(config)#stp bpdu-protection enable
```

14.6 Configuring VRRP Transparent Transmission in the S+C Forwarding Mode

In the S+C forwarding mode, after VRRP snooping is enabled, VRRP packets can be forwarded between two isolated upstream ports.

Context

To enhance the system reliability, the MA5600T/MA5603T is directly connected to two or more routers in the upstream direction for dual homing.

- In the S+C forwarding mode, the MAC address learning function needs to be disabled. In addition, to prevent broadcast storms, two upstream ports of the MA5600T/MA5603T need to be isolated. Therefore, the VRRP packets between upper-layer routers cannot be forwarded through the upstream ports of the MA5600T/MA5603T. To solve this problem, enable the VRRP transparent transmission function.
- In the VLAN+MAC forwarding mode, the VRRP transparent transmission function may not be enabled.

Procedure

Step 1 Configuring an isolation group.

Run the **isolate group** command to configure an isolation group. To avoid forwarding downstream service packets to another upstream port, you can add the upstream ports to an isolation group.

Step 2 Configure a snooping port.

Run the **vrrp-snoop port** command to configure the upstream port connecting the MA5600T/MA5603T and the router as a snooping port.

Step 3 Configure the virtual IP address and VLAN to be snooped.

Run the **vrrp-snoop ip** command to configure the IP address and VLAN of the virtual router to be snooped.

Step 4 Enable VRRP snooping.

Run the **vrrp-snoop enable** command to enable VRRP snooping.

----End

Example

Assume the following configurations: The MA5600T/MA5603T is connected to two routers through upstream ports 0/19/0 and 0/19/1. The VRRP packets between the routers need to be transparent transmitted through the upstream ports of the MA5600T/MA5603T.The VLAN forwarding mode is S+C, the VLAN ID is 100, and the IP address of the virtual router is 10.71.10.1. To perform these configurations, do as follows:

```
huawei(config)#isolate group port 0/19/0 0/19/1
huawei(config)#vrrp-snoop port 0/19/0
huawei(config)#vrrp-snoop port 0/19/1
huawei(config)#vrrp-snoop ip 10.71.10.1 vlan 100
huawei(config)#vrrp-snoop enable
```

14.7 Configuring RRPP

Rapid Ring Protection Protocol (RRPP) is a data link layer protocol specially applied to the Ethernet ring. When the Ethernet ring is complete, RRPP can prevent broadcast storms caused by a data loop. When a link on the Ethernet ring is disconnected, RRPP can quickly recover the communication channels between nodes on the Ethernet ring, increasing the network reliability.

Context

Most MANs and enterprise networks adopt the ring network structure to increase the reliability. Any faulty node on the ring does not affect the service. RRPP is a dedicated data link layer protocol applied to the Ethernet ring. Compared with other Ethernet ring technologies, RRPP has the following advantages:

- The topology convergence is quick.
- The convergence time is irrelevant with the number of nodes in the ring network. RRPP is applicable to the network that has a relatively large network diameter.
- A complete Ethernet ring can prevent broadcast storm caused by data loop.
- When a link in the Ethernet ring network is disconnected, RRPP can quickly recover the communication between nodes in the ring network by using the backup link.

Currently, the MA5600T/MA5603T supports only the single-ring network application of RRPP. The MA5600T/MA5603T can function as a primary node or a transmission node.

Procedure

- Configure the primary node.
  1. Run the **rrpp mode** command to configure the RRPP protocol mode.
     - You can select the RRPP standard mode or EAPS compatible mode. The RRPP standard mode is used by default.
     - When the RRPP function is enabled or an RRPP domain exists on the device, the RRPP protocol mode cannot be changed.
  2. Run the **rrpp domain** command to configure the RRPP domain.

Currently, the MA5600T/MA5603T supports only one RRPP domain.

3. Run the **control-vlan** command to configure the control VLAN of the RRPP domain.
   - The specified VLAN must be created through the **vlan** command and must be a standard VLAN.
   - During the configuration, you need to specify only the major control VLAN ID. The sub-control VLAN ID is specified by the system. Sub-control VLAN ID = Major control VLAN ID + 1.
   - The major control VLAN or sub-control VLAN cannot be a system reserved VLAN or a VLAN that is in use.
4. Run the **ring** command to configure the RRPP ring.
   - Currently, the MA5600T/MA5603T supports only one RRPP ring and the ring must be the primary ring.
   - The network role of a port joining the RRPP ring must be an upstream port. It cannot be a subtending port.

   NOTE

   On the same port, the RRPP function and the STP function cannot be enabled at the same time. Because the system enables the STP port-level switch by default, before creating an RRPP port, you must disable the STP function of the primary and secondary ports.
5. (Optional) Run the **timer hello-timer** command to configure the hello timer and fail time of the RRPP domain.
   - By default, the hello timer is 1s and the fail timer is 3s.
   - The value of the fail timer must be three times equal to or larger than the value of the hello timer.
6. Run the **ring enable** command to enable the RRPP ring.
7. Run the **rrpp enable** command to enable the RRPP protocol.
8. Run the **display rrpp brief domain** command to query the brief information about the RRPP domain.
9. Run the **display rrpp verbose domain** command to query details of the RRPP ring.

- Configure the transmission node.
  1. Run the **rrpp mode** command to configure the RRPP protocol mode. The configuration must be the same as that on the primary node.
     - You can select the RRPP standard mode or EAPS compatible mode. The RRPP standard mode is used by default.
     - When the RRPP function is enabled or an RRPP domain exists on the device, the RRPP protocol mode cannot be changed.
  2. Run the **rrpp domain** command to configure the RRPP domain. The domain ID must be the same as that on the primary node.

     Currently, the MA5600T/MA5603T supports only one RRPP domain.
  3. Run the **control-vlan** command to configure the control VLAN of the RRPP domain. The configuration must be the same as that on the primary node.
     - The specified VLAN must be created through the **vlan** command and must be a standard VLAN.
     - During the configuration, you need to specify only the major control VLAN ID. The sub-control VLAN ID is specified by the system. Sub-control VLAN ID = Major control VLAN ID + 1.

- The major control VLAN or sub-control VLAN cannot be a system reserved VLAN or a VLAN that is in use.

4. Run the **ring** command to configure the RRPP ring. The ring ID must be the same as that on the primary node.
   - Currently, the MA5600T/MA5603T supports only one RRPP ring and the ring must be the primary ring.
   - The network role of a port joining the RRPP ring must be an upstream port. It cannot be a subtending port.

   NOTE

   On the same port, the RRPP function and the STP function cannot be enabled at the same time. Because the system enables the STP port-level switch by default, before creating an RRPP port, you must disable the STP function of the primary and secondary ports.
5. (Optional) Run the **timer hello-timer** command to configure the hello timer and fail time of the RRPP domain.
   - By default, the hello timer is 1s and the fail timer is 3s.
   - The transmission node uses the fail timer as the timeout timer.
6. Run the **ring enable** command to enable the RRPP ring.
7. Run the **rrpp enable** command to enable the RRPP protocol.

----End

Example

To configure the MA5600T/MA5603T as the primary node of an RRPP ring with the following settings, do as follows:

- RRPP mode: standard
- Major control VLAN ID: 14; sub-control VLAN ID: 15
- RRPP primary port: 0/19/0; RRPP secondary port: 0/19/1
- RRPP domain ID: 1
- RRPP ring ID: 64

Other parameters adopt the default settings.

```
huawei(config)#vlan 14 standard
huawei(config)#vlan 15 standard
huawei(config)#port vlan 14-15 0/19 0-1
huawei(config)#stp port 0/19/0 disable
huawei(config)#stp port 0/19/1 disable
huawei(config)#rrpp mode rrpp
huawei(config)#rrpp domain 1
huawei(rrpp-domain-region-1)#control-vlan 14
huawei(rrpp-domain-region-1)#ring 64 node-mode master primary-port 0/19/0 second
ary-port 0/19/1 level 0
huawei(rrpp-domain-region-1)#ring 64 enable
huawei(rrpp-domain-region-1)#quit
huawei(config)#rrpp enable
huawei(config)#display rrpp brief domain 1
  ----------------------------------------------------------------------------
  Rrpp Protocol Status  : Enable
  Rrpp protocol mode    : RRPP
  Number of RRPP Domains: 1
  ----------------------------------------------------------------------------
  Domain Index          : 1
  Major Control VLAN    : 14
  Hello Timer           : 1  sec (default is 1 sec)
  Fail Timer            : 3  sec (default is 3 sec)
```

```
Number of RRPP Rings  : 1
----------------------------------------------------------------------------
 Ring   Ring    Node     Primary/Common         Secondary/Edge         Is
 ID     Level   Mode     Port                   Port                   Enabled
 ---------------------------------------------------------------------------
 64     0       M        GE 0/19/0              GE 0/19/1              Yes
----------------------------------------------------------------------------
Note: M - Master, T - Transit , E - Edge , A - Assistant-Edge
```

14.8 Configuring the BFD

This topic describes how to configure the BFD on the MA5600T/MA5603T.

Context

Bidirectional Forwarding Detection (BFD) protocol is a draft standardized by the Internet Engineering Task Force (IETF). BFD rapidly detects faults and monitors the forwarding and connectivity of links or IP routes of the network by quickly sending BFD control packets (the UDP packets in a specified format) at intervals between two nodes.

BFD provides the following functions:

- Allows fault detection with light load and high speed for paths between the neighboring forwarding engines.
- Provides a single mechanism to detect any medium and protocol layer in real time.

14.8.1 Configuring BFD Sessions

A bidirectional forwarding detection (BFD) session rapidly detects faults in direct links over a network.

Context

In the BFD detection mechanism, two systems set up a BFD session, and periodically send BFD control packets along the path between them. If one system does not receive BFD control packets within a specified period, the system considers that a fault occurs on the path.

NOTE

The MA5600T/MA5603T can detect a single-hop BFD of a virtual local area network (VLAN) interface link. Single-hop BFD is a mechanism that detects IP route connectivity between directly-connected systems.

BFD uses the local and remote discriminators to differentiate multiple BFD sessions between the same pair of systems. Based on the differences in methods of creating the local and the remote discriminators, MA5600T/MA5603T supports the following types of BFD sessions:

- Static BFD sessions with manually-specified discriminators

  The local and remote discriminators must be set manually. The discriminators on the remote end must also be manually specified.
- Static BFD sessions with automatically-negotiated discriminators

  If a dynamic BFD session is used by a remote device, a static BFD session with automatically negotiated discriminators must be created on a local device to interwork with the remote device and support the BFD for static routes. The discriminators on the remote end can be automatically negotiated or a dynamic BFD session can be established on the remote end.

- BFD sessions dynamically triggered by protocols, where no local or remote discriminator needs to be set:
  - BFD sessions with dynamically-allocated local discriminators.
  - BFD sessions with self-learned remote discriminators.

NOTE

The MA5600T/MA5603T supports dynamic creation of BFD sessions through open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS).

Procedure

Step 1 Enable BFD globally.

1. Run the **bfd** command to enable BFD globally and enter the BFD mode.

   BFD must be enabled globally before configurations relevant to BFD are performed. By default, BFD is disabled globally.

2. Run the **quit** command to quit the BFD mode.

Step 2 Create a BFD session.

1. Run the **bfd bind peer-ip** command to create a BFD session.

   If the **bfd bind peer-ip source-ip auto** command is run, a BFD session is set up through automatic negotiations over discriminators. The device on which such a BFD session is created can interoperate with another device on which a dynamic BFD is set up. This command is mainly used to configure BFD sessions for static routes.

   - If a single-hop BFD session is to be set up on an interface for the first time, the interface and its peer address must be bound to the BFD session. The bindings cannot be modified after the BFD session is successfully created.
   - During BFD configuration items are being created, the system checks only the format, not the correctness, of an IP address. Either an incorrect peer or source IP address leads to a failure in creating a BFD session.

2. Configure the discriminators.

   - Run the **discriminator local** *discr-value* command to configure a local discriminator.
   - Run the **discriminator remote** *discr-value* command to configure a remote discriminator.

   The local discriminator set on a device is equal to the remote discriminator set on a remote device, and the remote discriminator set on the local device is equal to the local discriminator set on the remote device. If the discriminators on the device and the remote device do not match, the session cannot be created. After the local and remote discriminators are set, they cannot be changed.

Step 3 (Optional) Configure the BFD parameters.

Select the following desired operations:

- Modify the detection time.
  - Run the **min-tx-interval** command to configure the interval for sending BFD packets. By default, the minimum sending interval is 1000 milliseconds.

  - Run the **min-rx-interval** command to configure the interval for receiving BFD packets. By default, the minimum sending interval is 1000 milliseconds.
- Run the **detect-multiplier** command to configure the local detection multiplier. By default, the local detection multiplier is 3.
- Run the **description** command to add the description of a BFD session. Descriptions of BFD sessions help you distinguish between various BFD sessions.

  NOTE

  The **description** command takes effect only on the statically configured BFD sessions, rather than the BFD sessions that are dynamically configured or the BFD sessions that are set up through automatic negotiations over discriminators.
- Run the **tos-exp** command to configure the priority of the BFD packet. By default, the highest priority 7 is adopted. When the system is congested, the BFD packet with higher priority can be sent first.

  NOTE

  You can configure the priority in static BFD mode but not in dynamic BFD mode.
- Run the **wtr** command to configure the time of waiting for recovery of the BFD session. By default, the value is 0, indicating no waiting.

  NOTE

  The BFD session is unidirectional. The detection is performed by BFD parameters configured on both ends respectively. If wait-to-recovery (WTR) is needed, configure it on two ends manually. Or, when the status of the session on one end changes, the applications on both ends can find that the states of the BFD sessions are inconsistent.

Step 4 Run the **commit** command to commit the configuration.

After necessary parameters, such as local and remote discriminators, are configured for a single-hop BFD session, the **commit** command must be run to make the configuration take effect.

NOTE

After a BFD session has been created, to modify a parameter, run a corresponding command (such as **min-tx-interval**, **min-rx-interval**, **detect-multiplier**, **description**, **tos-exp**, or **wtr**). The modification takes effect immediately without the **commit** command configured.

Step 5 Query the BFD session information and BFD session statistics.

- Run the **display bfd configuration** command to query the BFD configuration.
- Run the **display bfd interface** command to query the BFD configuration on an interface.
- Run the **display bfd session** command to query the BFD session information.
- Run the **display bfd statistics** command to query the BFD global statistics.
- Run the **display bfd statistics session** command to query the BFD session statistics.

----End

Example

Assume that the peer IP address is 10.1.1.1/24, BFD session name is test, the local discriminator is 100, the remote discriminator is 200, the minimum transmit interval and minimum receive interval of BFD control packets are both 10 milliseconds, the local detection multiplier is 3 (default value), VLAN 10 is created, and the IP address of VLAN interface 10 is configured. To configure BFD single-hop detection on VLAN interface 10, run the following commands:

```
huawei(config)#bfd
huawei(config-bfd)#quit
huawei(config)#bfd test bind peer-ip 10.1.1.1 interface vlanif 10
huawei(config-config-bfd-session-test)#discriminator local 100
huawei(config-config-bfd-session-test)#discriminator remote 200
huawei(config-config-bfd-session-test)#min-tx-interval 10
huawei(config-config-bfd-session-test)#min-rx-interval 10
huawei(config-config-bfd-session-test)#commit
```

14.8.2 Configuring BFD for Static Routes

The MA5600T/MA5603T supports detecting the fault of a static route by using the BFD. This topic describes how to configure the BFD link detection based on an example network.

Prerequisites

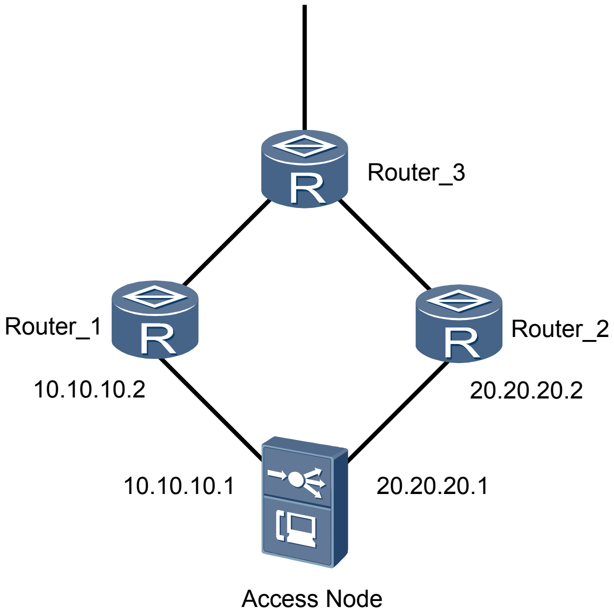
The BFD function must be enabled globally on the MA5600T/MA5603T.

Networking

Figure 14-3 shows an example network of the BFD for Static Routes.

Different static routes exist between the MA5600T/MA5603T and Router_3 through Router_1 and Router_2, and the BFD session is bound to the static route. When one link is faulty, the BFD session notifies the bound route for route switching.

Figure 14-3 Example network of the BFD for Static Routes



Data Plan

Table 14-2 provides the data plan for configuring the BFD for Static Routes.

Table 14-2 Data plan for configuring the BFD for Static Routes

Item	Data	Remarks
MA5600T/ MA5603T	Upstream ports: 0/19/0 and 0/19/1	-
VLAN	VLAN ID: 30 VLAN type: Smart VLAN IP address of the Layer 3 interface: 10.10.10.1/24	-
	VLAN ID: 40 VLAN type: Smart VLAN IP address of the Layer 3 interface: 20.20.20.1/24	-
BFD session	Session name: ToRouter_1 IP address of the peer interface: 10.10.10.2/24 Minimum transmit interval: 10 ms Minimum receive interval: 10 ms Detection multiplier: 3 Identifier: auto-negotiation	-
	Session name: ToRouter_2 IP address of the peer interface: 20.20.20.2/24 Minimum transmit interval: 10 ms Minimum receive interval: 10 ms Detection multiplier: 3 Identifier: auto-negotiation	-
Static route	Destination address: 30.30.30.1/24 Priority of the static route with next hop Router_1: 2 Priority of the static route with next hop Router_2: 6	-
Requirements for the upper-layer device	Router_1: ● IP address of the Layer 3 interface: see the example network ● VLAN ID: 30 ● BFD session parameters: consistent with the parameters of the MA5600T/MA5603T	For details about the configuration of the routers, see the corresponding configuration guide.
	Router_2: ● IP address of the Layer 3 interface: see the example network ● VLAN ID: 40 ● BFD session parameters: consistent with the parameters of the MA5600T/MA5603T	

Procedure

Step 1 Create VLANs and add upstream ports to the VLANs.

```
huawei(config)#vlan 30 smart
huawei(config)#port vlan 30 0/19 0
huawei(config)#vlan 40 smart
huawei(config)#port vlan 40 0/19 1
```

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

```
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.10.10.1 24
huawei(config-if-vlanif30)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#ip address 20.20.20.1 24
huawei(config-if-vlanif40)#quit
```

Step 3 Configure the BFD sessions.

You can configure BFD sessions only after the global BFD function is enabled.

```
huawei(config)#bfd
huawei(config-bfd)#quit
huawei(config)#bfd ToRouter_1 bind peer-ip 10.10.10.2 source-ip 10.10.10.1 auto
huawei(config-bfd-session-torouter_1)#min-rx-interval 10
huawei(config-bfd-session-torouter_1)#min-tx-interval 10
huawei(config-bfd-session-torouter_1)#detect-multiplier 3
huawei(config-bfd-session-torouter_1)#commit
huawei(config-bfd-session-torouter_1)#quit
huawei(config)#bfd ToRouter_2 bind peer-ip 20.20.20.2 source-ip 20.20.20.1 auto
huawei(config-bfd-session-torouter_2)#min-rx-interval 10
huawei(config-bfd-session-torouter_2)#min-tx-interval 10
huawei(config-bfd-session-torouter_2)#detect-multiplier 3
huawei(config-bfd-session-torouter_2)#commit
huawei(config-bfd-session-torouter_2)#quit
```

Step 4 Bind the BFD sessions to the static routes.

```
huawei(config)#ip route-static 30.30.30.1 24 10.10.10.2 preference 2 track bfd-
session ToRouter_1
huawei(config)#ip route-static 30.30.30.1 24 20.20.20.2 preference 6 track bfd-
session ToRouter_2
```

Step 5 Save the data.

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

----End

Result

BFD sessions ToRouter_1 and ToRouter_2 are in the up state. The priority of the route to which ToRouter_1 is bound takes effect and carries services because it has a higher priority. When a faulty link is detected, BFD session ToRouter_1 turns to the down state, which triggers the deactivation of the bound route. In this case, the route to which ToRouter_2 is bound takes effect and carries services.

14.8.3 Configuring BFD for OSPF

The MA5600T/MA5603T can detect the fault of a dynamic route by using the bidirectional forwarding detection (BFD). This topic describes how to configure the BFD link detection based on the dynamic routing protocol open shortest path first (OSPF).

Prerequisites

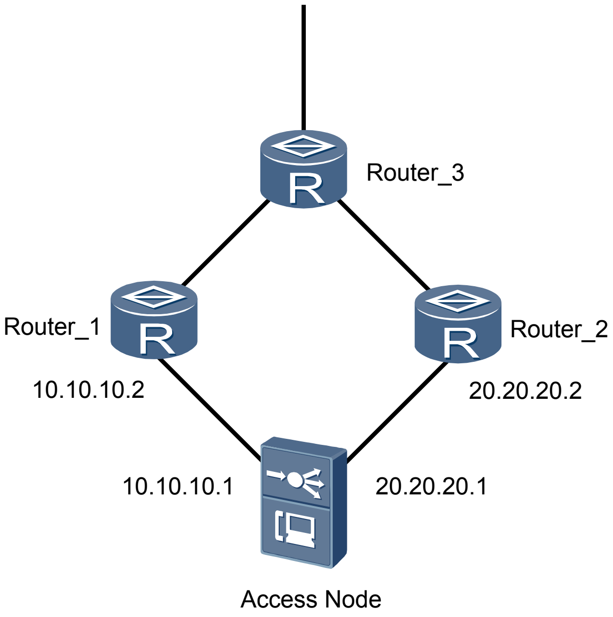
The BFD function must be globally enabled on the MA5600T/MA5603T.

Networking

Figure 14-4 shows an example network of the BFD for OSPF.

Dynamic routes between the MA5600T/MA5603T and Router_1, Router_2 are generated through OSPF. The BFD session is bound to the OSPF route. When one link is faulty, the BFD session reports that the bound OSPF neighbor is down, switching the route.

Figure 14-4 Example network of the BFD for OSPF



Data Plan

Table 14-3 provides the data plan for configuring the BFD for OSPF.

Table 14-3 Data plan for configuring the BFD for OSPF

Item	Data	Remarks
MA5600T/ MA5603T	Upstream ports: 0/19/0 and 0/19/1	-
VLAN	Virtual local area network (VLAN) ID: 30 VLAN type: Smart VLAN IP address of the Layer 3 interface: 10.10.10.1/24	-
	VLAN ID: 40 VLAN type: Smart VLAN IP address of the Layer 3 interface: 20.20.20.1/24	-

Item	Data	Remarks
BFD session	Minimum transmit interval: 10 ms Minimum receive interval: 10 ms Detection multiplier: 3	-
Requirements for the upper-layer device	Router_1: ● IP address of the Layer 3 interface: see the example network ● VLAN ID: 30 ● OSPF: enabled ● BFD session parameters: consistent with the parameters of the MA5600T/MA5603T	For details about the configuration of the router, see the corresponding configuration guide.
	Router_2: ● IP address of the Layer 3 interface: see the example network ● VLAN ID: 40 ● OSPF: enabled ● BFD session parameters: consistent with the parameters of the MA5600T/MA5603T	

Procedure

Step 1 Create VLANs and add upstream ports to the VLANs.

```
huawei(config)#vlan 30 smart
huawei(config)#port vlan 30 0/19 0
huawei(config)#vlan 40 smart
huawei(config)#port vlan 40 0/19 1
```

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

```
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.10.10.1 24
huawei(config-if-vlanif30)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#ip address 20.20.20.1 24
huawei(config-if-vlanif40)#quit
```

Step 3 Configure basic OSPF functions.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.10.10.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 20.20.20.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

Step 4 Configure BFD function on the OSPF interface.

You can configure BFD sessions only after the global BFD function is enabled.

```
huawei(config)#bfd
huawei(config-bfd)#quit
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ospf bfd enable
huawei(config-if-vlanif30)#ospf bfd min-rx-interval 10 min-tx-interval 10 detect-
multiplier 3
```

```
huawei(config-if-vlanif30)#ospf cost 30
huawei(config-if-vlanif30)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#ospf bfd enable
huawei(config-if-vlanif40)#ospf bfd min-rx-interval 10 min-tx-interval 10 detect-
multiplier 3
huawei(config-if-vlanif30)#ospf cost 40
huawei(config-if-vlanif40)#quit
```

Step 5 Save the data.

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

----End

Result

After establishing the neighbor relation with each router through OSPF, the MA5600T/MA5603T automatically creates two BFD sessions. When the active link is faulty, its bound BFD session is down, which triggers the OSPF neighbor relation to be down. Therefore, the route is switched to the standby link.

Run the **display ospf bfd session** command to query the BFD session information.

14.8.4 Configuring BFD for IS-IS

The MA5600T/MA5603T can detect the fault of a dynamic route by using the bidirectional forwarding detection (BFD). This topic describes how to configure the BFD link detection based on the dynamic routing protocol intermediate system to intermediate system (IS-IS).

Prerequisites

The BFD function must be globally enabled on the MA5600T/MA5603T.

Context

To accelerate IS-IS convergence speed when the link status changes, you can configure BFD on the IS-IS link. The MA5600T/MA5603T supports configuration of static and dynamic BFD for IS-IS. When BFD sessions are configured in both methods, the static BFD session takes precedence over the dynamic BFD session.

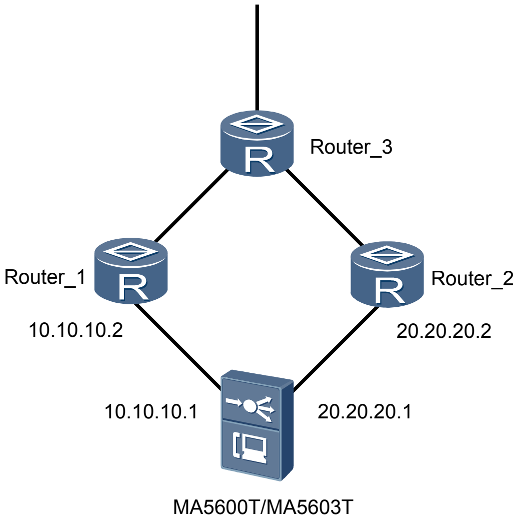
- Static BFD refers to configuring BFD session parameters manually including local and remote identifiers and delivering BFD session setup requests manually.
- Dynamic BFD refers to that routing protocols dynamically trigger the establishment of BFD sessions. When setting up new neighbor relationship, routing protocols send parameters of neighbors and detection parameters (including source and destination IP addresses) to the BFD module. BFD then sets up sessions according to the received parameters between neighbors. Dynamic BFD is more flexible than static BFD.

Networking

Figure 14-5 shows an example network of the BFD for IS-IS.

Dynamic routes between the MA5600T/MA5603T and Router_1, Router_2 are generated through IS-IS. The BFD session is bound to the IS-IS route. When one link is faulty, the BFD session reports that the bound IS-IS neighbor is down, switching the route.

Figure 14-5 Example network of the BFD for IS-IS



Data Plan

Table 14-4 provides the data plan for configuring the BFD for IS-IS.

Table 14-4 Data plan for configuring the BFD for IS-IS

Item	Data	Remarks
MA5600T/ MA5603T	Upstream ports: 0/19/0 and 0/19/1	-
VLAN	Virtual local area network (VLAN) ID: 30 VLAN type: Smart VLAN IP address of the Layer 3 interface: 10.10.10.1/24	-
	VLAN ID: 40 VLAN type: Smart VLAN IP address of the Layer 3 interface: 20.20.20.1/24	-
BFD session	Static BFD session name: ToRouter_1 IP address of the peer interface: 10.10.10.2/24 Local discriminator: 1 Remote discriminator: 2 Minimum transmit interval: 10 ms Minimum receive interval: 10 ms Detection multiplier: 3	-

Item	Data	Remarks
	Static BFD session name: ToRouter_2 IP address of the peer interface: 20.20.20.2/24 Local discriminator: 3 Remote discriminator: 4 Minimum transmit interval: 10 ms Minimum receive interval: 10 ms Detection multiplier: 3	
IS-IS	Network Entity Title (NET): aa.1111.1111.1111.00 Link cost of VLAN interface 30: 30 Link cost of VLAN interface 40: 40	-
Requirements for the upper-layer device	Router_1: ● IP address of the Layer 3 interface: see the example network ● VLAN ID: 30 ● IS-IS: enabled ● Local discriminator of the static BFD session: 2 ● Remote discriminator of the static BFD session: 1 ● Dynamic BFD session parameters: consistent with the parameters of the MA5600T/MA5603T	For details about the configuration of the router, see the correspondin g configuration guide.
	Router_2: ● IP address of the Layer 3 interface: see the example network ● VLAN ID: 40 ● IS-IS: enabled ● Local discriminator of the static BFD session: 4 ● Remote discriminator of the static BFD session: 3 ● Dynamic BFD session parameters: consistent with the parameters of the MA5600T/MA5603T	

Procedure

Step 1 Create VLANs and add upstream ports to the VLANs.

```
huawei(config)#vlan 30 smart
huawei(config)#port vlan 30 0/19 0
huawei(config)#vlan 40 smart
huawei(config)#port vlan 40 0/19 1
```

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

```
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.10.10.1 24
huawei(config-if-vlanif30)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#ip address 20.20.20.1 24
huawei(config-if-vlanif40)#quit
```

Step 3 Configure IS-IS.

```
huawei(config)#isis
huawei(config-isis-1)#network-entity aa.1111.1111.1111.00
huawei(config-isis-1)#quit
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#isis enable
huawei(config-if-vlanif30)#isis cost 30
huawei(config-if-vlanif30)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#isis enable
huawei(config-if-vlanif40)#isis cost 40
huawei(config-if-vlanif40)#quit
```

Step 4 Configure static BFD for IS-IS.

```
huawei(config)#bfd
huawei(config-bfd)#quit
huawei(config)#bfd ToRouter_1 bind peer-ip 10.10.10.2 interface vlanif 30
huawei(config-bfd-session-torouter_1)#discriminator local 1
huawei(config-bfd-session-torouter_1)#discriminator remote 2
huawei(config-bfd-session-torouter_1)#commit
huawei(config-bfd-session-torouter_1)#quit
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#isis bfd static
huawei(config-if-vlanif30)#quit
huawei(config)#bfd ToRouter_2 bind peer-ip 20.20.20.2 interface vlanif 40
huawei(config-bfd-session-torouter_2)#discriminator local 3
huawei(config-bfd-session-torouter_2)#discriminator remote 4
huawei(config-bfd-session-torouter_2)#commit
huawei(config-bfd-session-torouter_2)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#isis bfd static
huawei(config-if-vlanif40)#quit
```

Step 5 Configure dynamic BFD for IS-IS.

```
huawei(config)#isis
huawei(config-isis-1)bfd all-interfaces enable
huawei(config-isis-1)#quit
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#isis bfd enable
huawei(config-if-vlanif30)#isis bfd min-tx-interval 10 min-rx-interval 10 detect-
multiplier 3
huawei(config-if-vlanif30)#quit
huawei(config)#interface vlanif 40
huawei(config-if-vlanif40)#isis bfd enable
huawei(config-if-vlanif40)#isis bfd min-tx-interval 10 min-rx-interval 10 detect-
multiplier 3
huawei(config-if-vlanif40)#quit
```

Step 6 Save the data.

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

----End

Result

After establishing the neighbor relation with each router through IS-IS, the MA5600T/MA5603T creates two BFD sessions. When the active link is faulty, its bound BFD session is down, which triggers the IS-IS neighbor relation to be down. Therefore, the route is switched to the standby link.

Run the **display isis bfd interface** command to query the BFD configuration information of an IS-IS interface.

Run the **display isis bfd session** command to query the BFD session information.

14.9 Configuring ETH OAM

In a broad sense, operation, administration, and maintenance (OAM) means a set of methods for monitoring and diagnosing network faults. The Ethernet OAM feature includes two sub-features: Ethernet CFM OAM and Ethernet EFM OAM.

14.9.1 Configuring the Ethernet CFM OAM

CFM OAM is an OAM at the network level. It supports connectivity check, loopback testing and link tracking, and applies to the end-to-end fault detection in large-scale network.

Prerequisites

- ONT or Modem must support the 802.1ag protocol.
- Service configurations (VLAN configuration and service port configuration, for example) are finished, and the customer services are normal.

Context

The following table shows basic concepts for CFM OAM.

Concepts	Explanations
Maintenance Domain (MD)	Maintenance domain (MD) is a network or part of a network where the CFM management is implemented. The MD can be divided into three types according to the size of the range: customer domain, service provider domain, and operator domain.
Maintenance Association (MA) service	Maintenance association (MA) is a part of an MD, a instance of an MD, and it associates with the monitoring service. An MD consists of one or more MAs.
Maintenance association End Point (MEP)	MEP is the end point of an MA. For any device in the network running ethernet CFM, the MEP on the device is called as local MEP, MEPs on other devices in the same MA are called as remote MEP (relative to the local MEP).
MD Level	There are eight levels, from 0 to 7. It is carried in CFM packets. CFM packets with high-level can pass through the low-level MD. Therefore, different levels of MDs can be nested deployed.

For details about the principle of the CFM OAM, please refer to Ethernet OAM.

Networking

Figure 14-6 shows a typical FTTx integrated networking. Where,

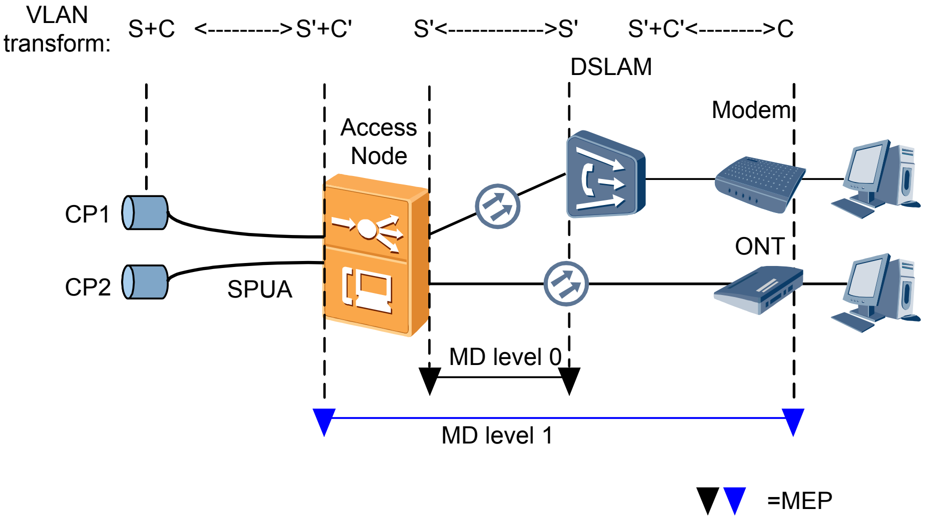
- MA5600T/MA5603T, functioning as access node, accesses the cascading DSLAM by SPUA board.

- MA5600T/MA5603T also functions as OLT, and provides multi-services for customers by accessing ONT.
- DSLAM provides multi-services for customers by accessing xDSL modem.

Through the deployment of CFM OAM, service providers can detect connectivity between any two devices based on their needs. When there is a connectivity problem, the system generates an alarm reporting the fault location.

- Deploy the MD for management channel between cascading port on MA5600T/MA5603T and upstream port on DSLAM.
- Deploy another MD for servide channel between upstream port on MA5600T/MA5603T and UNI port of ONT (or Modem). The level of this MD is higher than the former.

Figure 14-6 Typical networking of CFM OAM



Data Plan

Table 14-5 shows the key data plan for deploying the MD for management channel between cascading port on MA5600T/MA5603T and upstream port on DSLAM.

Table 14-5 Data plan for the Ethernet CFM OAM - MD for management channel

Item	Data
Access Node: MA5600T/ MA5603T	● MD ID: 0. MD name: fttc_md0 ● MD level: 0 ● MA ID: 0. MA name: fttc_ma0 ● MA VLAN: 100 (Management VLAN for the MA5600T/ MA5603T) ● MEP ID: 1. MEP port: 0/2/1 ● MEP VLAN tag: 8 (Management VLAN for the DSLAM). MEP direction: Down ● Remote MEP ID: 2 ● CC-interval: 10 minutes
DSLAM (supposed to be an MA5600T/ MA5603T)	● MD ID: 0. MD name: fttc_md0 ● MD level: 0 ● MA ID: 0. MA name: fttc_ma0 ● MA VLAN: 8 (Management VLAN for the DSLAM) ● MEP ID: 2. MEP port: 0/3/1 ● MEP direction: Down ● Remote MEP ID: 1 ● CC-interval: 10 minutes

Table 14-6 shows the key data plan for deploying another MD for servide channel between upstream port on MA5600T/MA5603T and UNI port of ONT (or Modem).

Table 14-6 Data plan for the Ethernet CFM OAM - MD for service channel

Item	Data
Access Node: MA5600T/ MA5603T	● MD ID: 1. MD name: fttc_md1 ● MD level: 1 ● MA ID: 1. MA name: fttc_ma1 ● MA VLAN: 0 (indicates the MA does not associate any VLAN in system) ● MEP ID: 1. MEP port: 0/2/1 ● MEP VLAN tag1: 1000 (SVLAN for data service on the upstream port of the SPUA board) ● MEP VLAN tag1: 10 (Inner VLAN for data service on the upstream port of the SPUA board) ● MEP direction: Up ● Remote MEP ID: 2 ● CC-interval: 10 minutes

Item	Data
UNI interface of the ONT (or Modem)	Fixed MEP with its level 1.

Procedure

- Configure the MD for management channel on the MA5600T/MA5603T (MD index 0 and MD level 0).

  Pay attention to the follows:

  - The MD name and MA name configured on MA5600T/MA5603T must be the same as that of on DSLAM.
  - Local MEP on MA5600T/MA5603T corresponds to the remote MEP on the DSLAM, and remote MEP on MA5600T/MA5603T corresponds to the local MEP on the DSLAM.

  1. Configure the MD.

     Configure MD 0 with a name of the character string type, name fttc_md0, and MD level 0.

     - MDs with the same index or level cannot be created.
     - The name type and the name of an MD must be unique.
     - The total length of the names of an MD and its MAs cannot be longer than 44 characters.
     - The MD name type, the MD name and the MD level must be consistent at both ends.

     ```
     huawei(config)#cfm md 0 name-format string fttc_md0 level 0 mhf-creation
     no-mhf
     ```

  2. Configure the MA.

     - The system supports up to 4096 MAs. That is, if an MD is configured with 4096 MAs, the other MDs in the system cannot be configured with any MA.
     - An MD of must be available for creating an MA.
     - An existing MA cannot be created again.
     - The total length of the names of an MD and its MAs cannot be longer than 44 characters.
     - The MA name type, the MA name and the sending period of CC packets must be consistent at both ends.

     Create an MA with the index 0/0. The name type is the character string type, and the name is fttc_ma0. The sending period of CC packets is 10 minutes (the sending period of CC packets is 1 minute by default).

     ```
     huawei(config)#cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
     ```

     Set the VLAN associated to the MA to 100, it is the management VLAN of the MA5600T/MA5603T.

     ```
     huawei(config)#cfm ma 0/0 vlan 100
     ```

Set the ID of MEP contained by the MA to 1 and 2. Currently, an MA supports a local MEP and a remote MEP, and their IDs must be unique. MEP ID 2 needs to be configured on the peer DSLAM.

```
huawei(config)#cfm ma 0/0 meplist 1   //local end MEP
huawei(config)#cfm ma 0/0 meplist 2 //remote end MEP on the DSLAM
```

3. Configure the MEP.
   - MEP refers to a maintenance association end points. Ethernet CFM OAM is used to test the link connectivity by using the MEPs at the two ends of a maintenance channel.
   - By default, the MEP management function is enabled, the priority of sending CFM packets is 7, and the function of sending CC packets is enabled.
   - There are two kinds of MEPs: UP MEP and DOWN MEP.An UP MEP indicates that the MEP transmits packets to the bridge trunk direction. A DOWN MEP indicates that the MEP transmits packets to the physical medium direction.
   - **vlantag1** or **vlantag2** must be configured, when you add an MEP is added for a port with service streams. **vlantag2** is the outer VLAN of the port carrying the service link for the MEP. **vlantag2** is the inner VLAN of the port carrying the service link for the MEP.
   - The MEP priority must be consistent at both ends.

```
huawei(config)#cfm mep 0/0/1 direction down port 0/2/1 vlantag1 8 priority
7
```

4. Enable the remote MEP detection function.

   The system can check the remote MEPs of an MA and report alarms for loss of CCM and RDI only when the following functions are enabled: the global CFM function, the global function of checking remote MEPs, and the function of checking the remote MEPs of the MA.

   By default, the remote MEP detection function of MA is enabled, while the global remote MEP detection function is disabled.

   a. Enable the remote MEP detection function of the MA.
   ```
   huawei(config)#cfm ma 0/0 remote-mep-detect enable
   ```
   b. Enable the continuity check function of the MEP.
   ```
   huawei(config)#cfm mep 0/0/1 cc enable
   ```
   c. Enable the global remote MEP detection function.
   ```
   huawei(config)#cfm remote-mep-detect enable
   ```

5. Enable the global CFM function.
```
huawei(config)#cfm enable
```

- Configure the MD for management channel on the DSLAM (MD index 0 and MD level 0).

1. Configure the MD.
```
huawei(config)#cfm md 0 name-format string fttc_md0 level 0 mhf-creation
no-mhf
```

2. Configure the MA.
```
huawei(config)#cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
```

   Set the VLAN associated to the MA to 8, it is the management VLAN of the DSLAM.

```
huawei(config)#cfm ma 0/0 vlan 8
```

Set the ID of MEP contained by the MA to 2 and 1. Currently, an MA supports a local MEP and a remote MEP, and their IDs must be unique. MEP ID 1 needs to be configured on the peer MA5600T/MA5603T.

```
huawei(config)#cfm ma 0/0 meplist 2  //local end MEP on the DSLAM
huawei(config)#cfm ma 0/0 meplist 1 // remote end MEP on the MA5600T/
MA5603T
```

3. Configure the MEP.

```
huawei(config)#cfm mep 0/0/2 direction down port 0/3/1 vlantag1 8 priority
7
```

4. Enable the remote MEP detection function.
   a. Enable the remote MEP detection function of the MA.
   ```
   huawei(config)#cfm ma 0/0 remote-mep-detect enable
   ```
   b. Enable the continuity check function of the MEP.
   ```
   huawei(config)#cfm mep 0/0/2 cc enable
   ```
   c. Enable the global remote MEP detection function.
   ```
   huawei(config)#cfm remote-mep-detect enable
   ```
5. Enable the global CFM function.

```
huawei(config)#cfm enable
```

- Configure the MD for service channel on the MA5600T/MA5603T (MD index 1 and MD level 1).

1. Configure the MD.

Configure MD 1 with a name of the character string type, name fttc_md1, and MD level 1.

```
huawei(config)#cfm md 1 name-format string fttc_md1 level 1 mhf-creation
no-mhf
```

2. Configure the MA.

Create an MA with the index 1/1. The name type is the character string type, and the name is fttc_ma1. The sending period of CC packets is 10 minutes (the sending period of CC packets is 1 minute by default).

```
huawei(config)#cfm ma 1/1 name-format string fttc_ma1 cc-interval 10m
```

This level of ETH OAM is based on point to point forwarding service, the MA VLAN should be 0, it means that the MA does not associate any VLAN in the system.

```
huawei(config)#cfm ma 1/1 vlan 0
```

Set the ID of MEP contained by the MA to 1 and 2. Currently, an MA supports a local MEP and a remote MEP, and their IDs must be unique. MEP ID 2 needs to be configured on the peer device.

```
huawei(config)#cfm ma 1/1 meplist 1   //local end MEP
huawei(config)#cfm ma 1/1 meplist 2   //remote end MEP on the ONT (or
Modem)
```

3. Configure the MEP.

Set the service VLAN to 1000 and inner vlan to 10 on the upstream port of SPUA board, which maps to an UNI port of the ONT (or Modem). Set the direction to up.

```
huawei(config)#cfm mep 1/1/1 direction up port 0/2/1 vlantag1 1000
vlantag2 10 priority 7
```

4. Enable the remote MEP detection function.

The system can check the remote MEPs of an MA and report alarms for loss of CCM and RDI only when the following functions are enabled: the global CFM function, the global function of checking remote MEPs, and the function of checking the remote MEPs of the MA.

By default, the remote MEP detection function of MA is enabled, while the global remote MEP detection function is disabled.

a. Enable the remote MEP detection function of the MA.
```
huawei(config)#cfm ma 1/1 remote-mep-detect enable
```
b. Enable the continuity check function of the MEP.
```
huawei(config)#cfm mep 1/1/1 cc enable
```
c. Enable the global remote MEP detection function.
```
huawei(config)#cfm remote-mep-detect enable
```

5. Enable the global CFM function.
```
huawei(config)#cfm enable
```

----End

Result

After the configuration is finished,

- MA5600T/MA5603T or DSLAM is able to learn the MEP ID and MAC address from its remote peer automatically. You can run the **display cfm mep** command to query MEP configuration.
- Disconnect MA5600T/MA5603T and DSLAM, the system will generate CFM OAM alarm automatically, reporting the fault location and cause.
- Run the **cfm loopback** command on the MA5600T/MA5603T to start a remote loopback test. Under normal circumstances, the number of packets sent and received must be the same.

Configuration File

Configure the MD for management channel on the MA5600T/MA5603T (MD index 0 and MD level 0).

```
cfm md 0 name-format string fttc_md0 level 0 mhf-creation no-mhf
cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
cfm ma 0/0 vlan 100
cfm ma 0/0 meplist 1   //local end MEP
cfm ma 0/0 meplist 2 //remote end MEP on the DSLAM
cfm mep 0/0/1 direction down port 0/2/1 vlantag1 8 priority 7
cfm ma 0/0 remote-mep-detect enable
cfm mep 0/0/1 cc enable
cfm remote-mep-detect enable
cfm enable
```

Configure the MD for management channel on the DSLAM (MD index 0 and MD level 0).

```
cfm md 0 name-format string fttc_md0 level 0 mhf-creation no-mhf
cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
cfm ma 0/0 vlan 8
cfm ma 0/0 meplist 2   //local end MEP
cfm ma 0/0 meplist 1 //remote end MEP on the MA5600T/MA5603T
cfm mep 0/0/2 direction down port 0/3/1 vlantag1 8 priority 7
cfm ma 0/0 remote-mep-detect enable
cfm mep 0/0/2 cc enable
cfm remote-mep-detect enable
cfm enable
```

Configure the MD for service channel on the MA5600T/MA5603T (MD index 1 and MD level 1).

```
cfm md 1 name-format string fttc_md1 level 1 mhf-creation no-mhf
cfm ma 1/1 name-format string fttc_ma1 cc-interval 10m
cfm ma 1/1 vlan 0
cfm ma 1/1 meplist 1   //local end MEP
cfm ma 1/1 meplist 2 //remote end MEP on the DSLAM
cfm mep 1/1/1 direction up port 0/2/1 vlantag1 1000 vlantag2 10 priority 7
cfm ma 1/1 remote-mep-detect enable
cfm mep 1/1/1 cc enable
cfm remote-mep-detect enable
cfm enable
```

14.9.2 Configuring the Ethernet EFM OAM

EFM OAM is OAM at the link level, it is used to monitor the link status between customer premises equipment and service provider. It focuses on point-to-point ethernet link management and maintenance.

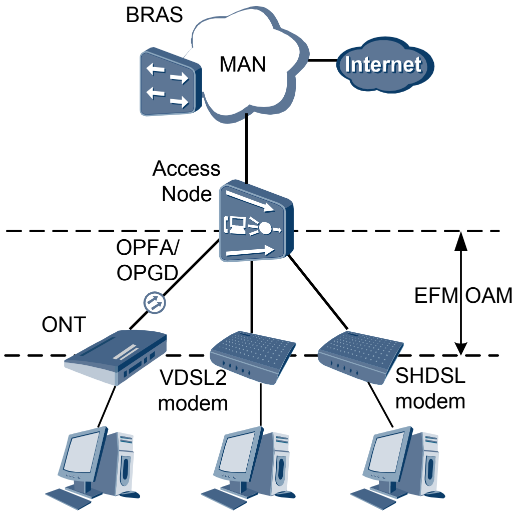
Prerequisites

- ONT or Modem must support the 802.3ah protocol, and Modem must support to run at the VDSL2 PTM mode or SHDSL PTM mode.
- Service configurations (VLAN configuration and service port configuration, for example) are finished, and the customer services are normal.

Context

- The service boards that support EFM OAM are OPFA, OPGD, VDSL2 boards and SHDSL boards.
- Ethernet EFM OAM is enabled on both local side (MA5600T/MA5603T) and remote side (ONT or Modem).
- When the remote end is faulty, the local end generates an alarm.
- The local end can be used to locate a fault through the EFM remote end loopback.

Figure 14-7 EFM OAM networking



Data Plan

Table 14-7 shows the data plan for configuring Ethernet EFM OAM.

Table 14-7 Data plan for configuring EFM OAM

Item	Data
Local end (MA5600T/ MA5603T)	Port: 0/2/0 EFM OAM mode: active
Remote end (ONT or Modem)	EFM OAM mode: passive Loopback control parameter: process

Procedure

- Configure the local end MA5600T/MA5603T.
  1. (Optional) Configure the Ethernet EFM OAM mode of the port.

     Configure Ethernet OAM port 0/2/0 to actively initiate the discovery process and the loopback control packet. The default mode is the active mode.

     ```
     huawei(config)#efm oam mode 0/2/0 active
     ```
  2. (Optional) Configure the loopback control parameter of the Ethernet EFM OAM port.

     By default, EFM remote loopback is disabled, and the configuration of the local end is process.

     ```
     huawei(config)#efm loopback 0/2/0 process
     ```
  3. Enable Ethernet EFM OAM of the port.

     After Ethernet EFM OAM is enabled, the loopback control parameter and Ethernet EFM OAM mode of the port cannot be modified.

     ```
     huawei(config)#efm oam 0/2/0 enable
     ```
  4. Save the data.

     ```
     huawei(config)#save
     ```
  5. (Optional) Enable EFM remote loopback.

     When the remote end is faulty, use the EFM remote loopback function to locate the fault.

     ```
     huawei(config)#efm loopback 0/2/0 start
       Starting loopback will interrupt all the services on this port. Are you 
     sure
     to start loopback? (y/n)[n]:y
     ```
- Configure the remote ONT or Modem.

  The parameter values configured on the remote end (ONT or Modem) are as follows:

  - EFM OAM mode: passive
  - loopback control parameter: enabled
  - EFM OAM function: enabled

  For details, please refer to the web configuration guide of the ONT or Modem.

----End

Result

After the configuration is completed, run the **display efm oam status** command on MA5600T/MA5603T to query the relevant information about the local end or remote end.

```
huawei#display efm oam status 0/2/0 local
  Admin Status                     : Enable
  Operation Status                 : Operational  //negotiation succeed
  OAM Mode                         : Active     //active mode
  Max OAM PDU Size                 : 1514
  Stable & Evaluation              : 3
  Configuration Revision           : 0
  Multiplexer Action               : Forward
  Parser Action                    : Forward
  Unidirectional Support           : No
  Loopback Support                 : Yes    //supports the remote loopback
  Event Support                    : Yes
  Variable Support                 : No
huawei#display efm oam status 0/2/0 remote
  MAC Address                      : 0020-d226-5679  //MAC address of remote OAM
entry
  Verdor OUI                       : 0x0020d2     //OUI of remote OAM entry
  Verdor Specific Info             : 0
  OAM Mode                         : Passive     //passive mode
  Max OAM PDU Size                 : 1514
  Stable & Evaluation              : 2
  Configuration Revision           : 2653
  Multiplexer Action               : Forward
  Parser Action                    : Forward
  Unidirectional Support           : No
  Loopback Support                 : Yes  //supports the remote loopback
  Event Support                    : Yes
  Variable Support                 : Yes
```

Follow-up Procedure

When one port on the service board of the MA5600T/MA5603Tis fault, EFM OAM will generate a event and report the local fault notification.

```
huawei(config)#interface opg 0/2
huawei(config-if-opg-0/2)#shutdown 0
! RUNNING MAJOR yy-mm-dd xx:xx:xx+8:00 EVENT NAME :Ethernet OAM link events
  PARAMETERS :FrameID:0 SlotID:2, PortID:0 OAM Alarm type: Link Fault
  Event AlarmLocation: Local
```

When one of the upstream port of ONT or Modem is fault, EFM OAM will generate a event and report the remote fault notification.

```
huawei(config)#
! RUNNING MAJOR yy-mm-dd xx:xx:xx+8:00 EVENT NAME :Ethernet OAM link events
  PARAMETERS :FrameID:0 SlotID:2, PortID:0 OAM Alarm type: Dying Gasp
  Event AlarmLocation: Remote
```

14.10 Configuring GPON Protection

The MA5600T/MA5603T supports Type B, Type C protection. This topic describes the configuration of each type of protection.

14.10.1 Configuring Type B Protection

Type B protection is to configure 1+1 redundancy backup of different GPON ports on MA5600T/MA5603T. In this way, when a GPON port is faulty, automatic switching is performed and the services are not affected.

Context

The GPON port supports redundancy backup on the same board and the redundancy on different boards. The differences are as follows:

- Port redundancy backup on the same board does not require extra GPON service board, which saves hardware resources. In case that the GPON service board fails, however, the services on the entire board are interrupted.
- Port redundancy backup on the different boards requires an independent standby GPON service board, which increases the hardware cost. In the case that the active GPON service board fails, however, the services can be automatically switched over to the GPON ports on the standby board, and the service access is not affected.

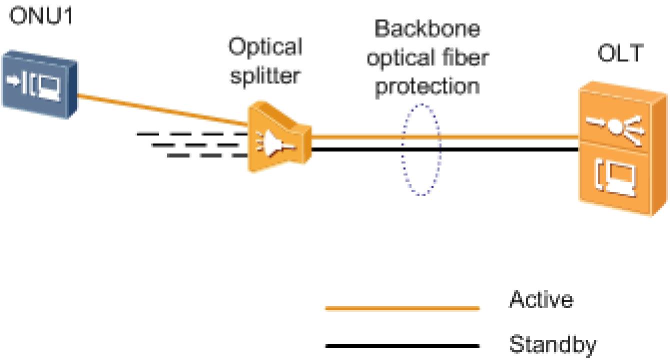
NOTE

Only GPON boards of the same type support inter-board redundancy backup.

After Type B protection is configured, service configuration on the ONU is the same as that before Type B protection is configured. That is, service configuration is applied to the active GPON port only.

Figure 14-8 shows the Type B protection network topology.

Figure 14-8 Type B protection network topology



Precautions

Type B protection, Type C single homing protection and Type C dual homing protection are mutually exclusive. Only one protection can be deployed on an ONU.

Procedure

Step 1 Create a GPON port protection group.

Run the **protect-group** command to add a protection group that protects the ports on the GPON access side.

NOTE

1. Configure **protect-target** to **gpon-uni-port**.
2. The working mode of the GPON port protection group can be only **timedelay**.

Step 2 Add members to the protection group.

Run the **protect-group member** command to add members to a protection group.

NOTE

- When adding members to the protection group, add a working member, and then add a protection member.
- Adding a protection group member based on the board is not supported for the GPON port, and only adding a protection group member based on the port is supported.
- The member ports can be ports on different GPON boards, but the GPON board types must be the same.

Step 3 Enable the protection group.

Run the **protect-group enable** command to enable the GPON protection group. After a protection group is created, the protection group is in the disabled state by default. You should enable the protection group to make the configuration take effect.

Step 4 Query the information about the protection group.

Run the **display protect-group** command to query the information about the protection group and all the members in the protection group.

NOTE

The GPON protection group supports the binding to a PPPoE single-MAC address pool. When the PPPoE single-MAC address function is enabled, run the **bind mac-pool single-mac** command to bind a GPON protection group to a PPPoE single-MAC address. If the GPON protection group is not bound to the PPPoE source MAC address, when the GPON protection group is switched over, the PPPoE service carried on this port is interrupted. In this case, you must re-dial and determine the service interruption time according to the BRAS configuration. This may fail to meet the switchover performance requirement that the service interruption time must not exceed 50 ms.

----End

Result

After the configuration, the active GPON port on the OLT is in the **active** state, while the standby GPON port is in the **standby** state.

The OLT will automatically switch services from active GPON port to the standby GPON port within 50 ms if one of the following conditions is met:

- The backbone optical fiber is broken.
- The bit error rate (BER) of the line is high.
- The active GPON port is faulty.
- The GPON board is reset or powered off.

Example

To configure redundancy backup for ports 0/2/0 and 0/2/1 on the same GPON board of the MA5600T/MA5603T so that when port 0/2/0 is faulty, the system can automatically switch the service to port 0/2/1 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 0/2/0 role work
huawei(protect-group-0)#protect-group member port 0/2/1 role protect
huawei(protect-group-0)#protect-group enable
```

To configure inter-board redundancy backup for ports 0/3/1 and 0/4/1 on different GPON boards of the MA5600T/MA5603T so that when port 0/3/1 is faulty, the system can automatically switch the service to port 0/4/1 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 0/4/1 role protect
huawei(protect-group-0)#protect-group enable
```

14.10.2 Configuring Type C Single Homing Protection

In a network topology with Type C single homing protection, the two PON ports of each ONU are connected upstream to two PON ports of the OLT using two different optical splitters, protecting the backbone optical fibers and tributary optical fibers. This ensures high reliability of the network.

Prerequisites

The example network as shown in **Figure 14-9** is complete.

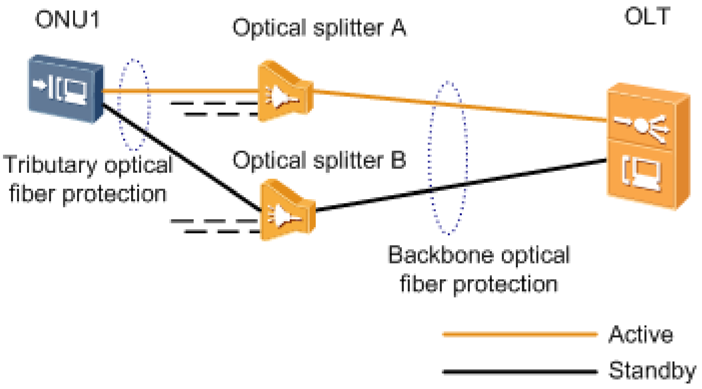
Context

Type C single homing protection is to protect the optical fiber link between the OLT and ONU. When the PON port of an ONU, optical splitter, or GPON port of the OLT malfunctions, the system automatically switches to the standby link and continue to provide services.

Figure 14-9 shows the Type C single homing protection network topology. Type C single homing protection requires two 1:N optical splitters, one connected to the active PON port on the OLT and the other to the standby PON port on the OLT. In this way, the backbone optical fibers and tributary optical fiber are protected at the same time.

Service configurations on the ONU before and after Type C single homing protection configuration are the same. That is, service configuration is applied only to the active PON ports (PON port of the OLT and PON port of the ONU).

Figure 14-9 Example network of Type C single homing


ONU1
Optical splitter A
OLT
Tributary optical fiber protection
Optical splitter B
Backbone optical fiber protection
Active
Standby

Procedure

Step 1 Add an ONU at the working side.

Run the **ont add** command to add an ONU at the working side.

Step 2 Add an ONU at the protection side.

Run the **ont add** *portid ontid* **protect-side** command to add an ONU at the protection side. **protect-side** must be selected.

Step 3 Add a Type C protect group.

Run the **protect-group protect-target gpon-uni-ont** command to add a protect group.

Step 4 Add a working member to the protect group.

Run the **protect-group member** command to add the ONU connected to the active GPON port to the protect group as a working member.

Step 5 Add a protection member to the protect group.

Run the **protect-group member** command to add the ONU connected to the standby GPON port to the protect group as a protection member.

NOTE

ONT *ontid* must be the same as the ONT ID specified in **Step 1**.

Step 6 Enable the protect group.

Run the **protect-group enable** command to enable the GPON protect group. After a protect group is created, the protect group is in the disabled state by default. You need to enable the protect group to make the protect group take effect.

----End

Example

As shown in **Figure 14-9**, to configure Type C protection for the optical fiber link between the MA5600T/MA5603T and the ONU with the following settings, do as follows:

- Ports 0/2/0 and 0/2/1 are on the same GPON service board.
- Port 0/2/0 functions as the working member.
- Port 0/2/1 functions as the protection member.
- ONU ID is 0.
- The ONU adopts SN (SN: hwhw-10101500) authentication and the OMCI management mode.
- The ONU is bound to line profile 10 and service profile 10.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 0 sn-auth hwhw-10101500 omci ont-lineprofile-
id 10 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 0 protect-side
huawei(config-if-gpon-0/2)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/2/0 ont 0 role work
huawei(protect-group-1)#protect-group member port 0/2/1 ont 0 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

14.10.3 Configuring Type C Dual Homing Protection

Type C dual homing is an enhancement of Type C single homing. Using Type C dual homing, any node between OLTs and ONUs is protected after ONUs dual home to two OLTs.

Context

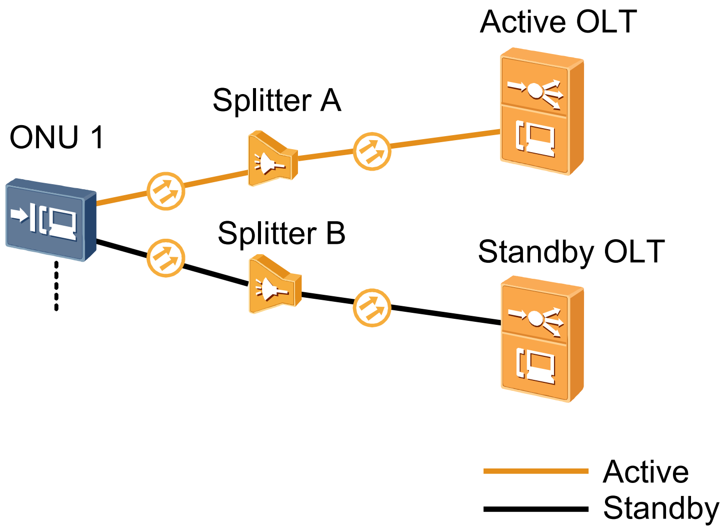
Figure 14-10 shows the network of Type C dual homing protection. The PON ports on two different OLTs, two PON ports on the ONU, backbone optical fiber, optical splitters and distribution optical fiber are in dual configuration. The main difference between Type C dual homing and Type C single homing is that ONUs need to dual home to two OLTs in Type C dual homing scenario.

NOTE

The MA5600T/MA5603T can be regarded as an OLT if ONUs are connected to the MA5600T/MA5603T through GPON. All the below-mentioned OLTs indicate the MA5600T/MA5603T.

Compared with Type C single homing, Type C dual homing can provide more comprehensive network protection. However, the networking will be more complicated and the cost will be higher. Currently, Type C dual homing is mainly used in the electric power protection, and it also can be used in the protection of QinQ private line services.

Figure 14-10 Example network of Type C dual homing



Precautions

1. Type C dual homing protection, Type B protection nad Type C single homing protection and are mutually exclusive. Only one protection can be deployed on a network.
2. The types and versions of control boards and GPON boards on the active and standby OLTs must be the same. In addition, the active and standby OLTs cannot perform the data synchronization automatically. Therefore, users must make sure the data consistency between the two OLTs.

Procedure

Step 1 Configure the active OLT.

1. Run the **ont add** command to add an active ONU.
2. Run the **protect-group** command to create a protect group.
   - Set the **protect-target** to **gpon-uni-port**.
   - The working mode of the GPON port protect group must be **dual-parenting**.
3. 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.

Step 2 Configure the standby OLT.

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

   NOTE

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

2. 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.
3. Run the **protect-group member** command to add members to the protect group.
4. Run the **protect-group enable** command to enable the protect group.

----End

Result

After the configuration, the active and standby GPON ports on the OLT are in the working state. The ONU and OLT will check the link status and determine whether the protection switching is performed according to the link status.

The OLT will automatically switch services from the active link to the standby link within 50 ms if one of the following conditions is met:

- The backbone optical fiber is broken.
- The branch optical fiber is broken.
- The quality of upstream or downstream optical signals becomes poor.
- The hardware (for example, a GPON port on the OLT or an upstream port on the ONU) is faulty.

Example

In the electric power network, the power system is required to collect information in real-time mode and to transmit information automatically. To meet such requirements, Type C dual homing protection is configured for the active and standby OLTs (huawei_A and huawei_B), with other related data configured as follows:

- 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
```

15 Configuring ARP Proxy for Interworking

This topic describes how to configure the Address Resolution Protocol (ARP) proxy of the Layer 3 interface so that users on isolated ports of the same broadcast domain or on ports of different broadcast domains can communicate with each other. To reduce the network load, the ARP request packets are limited in a VLAN.

Context

- By default, the ARP proxy function is disabled.
- When the ARP proxy function is enabled for a super VLAN, sub VLANs in the super VLAN can communicate with each other. To enable the nodes in a sub VLAN to communicate with each other, the ARP proxy function must be enabled for the sub VLAN. Configurations for different scenarios are as follows:
  - In a scenario for Layer 3 communication between users in different VLANs, enable the ARP proxy function for the system, for the super VLAN, and for the sub VLANs in the super VLAN.
  - In a scenario for Layer 3 communication between users in the same VLAN, enable the ARP proxy function for the system, and for the VLAN. The super VLAN does not need to be created.

Networking

Figure 15-1 and **Figure 15-2** shows an example network of the ARP proxy.

PC1 and PC2 are in sub VLAN 10, service ports are isolated, and PC3 is in sub VLAN 20. User packets can be forwarded in the Layer 3 forwarding mode through the super VLAN interface. The IP address of the super VLAN interface is 10.0.0.254, and the interface is in the same subnet as PC1, PC2, and PC3. After the ARP proxy function is enabled, PC1 and PC2 can communicate with each other, and PC3 can communicate with PC1 and PC2.

Figure 15-1 Example network of the ARP proxy in a DSLAM network

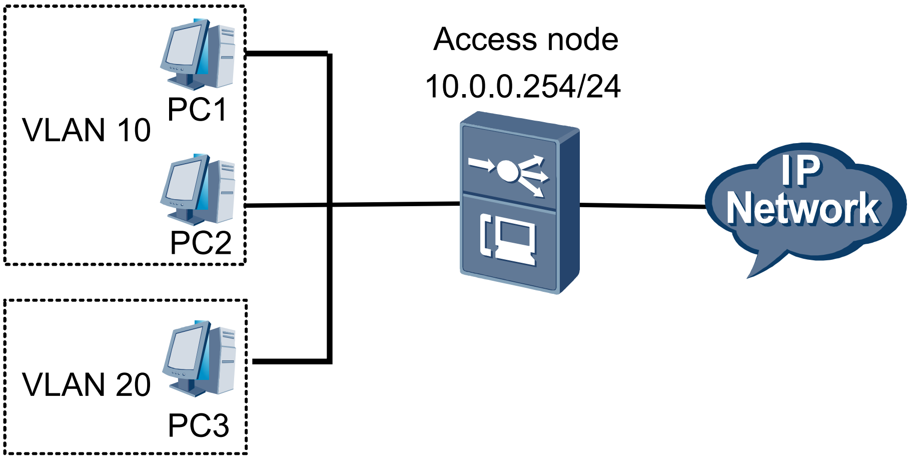
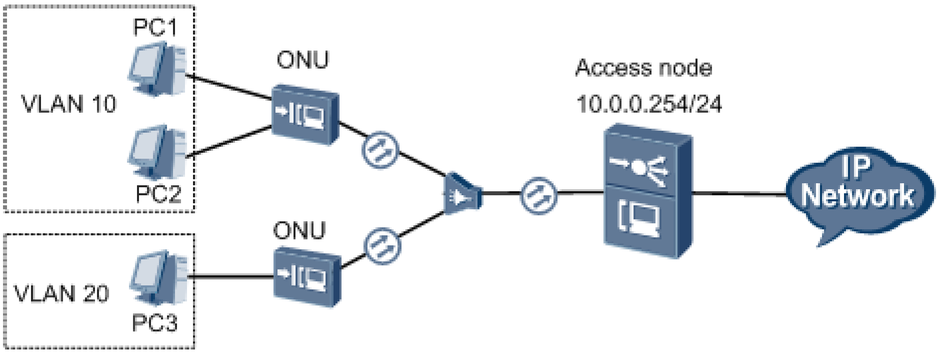


Figure 15-2 Example network of the ARP proxy in an FTTx network



Data Plan

Table 15-1 provides the data plan for configuring the ARP proxy.

Table 15-1 Data plan for configuring the ARP proxy

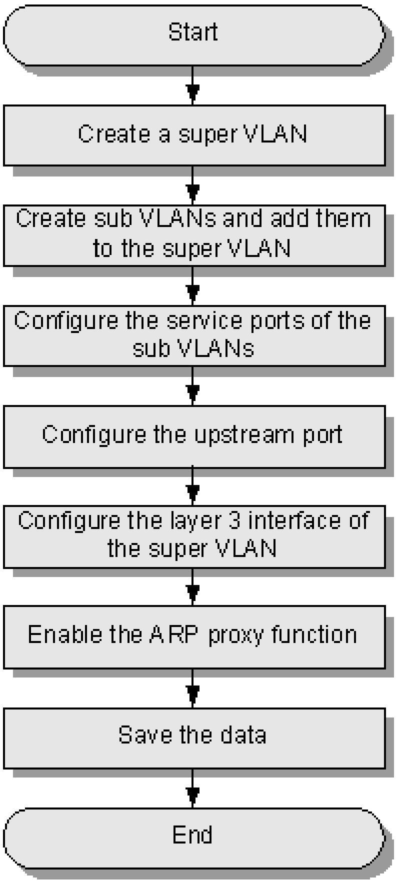
Item	Data
Super VLAN	VLAN ID: 100
	Sub VLAN: VLAN 10, VLAN 20
	IP address: 10.0.0.254/24
Sub VLAN	VLAN ID: 10
	VLAN type: smart VLAN
Sub VLAN	VLAN ID: 20
	VLAN type: MUX VLAN

Item	Data
Upstream port	Port: 0/19/0
	VLAN: standard VLAN 30
	IP address: 10.0.1.254/24

Configuration Flowchart

Figure 15-3 shows the flowchart for configuring the ARP proxy.

Figure 15-3 Flowchart for configuring the ARP proxy


Start
Create a super VLAN
Create sub VLANs and add them to the super VLAN
Configure the service ports of the sub VLANs
Configure the upstream port
Configure the layer 3 interface of the super VLAN
Enable the ARP proxy function
Save the data
End

Procedure

Step 1 Create a super VLAN.

```
huawei(config)#vlan 100 super
```

Step 2 Create sub VLANs, and add them to the super VLAN.

```
huawei(config)#vlan 10 smart
huawei(config)#vlan 20 mux
huawei(config)#supervlan 100 subvlan 10
huawei(config)#supervlan 100 subvlan 20
```

Step 3 Configure the service ports of the sub VLANs.

- Configurations in a DSLAM network

```
huawei(config)#service-port vlan 10 adsl 0/2/0 vpi 0 vci 35 rx-cttr 5 tx-cttr 5
huawei(config)#service-port vlan 10 adsl 0/2/1 vpi 0 vci 35 rx-cttr 5 tx-cttr 5
huawei(config)#service-port vlan 20 adsl 0/3/0 vpi 0 vci 35 rx-cttr 5 tx-cttr 5
```

NOTE

VPI/VCI configured on the modem must be 0/35.

- Configurations in an FTTx network

```
huawei(config)#service-port vlan 10 gpon 0/2/0 gemport 128 multi-service user-
vlan 15 rx-cttr 5 tx-cttr 5
huawei(config)#service-port vlan 10 gpon 0/2/1 gemport 129 multi-service user-
vlan 16 rx-cttr 5 tx-cttr 5
huawei(config)#service-port vlan 20 gpon  0/3/1 gemport 130 multi-service user-
vlan 17 rx-cttr 5 tx-cttr 5
```

Step 4 Configure the upstream port.

```
huawei(config)#vlan 30 standard
huawei(config)#port vlan 30 0/19 0
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.0.1.254 24
```

NOTE

The IP address of the Layer 3 interface of the super VLAN must be in the same subnet with the IP address obtained by the PC1-PC3.

Step 5 Configure a Layer 3 Interface for the super VLAN

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.0.0.254 24
```

NOTE

The IP address of the Layer 3 interface of the super VLAN must be in the same subnet with the IP address obtained by the PC.

Step 6 Enable ARP proxy.

1. Enable the ARP proxy function globally.

```
huawei(config)#arp proxy enable
```

2. Enable the global ARP proxy on the VLAN interface. After the command is executed, users in different VLANs can communicate with each other.

```
huawei(config-if-vlanif100)#arp proxy enable
```

3. Enable ARP proxy on the sub VLAN interface. After the command is executed, users in the same sub VLAN can communicate with each other.

NOTE

Skip this step if you only want PCs in different VLANs to communicate with each other.

```
huawei(config-if-vlanif100)#arp proxy enable subvlan 10
huawei(config-if-vlanif100)#quit
```

Step 7 Save the data.

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

----End

Result

- After the global ARP proxy function and the ARP proxy function of the super VLAN interface are enabled, PC1 and PC3, PC2 and PC3 in different VLANs can communicate with each other.
- After the global ARP proxy function, the ARP proxy function of the super VLAN interface, and that of the sub VLAN interface are enabled, PC1 and PC2 in the same VLAN can communicate with each other.

16 Configuring the DSLAM Subtending

About This Chapter

Multiple MA5600T/MA5603Ts can be subtended.

The MA5600T/MA5603Ts (NEs) can be directly connected to each other though the FE or GE port. Subtending saves the upstream optical fibers and simplifies networking and service configuration.

ATM-DSLAM access means that the MA5600T/MA5603T provides the ATM interface (for example, STM-1) for the subtending of earlier ATM-DSLAMs.

16.1 Configuring the NE Subtending Through the FE or GE Port

The MA5600T/MA5603Ts (NEs) can be directly connected to each other though the FE or GE port. Subtending saves the upstream optical fibers and simplifies networking and service configuration.

Context

- The two ports to be subtended must be the same in the port type, port rate, and port duplex mode.
- ETHB board supports to set the network role of the port based only on whole board, so if the ETHB board is used for subtending, the network role of the all ports on the ETHB board must be set as "cascade".
- GIU board supports to set the network role of each port, so if the GIU board is used for subtending, the network role of the specified port on the GIU board must be set as "cascade".

Procedure

Step 1 Configure the VLAN of the master NE.

The VLAN type is smart, and the VLAN attribute is common. For details about the configuration, see **2.6 Configuring a VLAN**.

Step 2 Add an upstream port to the VLAN of the master NE.

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

Step 3 Add a subtending port to the VLAN of the master NE.

Run the **port vlan** command to add a subtending port to the VLAN.

Step 4 Set the network role of the subtending port of the master NE.

1. Run the **interface eth** command or **interface giu** command to enter the ETH mode or GIU mode.
2. Run the **network-role** command to set the network role of the port to subtending.

   By default, the port of ETHB board functions as a cascade port, while the port of GIU board functions as an upstream port.

Step 5 Configure the VLAN of the slave NE. The VLAN of the slave NE is the same as the VLAN of the master VLAN.

The VLAN type is smart, and the VLAN attribute is common. For details about the configuration, see **2.6 Configuring a VLAN**.

Step 6 Add an upstream port to the VLAN of the slave NE.

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

----End

Example

Assume that master NE huawei_A and slave NE huawei_B are subtended through the GIU board. To add upstream port 0/19/0 and subtending port 0/19/1 of huawei_A to VLAN 100, and add upstream port 0/19/0 of huawei_B to VLAN 100, do as follows:

```
huawei_A(config)#vlan 100 smart
huawei_A(config)#port vlan 100 0/19 0
huawei_A(config)#port vlan 100 0/19 1
huawei_A(config)#interface giu 0/19
huawei_A(config-if-giu-0/19)#network-role 1 cascade

huawei_B(config)#vlan 100 smart
huawei_B(config)#port vlan 100 0/19 0
```

Assume that master NE huawei_A and slave NE huawei_B are subtended through the ETHB board. To add upstream port 0/19/0and subtending port 0/2/0 of huawei_A to VLAN 100, and add upstream port 0/19/0 of huawei_B to VLAN 100, do as follows:

```
huawei_A(config)#vlan 100 smart
huawei_A(config)#port vlan 100 0/19 0
huawei_A(config)#port vlan 100 0/2 0
huawei_A(config)#interface eth 0/2
huawei_A(config-if-eth-0/2)#network-role cascade
huawei_A(config-if-eth-0/2)#quit

huawei_B(config)#vlan 100 smart
huawei_B(config)#port vlan 100 0/19 0
```

16.2 Configuring the ATM-DSLAM Access Service

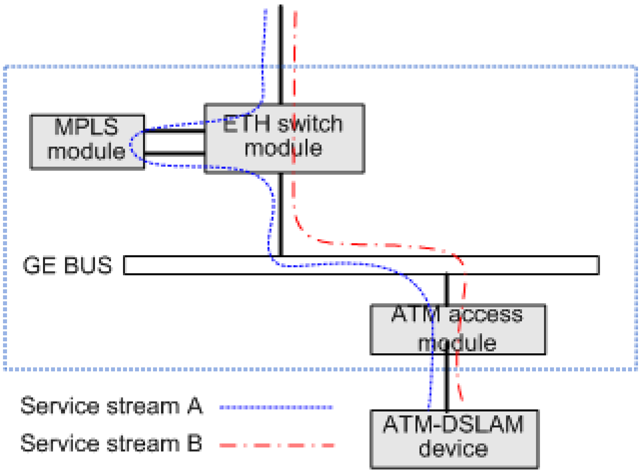
ATM-DSLAM access means that the MA5600T/MA5603T provides the ATM interface (for example, STM-1) for the subtending of earlier ATM-DSLAMs.

Context

In the evolution from ATM networks to IP networks, carriers will replace their ATM-DSLAM network devices in the access layer with IP network devices. In this evolution, a large number of ATM network devices still exist in the network for a long time. The MA5600T/MA5603T provides ATM ports for lower level ATM network devices to access the network.

The MA5600T/MA5603T provides four ATM optical ports (STM-1) through the AIUG board for connecting to the ATM-DSLAM, and also provides the common Ethernet upstream or MPLS upstream service, as shown in **Figure 16-1**.

Figure 16-1 ATM-DSLAM access



The MA5600T/MA5603T can provide two upstream transmission modes: direct Ethernet upstream transmission mode and MPLS upstream transmission mode.

- Directly Ethernet upstream transmission mode: Traffic stream B of the ATM-DSLAM is directly transmitted upstream to the upper-layer IP network through the Ethernet switching module of the SCU board. This mode is applicable to the common Internet access service.
- MPLS upstream transmission mode: The MA5600T/MA5603T functions as a provider edge (PE), transmitting and services of the subtended ATM-DSLAM through the upstream port to the MPLS network. This mode is applicable to the private line service. According to actual requirements, the data on the upstream port can be encapsulated in the ATM PWE3 mode or the ETH PWE3 mode.
  - ATM PWE3: The MA5600T/MA5603T creates a transparent transmission channel for private line users. After encapsulated in the ATM PWE3 mode, the data is transmitted upstream to the MPLS core network. After reaching the peer device, the data is decapsulated, and the ATM cells are transmitted downstream to peer users. This encapsulation mode is applicable to the scenario where the ATM-DSLAM needs to communicate with the peer ATM-DSLAM or peer ATM BRAS over the MPLS network.
  - ETH PWE3: The MA5600T/MA5603T creates a transparent transmission channel for users. After encapsulated in the ATM PWE3 mode, the data is transmitted upstream to the MPLS core network. After reaching the peer device, the data is decapsulated. This encapsulation mode is applicable to the scenario where xPoA private line users perform authentication and packet forwarding over the MPLS network.

    NOTE

    For xPoA users, the xPoA to xPoE protocol conversion should be configured.

17 Example: Configuring the DSLAM Services

About This Chapter

This topic describes how to configure the typical services such as Internet access, multicast, voice, and triple play services on the MA5600T/MA5603T.

17.1 Example: Configuring the xDSL Internet Access Service

This topic describes how to configure the xDSL Internet access service in the PPPoE, IPoE, PPPoA, IPoA and 802.1X modes.

17.1.1 Example: Configuring the xDSL Internet Access Service Through PPPoE Dialup

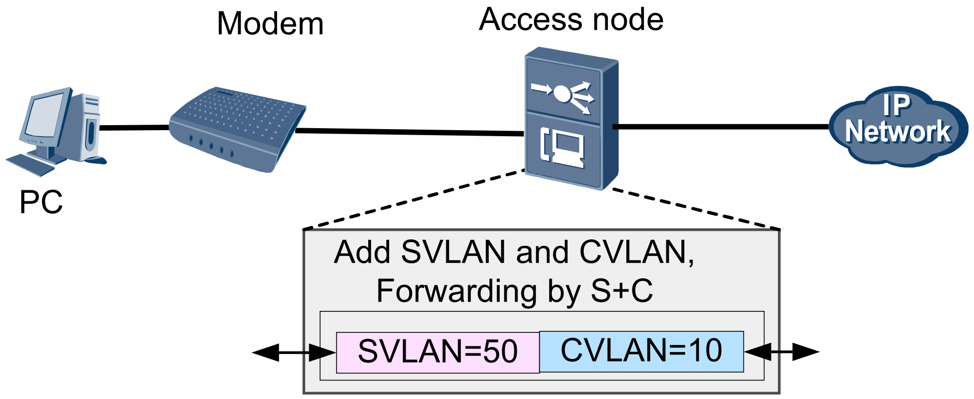
On a fiber to the x (FTTx) network, if the MA5600T/MA5603T provides x digital subscriber line (xDSL) services for broadband users and the users connect to the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dialup mode, you can configure the MA5600T/MA5603T by referring to this topic to provide users with high-speed Internet (HIS) services. The MA5600T/MA5603T functions as an optical network unit (ONU) in this service. PPPoE is a commonly used Internet access mode currently. In this mode, broadband users are authenticated, authorized, and charged in Authentication, Authorization and Accounting (AAA) method.

Service Requirements

- The user accesses the Internet through the PPPoE dialup.
- The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, that is, this is a 1:1 access scenario.
- A traffic profile is adopted for rate limitation. The user access rate is 2048 kbit/s.
- To ensure reliability, dual GE ports are adopted for upstream transmission, and link aggregation is configured for the two upstream ports.

Figure 17-1 shows an example network of the xDSL Internet access service through the PPPoE dialup.

Figure 17-1 Example network of the xDSL Internet access service through the PPPoE dialup



Prerequisite

- The AAA function must be configured.

- To enable the AAA function on the device, see **2.11 Configuring AAA**.
- If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Procedure

Step 1 Configure a VLAN.

Configure S-VLAN 50 with the stacking attribute. The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, and the VLAN forwarding mode is the S-VLAN+C-VLAN mode.

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#vlan forwarding 50 vlan-connect
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

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

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **4.1.1 Configuring an ADSL2+ Template**. The default ADSL2+ line template (line template 1) and the default ADSL2+ alarm template (alarm template 1) are used as an example.
2. Activate the ADSL port, and bind the ADSL2+ templates.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

   In the ADSL access mode, bind the default ADSL2+ line template 1 and ADSL2+ alarm template 1 to ADSL port 0/2/0.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 profile-index 1
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:
```

```
Command:
        display traffic table ip from-index 0
---------------------------------------------------------------------------
 TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
     (kbps)   (bytes)  (kbps)   (bytes)
---------------------------------------------------------------------------
   0 1024     34768    2048     69536      6 -                      tag-pri
   1 2496     81872    4992     163744     6 -                      tag-pri
   2 512      18384    1024     36768      0 -                      tag-pri
   3 576      20432    1152     40864      2 -                      tag-pri
   4 64       4048     128      8096       4 -                      tag-pri
   5 2048     67536    4096     135072     0 -                      tag-pri
   6 off      off      off      off        0 -                      tag-pri
---------------------------------------------------------------------------
Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. The index of the service port is 1, and the VPI and VCI of the service port must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39, and the access port ID is 0/2/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 1 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 1 10
huawei(config)#stacking inner-priority service-port 1 4
```

Step 4 In the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **4.1.2 Configuring SHDSL Profiles**. Add SHDSL line profile 3 of the PTM type, with the maximum line rate 2048 kbit/s.

```
huawei(config)#shdsl line-profile quickadd 3 ptm rate 512 2048
```

2. Activate SHDSL port 0/3/1, and bind the preset SHDSL line profile 3 and the default SHDSL alarm template (alarm template 1) to the port.

NOTE

By default, an SHDSL port is in the activated state. Before binding a profile or template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy          Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                       tag-pri
     1 2496     81872    4992     163744     6 -                       tag-pri
     2 512      18384    1024     36768      0 -                       tag-pri
     3 576      20432    1152     40864      2 -                       tag-pri
     4 64       4048     128      8096       4 -                       tag-pri
     5 2048     67536    4096     135072     0 -                       tag-pri
     6 off      off      off      off        0 -                       tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the SHDSL channel mode to PTM, and create service port 2 on SHDSL port 0/3/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 2 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 2 10
huawei(config)#stacking inner-priority service-port 2 4
```

Step 5 In the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example. For details about how to configure a VDSL profile in the VDSL TI mode, see **Configuring VDSL2 Profiles (TI Mode)**.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Profiles (TR129 Mode)**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2 rate
```

```
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL port 0/4/1, and bind the preset VDSL line template 3 and the default VDSL alarm template (alarm template 1) to the port.

   NOTE

   By default, a VDSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

   According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

   NOTE

   - If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
   - On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the VDSL channel mode to PTM, and create service port 3 on VDSL port 0/4/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-
table
index 5 outbound traffic-table index 5
huawei(config)#service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 3 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 3 10
huawei(config)#stacking inner-priority service-port 3 4
```

Step 6 Configure the user account security.

The PITP P mode can be enabled to protect the user account against theft and roaming. The RAIO mode can be customized according to actual requirements. The encoding format required by China Telecom is considered as an example. The encoding format required by China Telecom is a customized format, corresponding to the **cntel** option.

```
huawei(config)#pitp enable pmode
huawei(config)#raio-mode cntel pitp-pmode
```

NOTE

For details about the PITP configuration for the user account security, see **2.7.1 Configuring Anti-Theft and Roaming of User Account Through PITP**.

Step 7 Save the data.

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

----End

Verification

- Dialing verification on the user side:
  - Step 1: Configure the user name and password for the dialup on the modem (the user name and password must be the same as those configured on the BRAS).
  - Step 2: Dial up on the PC by using the PPPoE dialup software. After the dialup is successful, the user can access the Internet.
  - Step 3: When FTP is used to download files, after the dialup is performed on the PPPoE dialup software, the PPPoE dialup software prompts that the dialup is successful. Then, the PC can access the Internet in the PPPoE mode.
  - Step 4: When downloading files through FTP, you can open **Task Manager** in Windows and click **Networking** to check the link speed. Then, you can calculate the Internet access rate by the following formula: Attainable Internet access rate = Computer network adapter rate/48 x 53 x 8. The calculation result approximates to the planned 2048 kbit/s.
- Remote emulation dialing verification:
  - Step 1: On the MA5600T/MA5603T, run the **pppoe simulate start** command to start the PPPoE emulation dialer (the entered user name, password, and authentication mode must be the same as those configured on the BRAS).
  - Step 2: Run the **display pppoe simulate info** command to query status of PPPoE emulation dialing. If the PPPoE emulation dialing result is success, that is, simulating interaction between the user and the BRAS is successful, the user can access the Internet in the PPPoE access mode.
  - After the emulation verification is completed, run the **pppoe simulate stop** command to stop the PPPoE emulation dialing task initiated by the user.

Configuration File

Configuration File in the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
interface adsl 0/2
deactivate 0
activate 0 profile-index 1
```

```
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
stacking label service-port 1 10
stacking inner-priority service-port 1 4
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File in the SHDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/stacking
stacking label service-port 2 10
stacking inner-priority service-port 2 4
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File in the VDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/stacking
stacking label service-port 3 10
stacking inner-priority service-port 3 4
stacking inner-priority service-port 2 4
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

17.1.2 Example: Configuring the xDSL IPoE Internet Access Service

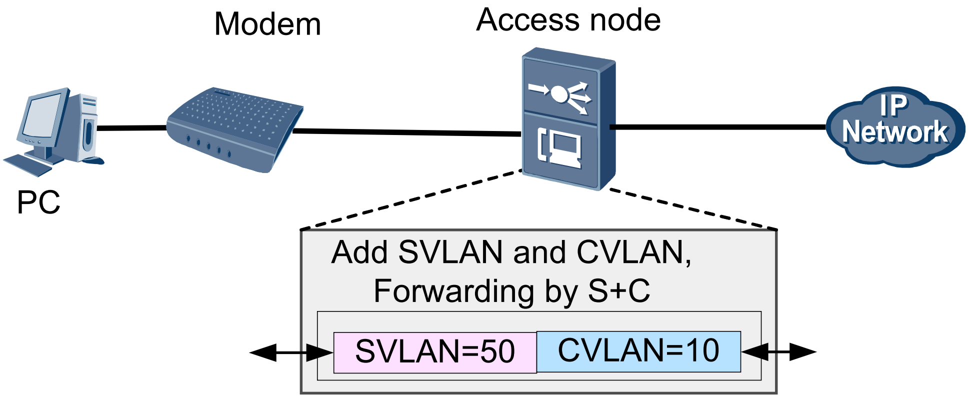
On a fiber to the x (FTTx) network, if the MA5600T/MA5603T provides x digital subscriber line (xDSL) services for broadband users and the users connect to the Internet in IP over Ethernet (IPoE) mode, you can configure the MA5600T/MA5603T by referring to this topic to provide users with high-speed Internet (HIS) services. The MA5600T/MA5603T functions as an optical network unit (ONU) in this service. IPoE is mainly used for private line IP access services. IPoE users are generally authenticated in Dynamic Host Configuration Protocol (DHCP) option 82 mode.

Service Requirements

- The OLT provides services for users in xDSL modes, including the asymmetric digital subscriber line 2 plus (ADSL2+), single-pair high-speed digital subscriber line (SHDSL), and very-high-speed digital subscriber line 2 (VDSL2) mode.
- Private line users connect to the Internet in IPoE mode. To prevent unauthorized access, user accounts are authenticated in DHCP option 82 mode.
- To trace service sources of users and control and manage quality of service (QoS) based on user and service, the Internet service is planned in per user per service per VLAN (PUPSPV) mode. To differentiate users, the MA5600T/MA5603T allocates a virtual local area network (VLAN) for each user. Double VLAN tags are added to user packets for upstream transmission, where the outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by a unique S-VLAN +C-VLAN. This is called the 1:1 access.
- The user access rate is 2048 kbit/s.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 17-2 shows an example network of the xDSL IPoE Internet access service.

Figure 17-2 Example network of the xDSL IPoE Internet access service



Prerequisite

The user PC can obtain an IP address from the DHCP server.

Procedure

Step 1 Configure a VLAN.

Configure S-VLAN 50 with the stacking attribute. The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, and the VLAN forwarding mode is the S-VLAN+C-VLAN mode.

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#vlan forwarding 50 vlan-connect
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

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

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **4.1.1 Configuring an ADSL2+ Template**. The default ADSL2+ line template (line template 1) and the default ADSL2+ alarm template (alarm template 1) are used as an example.
2. Activate the ADSL port, and bind the ADSL2+ templates.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

   In the ADSL access mode, bind the default ADSL2+ line template 1 and ADSL2+ alarm template 1 to ADSL port 0/2/0.

   ```
   huawei(config)#interface adsl 0/2
   huawei(config-if-adsl-0/2)#deactivate 0
   huawei(config-if-adsl-0/2)#activate 0 profile-index 1
   huawei(config-if-adsl-0/2)#alarm-config 0 1
   huawei(config-if-adsl-0/2)#quit
   ```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

   ```
   huawei(config)#display traffic table ip from-index 0
   { <cr>|to-index<K> }:

     Command:
             display traffic table ip from-index 0
     ---------------------------------------------------------------------------
      TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
          (kbps)   (bytes)  (kbps)   (bytes)
     ---------------------------------------------------------------------------
        0 1024     34768    2048     69536      6 -                      tag-pri
        1 2496     81872    4992     163744     6 -                      tag-pri
        2 512      18384    1024     36768      0 -                      tag-pri
        3 576      20432    1152     40864      2 -                      tag-pri
        4 64       4048     128      8096       4 -                      tag-pri
        5 2048     67536    4096     135072     0 -                      tag-pri
        6 off      off      off      off        0 -                      tag-pri
     ---------------------------------------------------------------------------
     Total Num : 7
   ```

   According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. The index of the service port is 1, and the VPI and VCI of the service port must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39, and the access port ID is 0/2/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 1 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 1 10
huawei(config)#stacking inner-priority service-port 1 4
```

Step 4 In the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **4.1.2 Configuring SHDSL Profiles**. Add SHDSL line profile 3 of the PTM type, with the maximum line rate 2048 kbit/s.

```
huawei(config)#shdsl line-profile quickadd 3 ptm rate 512 2048
```

2. Activate SHDSL port 0/3/1, and bind the preset SHDSL line profile 3 and the default SHDSL alarm template (alarm template 1) to the port.

NOTE

By default, an SHDSL port is in the activated state. Before binding a profile or template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the SHDSL channel mode to PTM, and create service port 2 on SHDSL port 0/3/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 2 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 2 10
huawei(config)#stacking inner-priority service-port 2 4
```

Step 5 In the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example. For details about how to configure a VDSL profile in the VDSL TI mode, see **Configuring VDSL2 Profiles (TI Mode)**.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Profiles (TR129 Mode)**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL port 0/4/1, and bind the preset VDSL line template 3 and the default VDSL alarm template (alarm template 1) to the port.

NOTE

By default, a VDSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
        display traffic table ip from-index 0
  ----------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ----------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ----------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the VDSL channel mode to PTM, and create service port 3 on VDSL port 0/4/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-
table
index 5 outbound traffic-table index 5
huawei(config)#service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 3 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 3 10
huawei(config)#stacking inner-priority service-port 3 4
```

Step 6 Configure the security of user accounts.

NOTE

- In this example, the MA5600T/MA5603T works in the Layer 2 DHCP mode. Therefore, the DHCP-related configurations are not required. If the MA5600T/MA5603T works in the Layer 3 DHCP mode, the DHCP-related configurations on the MA5600T/MA5603T are required. For details, see **3.3 Configuring DHCP**.
- For the details about the security of DHCP accounts, see **2.7.2 Configuring Anti-Theft and Roaming of User Accounts Through DHCP**.

Assume that the RAIO mode is the user-defined mode, the CID is the access node name frame/slot/port:vlanid, the RID is the label of the service port where the user is connected. To enable the DHCP option 82 function with these parameters, do as follows:

```
huawei(config)#dhcp option82 enable
huawei(config)#raio-mode user-defined dhcp-option82
huawei(config)#raio-format dhcp-option82 cid anid frame/slot/port:vlanid
huawei(config)#raio-format dhcp-option82 rid splabel
```

Step 7 Save the data.

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

----End

Verification

- Internet access verification on the user side:
  - Step 1: After the PC NIC automatically obtains an IP address and a connection to the Internet is set up, the user can access the Internet.
  - Step 2: To download a file through FTP, open **Windows Task Manager** and then click **Networking** to observe the link rate. Calculate the Internet access rate by the formula: attainable Internet access rate = computer NIC rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.
- DHCP emulation verification:
  - Step 1: On the MA5600T/MA5603T run the **dhcp simulation start** command to start DHCP emulation.
  - Step 2: Run the **display dhcp simulation** command to query the DHCP emulation status.
  - After emulation is verified, run the **dhcp simulation stop** command to stop DHCP emulation.

Configuration File

Configuration File for the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
interface adsl 0/2
deactivate 0
activate 0 template-index 1
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
stacking label service-port 1 10
stacking inner-priority service-port 1 4
dhcp option82 enable
raio-mode user-defined dhcp-option82
raio-format dhcp-option82 cid anid frame/slot/port:vlanid
raio-format dhcp-option82 rid splabel
save
```

Configuration File for the SHDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
```

```
service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/stacking
stacking label service-port 2 10
stacking inner-priority service-port 2 4
dhcp option82 enable
raio-mode user-defined dhcp-option82
raio-format dhcp-option82 cid anid frame/slot/port:vlanid
raio-format dhcp-option82 rid splabel
save
```

Configuration File for the VDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/stacking
stacking label service-port 3 10
stacking inner-priority service-port 3 4
stacking inner-priority service-port 2 4
dhcp option82 enable
raio-mode user-defined dhcp-option82
raio-format dhcp-option82 cid anid frame/slot/port:vlanid
raio-format dhcp-option82 rid splabel
save
```

17.1.3 Example: Configuring the xDSL PPPoA Internet Access Service

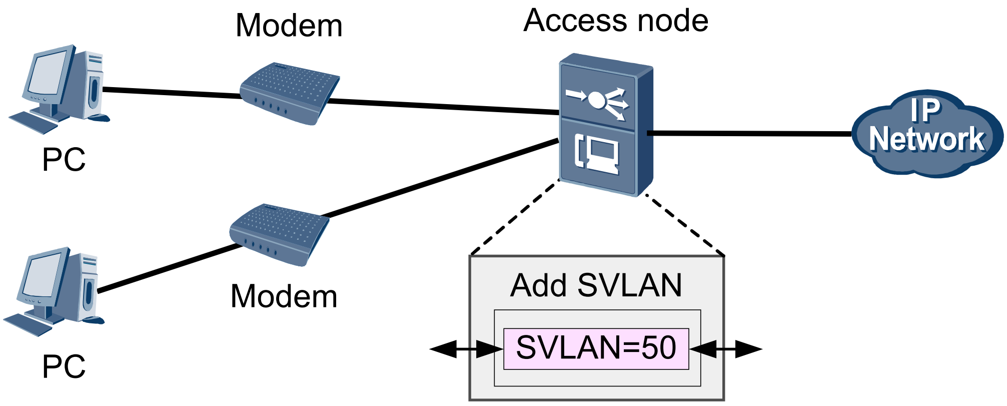
This topic describes how to configure a user so that the user can access the MA5600T/ MA5603T in the xDSL mode, and then access the Internet in the PPPoA mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the PPPoA mode.
- User packets, which carry a single VLAN tag, are transmitted in the upstream direction, and the services of multiple users are converged into one VLAN. This is called the N:1 access.
- PITP is enabled to protect user accounts from theft and roaming.
- A traffic profile is adopted for rate limitation. The user access rate is 2048 kbit/s.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 17-3 shows an example network of the xDSL PPPoA Internet access service.

Figure 17-3 Example network of the xDSL PPPoA Internet access service



Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.11 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Procedure

Step 1 Create a VLAN.

Create smart VLAN 50.

```
huawei(config)#vlan 50 smart
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

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

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the case of the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **4.1.1 Configuring an ADSL2+ Template**. The ID of the ADSL2+ line profile is 3, the downstream rate is 2048 kbit/s, the

channel mode is the interleave mode, the maximum interleave delay is 10 ms, and the SNR margin is 6 dB.

```
huawei(config)#adsl line-profile quickadd 3 snr 60 30 120 60 30 120
huawei(config)#adsl channel-profile quickadd 3 interleaved-delay 10 10 rate
1024
 2048 3096 1024 2048
3096
huawei(config)#adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2
3
```

2. Activate the ADSL port. The port is port 0/2/0, and ADSL line template 3 and the default alarm template (alarm template 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 3
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ----------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ----------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ----------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service port is 1, the access port is port 0/2/0, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description MA5600T/MA5603THW/Vlanid:50/
adsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 1 16
```

Step 4 In the case of the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **4.1.2 Configuring SHDSL Profiles**. The ID of the SHDSL line profile is 3, the line rate is 2048 kbit/s, and the profile is used to activate 4-wire ports.

```
huawei(config)#shdsl line-profile quickadd 3 line four-wire rate 2048
```

2. Activate the SHDSL port. The port is port 0/3/1, and SHDSL line profile 3 and the default alarm profile (alarm profile 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 2, the access port is port 0/3/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound
traffic-table
```

```
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description MA5600T/MA5603THW/Vlanid:50/
shdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 2 16
```

Step 5 In the case of the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example. For how to configure a VDSL profile in the VDSL TI mode, see **Configuring VDSL2 Profiles (TI Mode)**.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Profiles (TR129 Mode)**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode atm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate the VDSL port. The access port is port 0/4/1, and VDSL line template 3 and the default VDSL alarm template (alarm template 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy          Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                       tag-pri
     1 2496     81872    4992     163744     6 -                       tag-pri
     2 512      18384    1024     36768      0 -                       tag-pri
     3 576      20432    1152     40864      2 -                       tag-pri
     4 64       4048     128      8096       4 -                       tag-pri
     5 2048     67536    4096     135072     0 -                       tag-pri
     6 off      off      off      off        0 -                       tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 3, the access port is port 0/4/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5600T/MA5603THW/Vlanid:50/
vdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 3 16
```

Step 6 Configure the PPPoA-PPPoE protocol conversion.

This step is to configure the PPPoA MAC address pool. The start MAC address in the MAC address pool is 0000-1111-1010, and the maximum number of the MAC addresses in the MAC address pool is 300. The PPPoA-PPPoE protocol conversion is enabled and the service encapsulation mode is LLC.

```
huawei(config)#mac-pool xpoa 0000-1111-1010 300
huawei(config)#pppoa enable
huawei(config)#encapsulation 0/2/0 vpi 1 vci 39 type pppoa llc
huawei(config)#encapsulation 0/3/1 vpi 1 vci 39 type pppoa llc
huawei(config)#encapsulation 0/4/1 vpi 1 vci 39 type pppoa llc
```

Step 7 Configure the user account security.

The PITP P mode can be enabled to protect the user account against theft and roaming. The RAIO mode can be customized according to actual requirements. The encoding format required by China Telecom is considered as an example. The encoding format required by China Telecom is a customized format, corresponding to the **cntel** option.

```
huawei(config)#pitp enable pmode
huawei(config)#raio-mode cntel pitp-pmode
```

NOTE

For details about the PITP configuration for the user account security, see **2.7.1 Configuring Anti-Theft and Roaming of User Account Through PITP**.

Step 8 Save the data.

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

----End

Verification

- Step 1: Set the VPI/VCI of the modem to 1/39 and encapsulation mode to **llc-pppoa**. Configure the user name and password used for dialing (the user name and password must be the same as those configured on the BRAS.)

- Step 2: After the settings on the modem are completed, dialing is initialized, a network connection is automatically set up, and the user can access the Internet.
- Step 3: To download a file through FTP, open **Windows Task Manager** and then click **Networking** to observe the link rate. Calculate the Internet access rate by the formula: attainable Internet access rate = computer NIC rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.

Configuration File

Configuration File for the ADSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
adsl line-profile quickadd 3 2 snr 60 30 120 60 30 120
adsl channel-profile quickadd 3 interleaved-delay 10 10 rate 1024 2048 3096 1024
2048 3096
adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2 3
interface adsl 0/2
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description MA5600T/MA5603THW/Vlanid:50/adsl/smart
mac-address max-mac-count service-port 1 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/2/0 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File for the SHDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5600T/MA5603THW/Vlanid:50/shdsl/smart
mac-address max-mac-count service-port 2 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/3/1 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File for the VDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode atm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
```

```
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5600T/MA5603THW/Vlanid:50/vdsl/smart
mac-address max-mac-count service-port 3 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/4/1 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

17.1.4 Example: Configuring the xDSL IPoA Internet Access Service

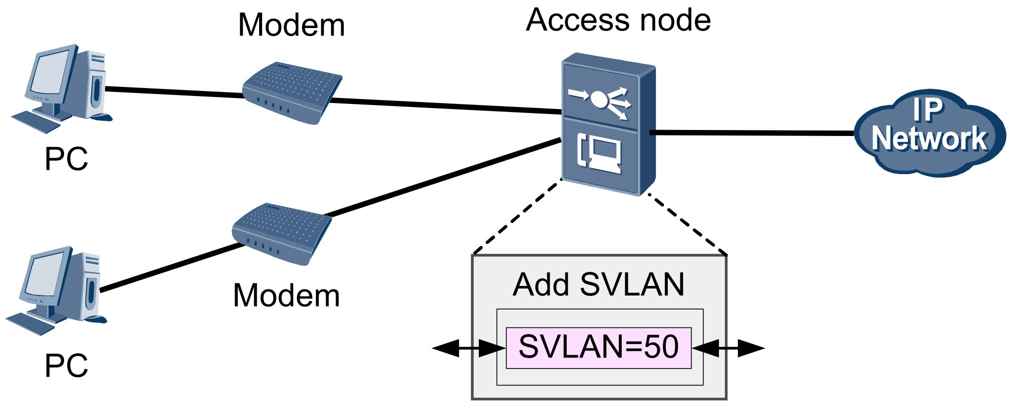
On a fiber to the x (FTTx) network, if the MA5600T/MA5603T provides x digital subscriber line (xDSL) services for broadband users and the users connect to the Internet in IP over ATM (IPoA) mode, you can configure the MA5600T/MA5603T by referring to this topic to provide users with high-speed Internet (HIS) services. The MA5600T/MA5603T functions as an optical network unit in this service. IPoA is generally used on a private line network to meet operators' requirements for transferring from an asynchronous transfer mode (ATM) network to the IP network. An authentication is generally not required for IPoA users.

Service Requirements

- The user accesses the Internet in the IPoA mode.
- To trace service sources of users and control and manage quality of service (QoS) based on user and service, the Internet service is planned in per user per service per VLAN (PUPSPV) mode. To differentiate users, the MA5600T/MA5603T allocates a virtual local area network (VLAN) for each user. On the OLT, use dual VLANs (S-VLAN+C-VLAN) to differentiate users for the Internet access service.
- The user access rate is 2048 kbit/s.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 17-4 shows an example network of the xDSL IPoA Internet access service.

Figure 17-4 Example network of the xDSL IPoA Internet access service



Procedure

Step 1 Create a VLAN.

Create smart VLAN 50.

```
huawei(config)#vlan 50 smart
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

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

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the case of the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **4.1.1 Configuring an ADSL2+ Template**. The ID of the ADSL2+ line profile is 3, the downstream rate is 2048 kbit/s, the channel mode is the interleave mode, the maximum interleave delay is 10 ms, and the SNR margin is 6 dB.

```
huawei(config)#adsl line-profile quickadd 3 snr 60 30 120 60 30 120
huawei(config)#adsl channel-profile quickadd 3 interleaved-delay 10 10 rate 
1024
 2048 3096 1024 2048
3096
huawei(config)#adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2 
3
```

2. Activate the ADSL port. The port is port 0/2/0, and ADSL line template 3 and the default alarm template (alarm template 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 3
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
```

```
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ----------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service port is 1, the access port is port 0/2/0, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description MA5600T/MA5603THW/Vlanid:50/
adsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 1 16
```

Step 4 In the case of the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **4.1.2 Configuring SHDSL Profiles**. The ID of the SHDSL line profile is 3, the line rate is 2048 kbit/s, and the profile is used to activate 4-wire ports.

```
huawei(config)#shdsl line-profile quickadd 3 line four-wire rate 2048
```

2. Activate the SHDSL port. The port is port 0/3/1, and SHDSL line profile 3 and the default alarm profile (alarm profile 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy          Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                       tag-pri
     1 2496     81872    4992     163744     6 -                       tag-pri
     2 512      18384    1024     36768      0 -                       tag-pri
     3 576      20432    1152     40864      2 -                       tag-pri
     4 64       4048     128      8096       4 -                       tag-pri
     5 2048     67536    4096     135072     0 -                       tag-pri
     6 off      off      off      off        0 -                       tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 2, the access port is port 0/3/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound
traffic-table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description MA5600T/MA5603THW/Vlanid:50/
shdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 2 16
```

Step 5 In the case of the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example. For how to configure a VDSL profile in the VDSL TI mode, see **Configuring VDSL2 Profiles (TI Mode)**.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Profiles (TR129 Mode)**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode atm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate the VDSL port. The access port is port 0/4/1, and VDSL line template 3 and the default VDSL alarm template (alarm template 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ----------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ----------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ----------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 3, the access port is port 0/4/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5600T/MA5603THW/Vlanid:50/
vdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 3 16
```

Step 6 Enable the IPoA-IPoE protocol conversion.

This step is to configure the IPoA MAC address pool. The start MAC address in the MAC address pool is 0000-1111-1010, and the maximum number of the MAC addresses in the MAC address pool is 300. The IPoA-IPoE protocol conversion is enabled, the default gateway is the same as the IP address (192.168.1.20) of the upper-layer router, and the service encapsulation mode is LLC-IPoA. The IP address of the modem is 192.168.1.1.

```
huawei(config)#mac-pool xpoa 0000-1111-1010 300
huawei(config)#ipoa enable
huawei(config)#ipoa default gateway 192.168.1.20
huawei(config)#encapsulation 0/2/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
huawei(config)#encapsulation 0/3/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
huawei(config)#encapsulation 0/4/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
```

Step 7 Save the data.

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

----End

Verification

- Step 1: Set the VPI/VCI of the modem to 1/39, encapsulation mode to llc-ipoa, and IP address to 192.168.1.1.
- Step 2: After the settings on the modem are completed, the network connection is automatically set up and the user can access the Internet.
- Step 3: When downloading files through FTP, you can open **Task Manager** in Windows and click **Networking** to check the link rate. Calculate the Internet access rate by the formula: Attainable Internet access rate = Computer NIC rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.

Configuration File

Configuration File of the ADSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
adsl line-profile quickadd 3 2 snr 60 30 120 60 30 120
adsl channel-profile quickadd 3 interleaved-delay 10 10 rate 1024 2048 3096 1024
2048 3096
adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2 3
interface adsl 0/2
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description MA5600T/MA5603THW/Vlanid:50/adsl/smart
mac-address max-mac-count service-port 1 16
mac-pool xpoa 0000-1111-1010 300
ipoa enable
ipoa default gateway 192.168.1.20
encapsulation 0/2/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

Configuration File of the SHDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
```

```
quit
service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5600T/MA5603THW/Vlanid:50/shdsl/smart
mac-address max-mac-count service-port 2 16
mac-pool xpoa 0000-1111-1010 300
ipoa enable
ipoa default gateway 192.168.1.20
encapsulation 0/3/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

Configuration File of the VDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode atm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5600T/MA5603THW/Vlanid:50/vdsl/smart
mac-address max-mac-count service-port 3 16
mac-pool xpoa 0000-1111-1010 300
ipoa enable
ipoa default gateway 192.168.1.20
encapsulation 0/4/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

17.1.5 Example: Configuring the Internet Access Service in the xDSL 802.1X Mode

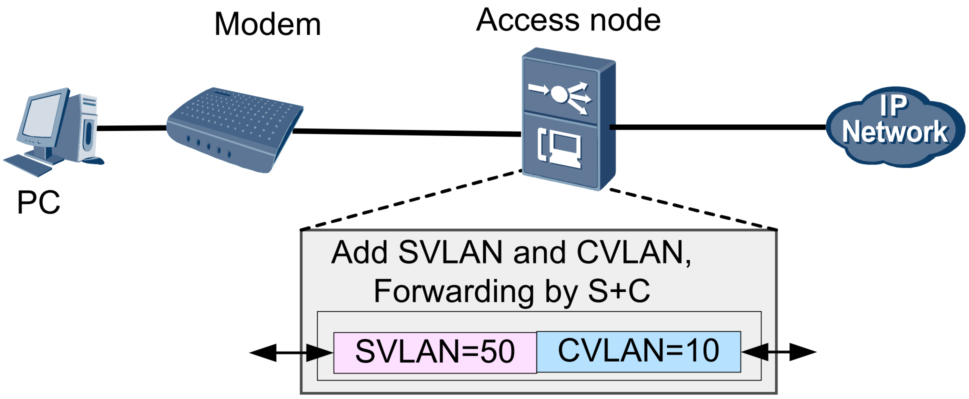
This topic describes how to configure a user to access the MA5600T/MA5603T in the xDSL mode, and then access the Internet in the 802.1X authentication mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the 802.1X authentication mode and is authenticated locally.
- User packets are tagged with two VLAN tags and then transmitted upstream. The outer VLAN tag is used to identify the service. The inner VLAN tag is used to identify the user. The service of each user is identified by S+C, which is a 1:1 access scenario.
- The user access rate is 2048 kbit/s, which is restricted by the traffic profile.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 17-5 shows an example network of the Internet access service in the xDSL 802.1X mode.

Figure 17-5 Example network of the Internet access service in the xDSL IPoE mode



Prerequisite

- The user already installs the client software that supports 802.1X.
- The user name and the password for authentication are already configured properly on the RADIUS server.

Procedure

Step 1 Configure a VLAN.

Configure S-VLAN 50 with the stacking attribute. The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, and the VLAN forwarding mode is the S-VLAN+C-VLAN mode.

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#vlan forwarding 50 vlan-connect
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

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

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **4.1.1 Configuring an ADSL2+ Template**. The default ADSL2+ line template (line template 1) and the default ADSL2+ alarm template (alarm template 1) are used as an example.
2. Activate the ADSL port, and bind the ADSL2+ templates.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

   In the ADSL access mode, bind the default ADSL2+ line template 1 and ADSL2+ alarm template 1 to ADSL port 0/2/0.

   ```
   huawei(config)#interface adsl 0/2
   huawei(config-if-adsl-0/2)#deactivate 0
   huawei(config-if-adsl-0/2)#activate 0 profile-index 1
   huawei(config-if-adsl-0/2)#alarm-config 0 1
   huawei(config-if-adsl-0/2)#quit
   ```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

   ```
   huawei(config)#display traffic table ip from-index 0
   { <cr>|to-index<K> }:

     Command:
             display traffic table ip from-index 0
     ---------------------------------------------------------------------------
      TID CIR       CBS       PIR       PBS       Pri Copy-policy         Pri-Policy
          (kbps)    (bytes)   (kbps)    (bytes)
     ---------------------------------------------------------------------------
        0 1024      34768     2048      69536       6 -                      tag-pri
        1 2496      81872     4992      163744      6 -                      tag-pri
        2 512       18384     1024      36768       0 -                      tag-pri
        3 576       20432     1152      40864       2 -                      tag-pri
        4 64        4048      128       8096        4 -                      tag-pri
        5 2048      67536     4096      135072      0 -                      tag-pri
        6 off       off       off       off         0 -                      tag-pri
     ---------------------------------------------------------------------------
     Total Num : 7
   ```

   According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

   NOTE

   - If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
   - On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. The index of the service port is 1, and the VPI and VCI of the service port must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39, and the access port ID is 0/2/0. To facilitate the maintenance of the service port, also configure the service port description.

   ```
   huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
   table index 5 outbound traffic-table index 5
   huawei(config)#service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/
   stacking
   ```

5. Set the C-VLAN ID of the preset service port 1 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 1 10
huawei(config)#stacking inner-priority service-port 1 4
```

Step 4 In the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **4.1.2 Configuring SHDSL Profiles**. Add SHDSL line profile 3 of the PTM type, with the maximum line rate 2048 kbit/s.

```
huawei(config)#shdsl line-profile quickadd 3 ptm rate 512 2048
```

2. Activate SHDSL port 0/3/1, and bind the preset SHDSL line profile 3 and the default SHDSL alarm template (alarm template 1) to the port.

NOTE

By default, an SHDSL port is in the activated state. Before binding a profile or template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the SHDSL channel mode to PTM, and create service port 2 on SHDSL port 0/3/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-
table
 index 5 outbound traffic-table index 5
```

```
huawei(config)#service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 2 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 2 10
huawei(config)#stacking inner-priority service-port 2 4
```

Step 5 In the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example. For details about how to configure a VDSL profile in the VDSL TI mode, see **Configuring VDSL2 Profiles (TI Mode)**.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Profiles (TR129 Mode)**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL port 0/4/1, and bind the preset VDSL line template 3 and the default VDSL alarm template (alarm template 1) to the port.

NOTE

By default, a VDSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS       Pri Copy-policy          Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536       6 -                       tag-pri
     1 2496     81872    4992     163744      6 -                       tag-pri
     2 512      18384    1024     36768       0 -                       tag-pri
     3 576      20432    1152     40864       2 -                       tag-pri
     4 64       4048     128      8096        4 -                       tag-pri
     5 2048     67536    4096     135072      0 -                       tag-pri
     6 off      off      off      off         0 -                       tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the VDSL channel mode to PTM, and create service port 3 on VDSL port 0/4/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-
table
index 5 outbound traffic-table index 5
huawei(config)#service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 3 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 3 10
huawei(config)#stacking inner-priority service-port 3 4
```

Step 6 Configure the 802.1X authentication.

1. Enable the 802.1X global switch. Enable the 802.1X authentication for ports 1, 2, and 3. The 802.1X needs to be triggered by DHCP. Therefore, the DHCP-trigger authentication must be enabled.

```
huawei(config)#dot1x enable
huawei(config)#dot1x service-port 1
huawei(config)#dot1x service-port 2
huawei(config)#dot1x service-port 3
huawei(config)#dot1x dhcp-trigger enable
```

2. Configure an 802.1X parameters. In the local termination authentication, the 802.1X parameters should be configured to be in the EAP termination mode. The count of allowed handshake failure is 1 and the handshake interval is 20s.

```
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 1
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 2
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 3
huawei(config)#dot1x eap-end service-port 1
huawei(config)#dot1x eap-end service-port 2
huawei(config)#dot1x eap-end service-port 3
```

3. Name the AAA authentication scheme **huawei** and name the AAA accounting scheme **huawei**. During the local authentication, the AAA authentication scheme is a local authentication. Therefore, you do not need to configure the RADIUS server profile; however, you need to configure the accounting mode in the accounting scheme to **none**.

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme huawei
huawei(config-aaa-authen-huawei)#authentication-mode local
huawei(config-aaa-authen-huawei)#quit
huawei(config-aaa)#accounting-scheme huawei
huawei(config-aaa-accounting-huawei)#accounting-mode none
huawei(config-aaa-accounting-huawei)#quit
```

4. Create a local user with the user name **shenzhen** and the password **shenzhen**.

```
huawei(config-aaa)#local-user shenzhen@huawei password shenzhen
```

5. Name the AAA domain **huawei**. Bind the domain with the accounting scheme named **huawei**, authentication scheme named **huawei**.

```
huawei(config-aaa)#domain huawei
huawei(config-aaa-domain-huawei)#authentication-scheme huawei
huawei(config-aaa-domain-huawei)#accounting-scheme huawei
huawei(config-aaa-domain-huawei)#quit
huawei(config-aaa)#quit
```

Step 7 Save the data.

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

----End

Verification

The procedure for triggering the 802.1X client by DHCP in the Windows XP OS is as follows:

- Step 1: Choose **Start** > **Control Panel** > **Network Connections**. Right-click **Local Area Connection** and then choose **Properties**.
- Step 2: In the dialog box that is displayed,
  1. On the **General** tab page, set **Internet Protocol (TCP/IP)** to **Obtain an IP address automatically**.
  2. On the **Authentication** tab page, select **Enable IEEE 802.1x authentication for this network**.
  3. Click **OK**.
- Step 3: Right-click **Local Area Connection** and then choose **Disable**.
- Step 4: Right-click **Local Area Connection** and then choose **Enable**.
- After a while, the **modem2** prompt icon will be displayed in the lower right corner on the PC desktop. Click the icon. In the dialog box that is displayed, enter the user name **shenzhen** and the password **shenzhen**, and then click **OK** to start the actual service authentication. After passing the authentication, you can access the Internet.
- When a file is downloaded through FTP, you can open Windows Task Manager and then click **Networking** to observe the link speed. Calculate the Internet access rate by the formula: Attainable Internet access rate = Computer network adapter rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.

Configuration File

Configuration File of the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
interface adsl 0/2
deactivate 0
activate 0 template-index 1
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
stacking label service-port 1 10
stacking inner-priority service-port 1 4
dot1x enable
dot1x service-port 1
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 1
dot1x eap-end service-port 1
aaa
```

```
authentication-scheme huawei
authentication-mode local
quit
accounting-scheme huawei
accounting-mode none
quit
local-user shenzhen@huawei password shenzhen
domain huawei
authentication-scheme huawei
accounting-scheme huawei
quit
quit
save
```

Configuration File of the SHDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/stacking
stacking label service-port 2 10
stacking inner-priority service-port 2 4
dot1x enable
dot1x service-port 2
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 2
dot1x eap-end service-port 2
aaa
authentication-scheme huawei
authentication-mode local
quit
accounting-scheme huawei
accounting-mode none
quit
local-user shenzhen@huawei password shenzhen
domain huawei
authentication-scheme huawei
accounting-scheme huawei
quit
quit
save
```

Configuration File of the VDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-table index 5 outbound
```

```
traffic-table index 5
service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/stacking
stacking label service-port 3 10
stacking inner-priority service-port 3 4
stacking inner-priority service-port 2 4
dot1x enable
dot1x service-port 3
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 3
dot1x eap-end service-port 3
aaa
authentication-scheme huawei
authentication-mode local
quit
accounting-scheme huawei
accounting-mode none
quit
local-user shenzhen@huawei password shenzhen
domain huawei
authentication-scheme huawei
accounting-scheme huawei
quit
quit
save
```

17.1.6 Configuration Example of Changing ADSL Internet Access Service to VDSL Internet Access Service (for the VDSL2 Board)

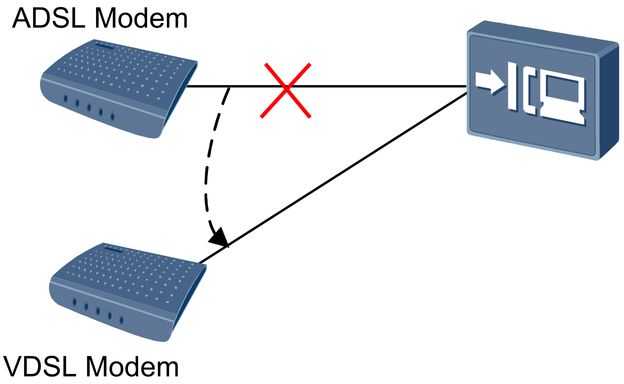
Driven by customer demands for higher bandwidth, the ADSL Internet access service of the VDSL2 board needs to change to the VDSL2 Internet access service. This topic describes how to achieve so.

Service Requirements

- During network restructuring, the ADSL Internet access service of the VDSL2 board needs to change to the VDSL2 Internet access service.
- Users request a higher bandwidth of 8192 kbit/s.
- The VDSL modem is a PTM-mode modem that uses the G993.2 profile 12a.
- Users expect that new requirements are met by modifying certain configurations of the original ADSL service alone. PITP (protecting user accounts from theft), roaming, and upstream link aggregation are configured.

Figure 17-6 shows an example network of the Internet access service through PPPoE dialup.

Figure 17-6 Example network of the Internet access service through PPPoE dialup



Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.11 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Procedure

Step 1 Confirm the line template bound to a port that needs such service modifications, for example, port 0/2/4.

Run the **display port state** command to query the line template bound to the port.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#display port state 4
  ------------------------------------------------------------------------------
  Port     Status          Loopback   Line Template Alarm Template Bonding-group
  ------------------------------------------------------------------------------
   4     Activated          Disable             10              1             -
  ------------------------------------------------------------------------------
```

The query result shows that line template 10 is bound to port 4. Run the **display vdsl line-template** command to query the channel profile and line profile in the line template.

```
huawei(config-if-vdsl-0/2)#display vdsl line-template 10
  ------------------------------------------------------------------------------
  Template index: 10     Name: VDSL LINE TEMPLATE 10
  Line profile index                         : 1
  Channel1 profile index                     : 10
  Channel1 rate adaptation ratio downstream   : 100
  Channel1 rate adaptation ratio upstream     : 100
  ------------------------------------------------------------------------------
```

Step 2 Confirm whether to change the transmission mode and signal noise ratio (SNR).

The query result shows that line profile 1 and channel profile 10 are in line template 10. Run the **display vdsl line-profile** command to query the transmission mode and SNR configured in the line profile.

```
huawei(config-if-vdsl-0/2)#display vdsl line-profile
1
  ------------------------------------------------------------------------------
  Profile index: 1      Name: DEFVAL
  Transmission mode:
    T1.413                           G.992.1(Annex A/B/C)
    G.992.2(Annex A/C)               G.992.3(Annex A/B/I/J/L/M)
    G.992.4(Annex A/I)               G.992.5(Annex A/B/I/J/M)
    G.993.2(Annex A/B/C)
  Bit swap downstream                            : Enable
  Bit swap upstream                              : Enable
  Form of transmit rate adaptation downstream    : AdaptAtStartup
  Form of transmit rate adaptation upstream      : AdaptAtStartup
  Target SNR margin downstream(0.1dB)            : 60
  Minimum SNR margin downstream(0.1dB)           : 0
  Maximum SNR margin downstream(0.1dB)           : 300
  Target SNR margin upstream(0.1dB)              : 60
  Minimum SNR margin upstream(0.1dB)             : 0
  Maximum SNR margin upstream(0.1dB)             : 300
  UPBO US1 band reference PSD parameters[a, b]   : 1650,1020
  UPBO US2 band reference PSD parameters[a, b]     : 1650,615
  UPBO US3 band reference PSD parameters[a, b]     : 0,0
  UPBO US4 band reference PSD parameters[a, b]     : 0,0
---- More ( Press 'Q' to break ) ----
```

- If the transmission mode is ADSL, change the transmission mode to VDSL or ALL. To do so, proceed to **Step 3**.
- If the SNR value does not meet actual requirements over the live network, change it according to actual conditions. To do so, proceed to **Step 3**.
- If the transmission mode is VDSL or ALL and the SNR value also meets actual conditions over the live network, go to **Step 4**.

Step 3 Run the **vdsl line-profile quickadd** command to reconfigure the transmission mode and SNR. In addition, configure exclusive VDSL parameters.

1. According to actual conditions over the live network, SNR is planned to 7 dB, transmission mode to all (its value is 1), and line profile index to 11.

```
huawei(config-if-vdsl-0/2)#vdsl line-profile quickadd 11 transmode 1 snr 70 0
300 70 0 300
```

2. All parameters following **vdsl-parameter** are VDSL parameters in contrast to ADSL. These parameters do not need to be configured in the case of the ADSL Internet access service. However, in the case of the VDSL Internet access service, these parameters need to be configured according to actual conditions. The default G993.2 profile is profile 12a, which is consistent with the required profile in this example. Hence, no modification is required.

Step 4 Run the **display vdsl channel-profile** command to query the data path mode and line rate in the channel profile.

```
huawei(config-if-vdsl-0/2)#display vdsl channel-profile
10
  -----------------------------------------------------------------------------
  Profile index: 10      Name: VDSL CHANNEL PROFILE 10
  Data path mode                                    : ATM
  Minimum impulse noise protection downstream      : NoProtection
  Minimum impulse noise protection upstream        : NoProtection
  Maximum interleaving delay downstream(ms)        : 20
  Maximum interleaving delay upstream(ms)          : 20
  Minimum transmit rate downstream(Kbps)           : 32
  Minimum reserved transmit rate downstream(Kbps)  : 32
  Maximum transmit rate downstream(Kbps)           : 200000
  Minimum transmit rate upstream(Kbps)             : 32
  Minimum reserved transmit rate upstream(Kbps)    : 32
  Maximum transmit rate upstream(Kbps)             : 200000
---- More ( Press 'Q' to break ) ----
```

- If the data path mode is ATM, change it to both. To do so, proceed to **Step 5**.

  NOTE

  The ADSL data path supports only ATM, whereas the VDSL data path supports both ATM and PTM. It is recommended that you change the data path mode to both. In this way, the system automatically selects a proper data path mode according to actual conditions.

- If the line rate does not meet the requirements of users, change it. To do so, proceed to **Step 5**.
- If the data path mode is both and the line rate does not need to be changed, proceed to **Step 6**.

Step 5 Run the **vdsl channel-profile quickadd** command to reconfigure the data path mode and line rate.

To meet customer demands, increase bandwidth to 8192 kbit/s, set the data path mode to both and add a new channel profile (channel profile 11).

```
huawei(config-if-vdsl-0/2)#vdsl channel-profile quickadd 11 path-mode both rat
e 32 81920 32 2048
```

Step 6 Bind the required VDSL2 line template 11 to port 0/2/4.

NOTE

By default, a port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config-if-vdsl-0/2)#vdsl line-template quickadd 11 line 11 channel1 11 100
100
huawei(config-if-vdsl-0/2)#deactivate 4
huawei(config-if-vdsl-0/2)#activate 4 template-index 11
huawei(config-if-vdsl-0/2)#quit
```

Step 7 Add a traffic profile.

1. Run the **display traffic table ip** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ---------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                      tag-pri
     1 2496     81872    4992     163744     6 -                      tag-pri
     2 512      18384    1024     36768      0 -                      tag-pri
     3 576      20432    1152     40864      2 -                      tag-pri
     4 64       4048     128      8096       4 -                      tag-pri
     5 2048     67536    4096     135072     0 -                      tag-pri
     6 off      off      off      off        0 -                      tag-pri
  ---------------------------------------------------------------------------
  Total Num : 7
```

According to customer requirements, the user access rate is 8192 kbit/s. The query result shows that no traffic profile meets customer requirements. Therefore, run the **traffic table ip** command to configure a new traffic profile (traffic profile 7) and set the rate to 8192 kbit/s in the new traffic profile.

NOTE

You can configure the traffic profile or the VDSL2 line profile on the MA5600T/MA5603T to limit the user access rate. When both profiles are configured, the bandwidth of the user is the minimum value of the two profiles. In this example, the traffic profile is used to limit the user access rate.

```
huawei(config)#traffic table ip index 7 cir 8192 priority 6 priority-policy
local-Setting
```

Step 8 Configure a service port.

Run the **display service-port** command to query the original service port.

```
huawei(config)#display service-port port 0/2/4
{ <cr>|autosense<K>|ont<K>|sort-by<K> }:

  Command:
          display service-port port 0/2/4
  Switch-Oriented Flow List
  -----------------------------------------------------------------------------
  INDEX VLAN VLAN      PORT F/ S/  P VPI  VCI   FLOW  FLOW       RX   TX   STATE
        ID   ATTR      TYPE                     TYPE  PARA
  -----------------------------------------------------------------------------
      5  101 common    vdl  0/2/4  0    35    vlan  untag       6    6    up
  -----------------------------------------------------------------------------
   Total : 1  (Up/Down :    1/0)
```

The query result shows that VPI and VCI are configured, which indicate that VDSL is in the ATM mode. In this example, however, the VDSL is in the PTM mode. Run the **service-port** command to create a service port, adopt traffic profile 7, and set the S-VLAN ID to 101. Set the index of the service port to 3 (the index must be different from the original index) and the access port to 0/2/4. To facilitate maintenance of the service port, configure the service port description.

NOTE

Generally, the ADSL is in the ATM mode and the VDSL is in the PTM mode. If an ATM service port only is configured, a PTM service port needs to be added.

```
huawei(config)#service-port 3 vlan 101 vdsl mode ptm 0/2/4 rx-cttr 7 tx-cttr 7
huawei(config)#service-port desc 3 description Vlanid:101/vdsl/ptm
```

Step 9 Save the data.

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

----End

Verification

- Step 1: Configure the user name and password for the dialup on the modem (the user name and password must be the same as those configured on the BRAS).
- Step 2: Dial up on the PC by using the PPPoE dialup software. After the dialup is successful, the user can access the Internet.
- Step 3: When FTP is used to download files and after the dialup is performed on the PPPoE dialup software, the PPPoE dialup software prompts that the dialup is successful. Then, the PC can access the Internet in the PPPoE mode.
- Step 4: When downloading files through FTP, you can open Task Manager in Windows and click Networking to check the link speed. Then, you can calculate the Internet access rate by the following formula: Attainable Internet access rate = Computer network adapter rate/48 x 53 x 8. The calculated result approximates to the planned 8192 kbit/s.

17.1.7 Configuration Example of the VDSL2 Internet Access Services on a Vectoring-Enabled MA5603T

On a fiber to the building (FTTB) or fiber to the curb (FTTC) network, an MA5603T has the vectoring function enabled and provides the Point-to-Point Protocol over Ethernet (PPPoE) Internet access service for very-high-speed digital subscriber line 2 (VDSL2) users. This topic describes how to configure VDSL2 Internet access service on such an MA5603T.

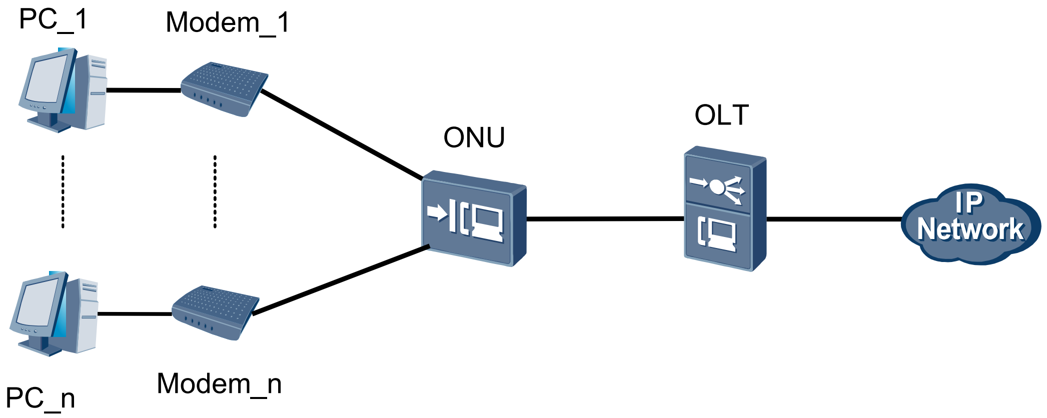
Service Requirements

- In a new VDSL2 vectoring office, all VDSL2 lines connected to the MA5603T are physically bundled together, and all users connect to the Internet in PPPoE mode.
- A customer premises equipment (CPE) that supports the vectoring function and a CPE that does not support the vectoring function are connected to the MA5603T. (A CPE that does not support the vectoring function is called a vectoring legacy CPE.)
- Different virtual local area networks (VLANs) are used to differentiate access users.
- The user access rates are not limited to prevent the vectoring performance from being affected.
- The vectoring function takes effect in upstream and downstream directions of the VDSL2 lines to cancel the far-end crosstalk (FEXT).
- User accounts must be protected against theft and roaming.

- The VDSL2 mode is set to TR129 and aVDSL2 profile in the common mode is used on the MA5603T.

Figure 17-7 shows a VDSL2 Internet access service network that uses a vectoring-enabled MA5603T.

Figure 17-7 VDSL2 Internet access service network that uses a vectoring-enabled MA5603T



Prerequisite

The user name and password must be configured on the broadband remote access server (BRAS) for the BRAS to implement the Authentication, Authorization and Accounting (AAA) function. To implement AAA, the BRAS needs to identify the VLAN tags carried in the user packets forwarded by the MA5603T upstream.

Procedure

Step 1 Create a service VLAN (SVLAN) and add an uplink port to the SVLAN.

Create Smart SVLAN 50 and add uplink port 0/19/0 to SVLAN 50.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
```

Step 2 Configure a VDSL2 access mode.

1. Configure a VDSL2 profile. For details, see **Configuring the VDSL2 Profile (TR129 Mode)**. For how to configure a VDSL2 profile in VDSL2 TI mode, see **Configuring the VDSL2 Profile (TI Mode)**. Set the IDs of the VDSL2 line profile, VDSL2 channel profile, and VDSL2 line template to 3, channel mode to interleave, maximum downstream interleave delay to 8 ms, maximum upstream interleave delay to 2 ms, noise margin to 6 dB, minimum downstream impulse noise protection (INP) to 4, and minimum upstream INP to 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL2 port 0/4/1, and bind the configured VDSL2 line template 3 and the default VDSL2 alarm template 1 to this port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the configured traffic profile in the system.

```
huawei(config)#<b>display traffic table ip from-index 0  </
b>
{ <cr>|to-
index<K> }:


Command:
          display traffic table ip from-index
0

---------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-
Policy
       (kbps)   (bytes)  (kbps)
(bytes)

---------------------------------------------------------------------------
     0 512      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
```

The Internet access service requires that the user access rates not be limited. The query result shows that traffic profile 6 meets the requirements.

NOTE

- If an expected traffic profile is not available in the system, run the **traffic table** command to configure one.
- On the MA5603T, the user access rate can be limited by either a traffic profile or a VDSL2 line profile. When both profiles are configured, the smaller rate configured in the two profiles is used as the user bandwidth.

4. Run the **service-port** command to create a service port on user port 0/4/1. The traffic profile is profile 2 that meets the service requirements, SVLAN is 50, VDSL2 channel mode is PTM, and service port index is 3. To facilitate maintenance, the service port description information is also configured.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 multi-service user-
vl
an untagged inbound traffic-table index 6 outbound traffic-table index 6
huawei(config)#service-port desc 3 description Vlanid:50/vdsl
```

Step 3 Configure a security mode for the user account.

The Policy Information Transfer Protocol (PITP) P mode can be used to protect user accounts against theft and roaming. The relay agent info option (RAIO) mode can be customized based on site requirements. This procedure uses the common mode as an example.

```
huawei(config)#<b>pitp enable pmode</b>
huawei(config)#<b>raio-mode common pitp-pmode</b>
```

NOTE

For details about the PITP configuration for user account security, see **Configuring Anti-Theft and Roaming of User Account Through PITP**.

Step 4 Configure the VDSL2 vectoring function.

1. Set the global bandplan to default values (998ade for bandplan type and type-a for US0 type).
2. Use the default vectoring group (group 1) to cancel the crosstalk on all frequency bands.

```
huawei(config)#display xdsl vectoring-group 1

------------------------------------------------------------------------------
  Vectoring group index     :
1
  Lines in a vectoring
group:
    0/2
  FEXT cancellation not required frequency bands downstream:
-
  FEXT cancellation not required frequency bands upstream   :
-

------------------------------------------------------------------------------
```

3. Run the **display xdsl vectoring-profile** command to query the default vectoring profile (profile 1).

```
huawei(config)#display xdsl vectoring-profile 1

------------------------------------------------------------------------------
  Profile index   :
1
  Profile name    :
DEFVAL
  FEXT cancellation control upstream        :
Enable
  FEXT cancellation control downstream      :
Enable

------------------------------------------------------------------------------
```

The query result shows that vectoring profile 1 meets the requirements and can be used.

4. Configure the vectoring legacy CPE activation policy to auto in consideration that the vectoring function is currently in the beginning phase of applications.

```
huawei(config)#xdsl vectoring legacy-cpe activate-policy auto
```

5. Enable the global vectoring function.

```
huawei(config)#xdsl vectoring enable
```

Step 5 Save the data.

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

----End

Verification

- Setp 1: Configure the dialup user name and password on the modem. Ensure that the configurations be the same as the user name and password configured on the BRAS.
- Step 2: After the settings on the modem are completed, dialing is initialized, a network connection is automatically set up, and the user can access the Internet.

- Step 3: Log in to a network rate test website to test the rate. It is found that the upstream and downstream rates are 95% higher than the rates when the vectoring function is not enabled on the device.

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2
vdsl line-template quickadd 3 line 3 channel1 3 100 100
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 multi-service user-vlan untagged inbound
traffic-table index 6 outbound traffic-table index 6
service-port desc 3 description Vlanid:50/vdsl
pitp enable pmode
raio-mode common pitp-pmode
display xdsl vectoring-group 1
display xdsl vectoring-profile 1
xdsl vectoring legacy-cpe activate-policy auto
xdsl vectoring enable
save
```

17.2 Example: Configuring the xDSL Multicast Service

This topic describes how to configure the multicast video service.

17.2.1 Configuration Example of the Multicast Video Service (Static Program Configuration)

Static program configuration for multicast services is fine-grained program configuration and management, with functions of program/user multicast bandwidth management, program preview, and program prejoin. This configuration mode applies to multicast services that have strict requirements on program and user management.

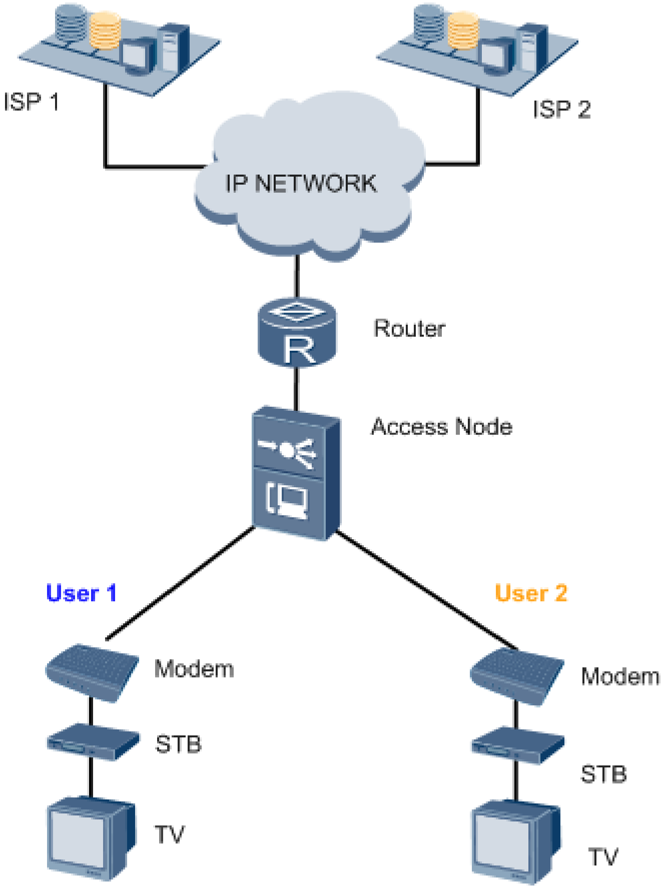
Service Requirements

- ISP 1 has two popular music programs, and ISP 2 has one popular music program and one popular video program. These programs can be ordered continuously and in time.
- The program ordering status can be recorded, collected, and reported for monitoring and charging.
- User 1 has purchased only the music program package from ISP 1, while user 2 has purchased only the video program package from ISP 2. Rights management is required for the two users.
- The package purchased by user 1 limits the maximum available multicast bandwidth to 10 Mbit/s, and the package purchased by user 2 limits the maximum available multicast bandwidth to 5 Mbit/s. Bandwidth restriction is required for the two users.

Figure 17-8 shows an example network of the multicast service.

User 1 and user 2 are connected to the MA5600T/MA5603T in VDSL IPoE mode.

Figure 17-8 **Example network of the multicast service**



Data Plan

Table 17-1 lists the data plan for configuring the multicast video service with static program configuration.

Table 17-1 Data plan for configuring the multicast video service with static program configuration

Item	Data
Multicast VLAN	Multicast domain of ISP 1: VLAN 10 Multicast domain of ISP 2: VLAN 20 **NOTE** It is recommended that different multicast VLANs be planned for different ISPs.
Multicast upstream port	0/19/0
Multicast mode	IGMP proxy
Multicast protocol	IGMPv3

Item	Data
Multicast program	ISP 1 ● Program source address: 10.10.10.10 ● program1: 224.1.1.1 ● program2: 224.1.1.2 ● Maximum program bandwidth: 3500 kbit/s ● Program log reporting: enabled ISP 2 ● Program source address: 10.10.10.11 ● program3: 224.1.1.3 ● program4: 224.1.1.4 ● Maximum program bandwidth: 5000 kbit/s ● Program log reporting: enabled
Right profile	Music program ● Profile name: music ● Program right: watch Video program ● Profile name: movie ● Program right: watch
VDSL port attribute	Working mode: PTM Bound line profile and alarm profile: default profiles (profile ID: 1) Port connected to user 1: 0/2/1 Port connected to user 2: 0/4/1
Multicast user	User 1: ● Name of the bound right profile: music ● Maximum multicast bandwidth: 10 Mbit/s ● Multicast user log recording: enabled User 2: ● Name of the bound right profile: movie ● Maximum multicast bandwidth: 5 Mbit/s ● Multicast user log recording: enabled

Procedure

Step 1 Configure multicast VLANs and programs.

Configure smart VLAN 10 as the multicast domain of ISP 1, and smart VLAN 20 as the multicast domain of ISP 2.

1. Configure the protocol, multicast upstream port, and program list of multicast VLAN 10.

Set the multicast VLAN to VLAN 10, multicast mode to IGMP proxy, multicast protocol to IGMPv3 (system default), multicast upstream port to port 0/19/0, statically configured programs to 224.1.1.1 and 224.1.1.2, program source address to 10.10.10.10, and program bandwidth to 3500 kbit/s, and enable program log reporting.

```
huawei(config)#vlan 10 smart
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp mode proxy
huawei(config-mvlan10)#igmp uplink-port 0/19/0
huawei(config-mvlan10)#igmp program add name program1 ip 224.1.1.1 sourceip
10.10.10.10
 bandwidth 3500 log enable
huawei(config-mvlan10)#igmp program add name program2 ip 224.1.1.2 sourceip
10.10.10.10
 bandwidth 3500 log enable
huawei(config-mvlan10)#quit
```

2. Configure the multicast protocol, multicast upstream port, and program list of multicast VLAN 20.

   Set the multicast VLAN to VLAN 20, multicast mode to IGMP proxy, multicast protocol to IGMPv3 (system default), multicast upstream port to port 0/19/0, statically configured programs to 224.1.1.3 and 224.1.1.4, program source address to 10.10.10.11, and program bandwidth to 5000 kbit/s, and enable program log reporting.

```
huawei(config)#vlan 20 smart
huawei(config)#multicast-vlan 20
huawei(config-mvlan20)#igmp mode proxy
huawei(config-mvlan20)#igmp uplink-port 0/19/0
huawei(config-mvlan20)#igmp program add name program3 ip 224.1.1.3 sourceip
10.10.10.11
 bandwidth 5000 log enable
huawei(config-mvlan20)#igmp program add name program4 ip 224.1.1.4 sourceip
10.10.10.11
 bandwidth 5000 log enable
```

Step 2 Configure right profiles named **music** and **movie** with the watch right, and bind the right profiles to the programs.

```
huawei(config-mvlan20)#btv
huawei(config-btv)#igmp profile add profile-name music
huawei(config-btv)#igmp profile profile-name music program-name program1 watch
huawei(config-btv)#igmp profile profile-name music program-name program2 watch
huawei(config-btv)#igmp profile profile-name music program-name program3 watch
huawei(config-btv)# igmp profile add profile-name movie
huawei(config-btv)#igmp profile profile-name movie program-name program4 watch
huawei(config-btv)#quit
```

Step 3 Activate the VDSL ports, and bind the ports to the line profile and alarm profile.

Bind VDSL port 0/2/1 and VDSL port 0/4/1 to the default line profile (line profile 1) and the default alarm profile (alarm profile 1).

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#deactivate 1
huawei(config-if-vdsl-0/2)#activate 1 template-index 1
huawei(config-if-vdsl-0/2)#alarm-config 1 1
huawei(config-if-vdsl-0/2)#quit
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 1
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

Step 4 Configure multicast users.

1. Create the service channels of the multicast users.

   Create service port 100 on VDSL port 0/2/1, and service port 101 on VDSL port 0/4/1.

```
huawei(config)#port vlan 10 0/19 0
huawei(config)#port vlan 20 0/19 0
huawei(config)#service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr
2
huawei(config)#service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr
2
```

2. Configure the attributes of the multicast users.

   Configure multicast user 0/2/1 as the authentication type, with log reporting enabled, and with the maximum bandwidth 10 Mbit/s. Configure multicast user 0/4/1 as the authentication type, with log reporting enabled, and with the maximum bandwidth 5 Mbit/s.

```
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 100 auth log enable max-
bandwidth 10240
huawei(config-btv)#igmp user add service-port 101 auth log enable max-
bandwidth 5120
```

3. Bind the multicast users to the right profiles.

   Bind VDSL user 0/2/1 to right profile **music**, and VDSL user 0/4/1 to right profile **movie**.

```
huawei(config-btv)#igmp user bind-profile service-port 100 profile-name music
huawei(config-btv)#igmp user bind-profile service-port 101 profile-name movie
```

4. Add the VDSL users to the multicast VLANs so that the VDSL users are multicast members.

```
huawei(config-btv)#multicast-vlan 10
huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
huawei(config-mvlan10)#multicast-vlan 20
huawei(config-mvlan20)#igmp multicast-vlan member service-port 101
huawei(config-mvlan20)#quit
```

Step 5 Save the configuration.

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

----End

Result

- VDSL user 0/1/0 can watch the programs with IP addresses 224.1.1.1 and 224.1.1.2 that are provided by ISP 1, but VDSL user 0/1/0 cannot watch the program with IP address 224.1.1.3.
- VDSL user 0/2/0 can watch the program with IP address 224.1.1.4 that is provided by ISP 2.

Configuration File

```
vlan 10 smart
multicast-vlan 10
igmp mode proxy
igmp uplink-port 0/19/0
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
 bandwidth 3500 log enable
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.10
 bandwidth 3500 log enable
quit
vlan 20 smart
igmp mode proxy
igmp uplink-port 0/19/0
igmp program add name program3 ip 224.1.1.3 sourceip 10.10.10.11
 bandwidth 5000 log enable
```

```
igmp program add name program4 ip 224.1.1.4 sourceip 10.10.10.11
 bandwidth 5000 log enable
btv
igmp profile add profile-name music
igmp profile profile-name music program-name program1 watch
igmp profile profile-name music program-name program2 watch
igmp profile profile-name music program-name program3 watch
igmp profile add profile-name movie
igmp profile profile-name movie program-name program4 watch
quit
interface vdsl 0/2
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
interface vdsl 0/4
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
port vlan 10 0/19 0
port vlan 20 0/19 0
service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr 2
service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr 2
btv
igmp user add service-port 100 auth log enable max-bandwidth 10240
igmp user add service-port 101 auth log enable max-bandwidth 5120
igmp user bind-profile service-port 100 profile-name music
igmp user bind-profile service-port 101 profile-name movie
multicast-vlan 10
igmp multicast-vlan member service-port 100
multicast-vlan 20
igmp multicast-vlan member service-port 101
quit
save
```

17.2.2 Configuration Example of the Multicast Video Service (Dynamic Program Generation)

Dynamic program generation simplifies multicast service configuration and reduces maintenance cost, but does not support functions of program/user multicast bandwidth management, program preview, and program prejoin. This configuration mode applies to multicast services that do not have strict requirements on program and user management or to those having programs and users managed on the upper-layer device.

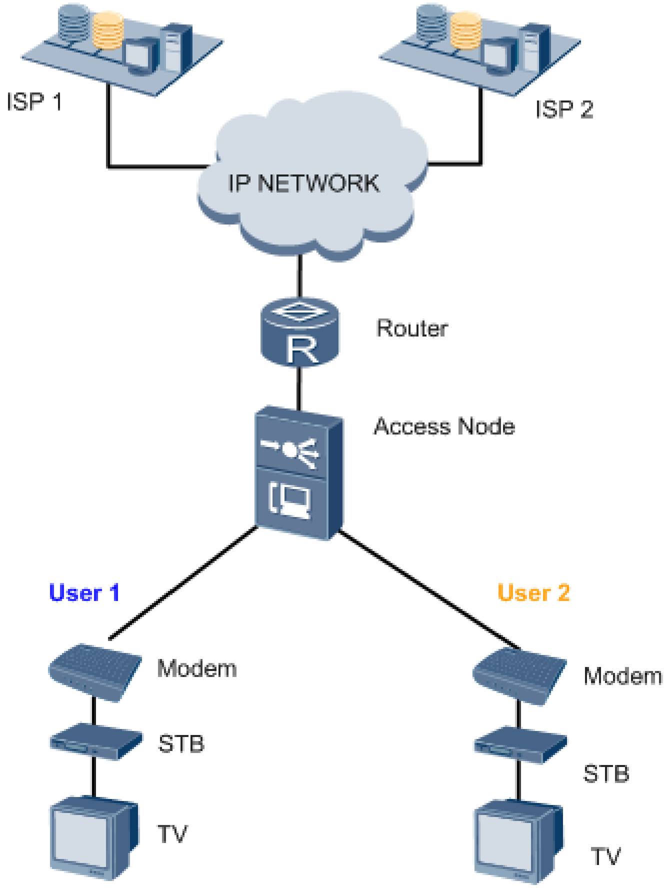
Service Requirements

- ISP 1 and ISP 2 each have an address segment corresponding to multicast programs, which do not require strict management and are dynamically updated according to the ordering situation.
- The service package purchased by user 1 allows user 1 to watch programs of ISP 1 only. The service package purchased by user 2 allows user 2 to watch programs of ISP 2 only.
- The ordering information about users can be recorded for monitoring and charging.

Figure 17-9 shows an example network of the multicast service.

User 1 and user 2 are connected to the MA5600T/MA5603T in VDSL IPoE mode.

Figure 17-9 Example network of the multicast service



Data Plan

Table 17-2 lists the data plan for configuring the multicast video service with dynamic program generation.

Table 17-2 Data plan for configuring the multicast video service with dynamic program generation

Item	Data
Multicast VLAN	Multicast domain of ISP 1: VLAN 10 Multicast domain of ISP 2: VLAN 20 **NOTE** It is recommended that different multicast VLANs be planned for different ISPs.
Multicast upstream port	0/19/0
Multicast mode	IGMP proxy
Multicast protocol	IGMPv3

Item	Data
Multicast program	Dynamic generation Program address range of ISP 1: 224.1.1.1-224.1.1.2 Program address range of ISP 2: 224.1.1.3-224.1.1.4
VDSL port attribute	Working mode: PTM Bound line profile and alarm profile: default profiles (profile ID: 1) Port connected to user 1: 0/2/1 Port connected to user 2: 0/4/1
Multicast user	Multicast user log recording: enabled

Procedure

Step 1 Configure multicast VLANs and programs.

Configure smart VLAN 10 as the multicast domain of ISP 1, and smart VLAN 20 as the multicast domain of ISP 2.

1. Configure the protocol, multicast upstream port, and program list of multicast VLAN 10.

   Configure multicast VLAN 10 with the dynamic program generation mode, and specify the range of the IP addresses of the programs that can be requested by the users in multicast VLAN 10 as 224.1.1.1 to 224.1.1.2. Multicast VLAN 10 adopts IGMP proxy, IGMP v3 (system default value), and multicast upstream port 0/19/0.

   ⚠ **CAUTION**

   The multicast program configuration mode can be changed only when **igmp match mode** is set to **off**. However, setting **igmp match mode** to **off** will cause users to go offline. Therefore, it is recommended that the program configuration mode be planned beforehand.

```
huawei(config)#vlan 10 smart
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp match mode disable
huawei(config-mvlan10)#igmp match group ip 224.1.1.1 to-ip 224.1.1.2
huawei(config-mvlan10)#igmp uplink-port 0/19/0
huawei(config-mvlan10)#igmp mode proxy
huawei(config-mvlan10)#quit
```

2. Configure the protocol, multicast upstream port, and program list of multicast VLAN 20.

   Configure multicast VLAN 20 with the dynamic program generation mode, and specify the range of the IP addresses of the programs that can be requested by the users in multicast VLAN 10 as 224.1.1.3 to 224.1.1.4. Multicast VLAN 20 adopts IGMP proxy, IGMP v3 (system default value), and multicast upstream port 0/19/0.

```
huawei(config)#vlan 20 smart
huawei(config)#multicast-vlan 20
huawei(config-mvlan20)#igmp match mode disable
huawei(config-mvlan20)#igmp match group ip 224.1.1.3 to-ip 224.1.1.4
huawei(config-mvlan20)#igmp uplink-port 0/19/0
huawei(config-mvlan20)#igmp mode proxy
huawei(config-mvlan20)#quit
```

Step 2 Activate the VDSL ports, and bind the ports to the line profile and alarm profile.

Bind VDSL port 0/2/1 and VDSL port 0/4/1 to the default line profile (line profile 1) and the default alarm profile (alarm profile 1).

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#deactivate 1
huawei(config-if-vdsl-0/2)#activate 1 template-index 1
huawei(config-if-vdsl-0/2)#alarm-config 1 1
huawei(config-if-vdsl-0/2)#quit
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 1
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

Step 3 Configure multicast users.

1. Create the service channels of the multicast users.

   Create service port 100 on VDSL port 0/2/1, and service port 101 on VDSL port 0/4/1.

```
huawei(config)#port vlan 10 0/19 0
huawei(config)#port vlan 20 0/19 0
huawei(config)#service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr
2
huawei(config)#service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr
2
```

2. Configure the attributes of the multicast users.

   Enable the log reporting for multicast users 0/2/1 and 0/4/1. The authentication status and multicast bandwidth of the multicast users do not need to be configured.

```
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 100 log enable
huawei(config-btv)#igmp user add service-port 101 log enable
huawei(config-btv)#quit
```

3. Add the VDSL users to the multicast VLANs so that the VDSL users are multicast members.

```
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
huawei(config-mvlan10)#quit
huawei(config-btv)#multicast-vlan 20
huawei(config-mvlan20)#igmp multicast-vlan member service-port 101
huawei(config-mvlan20)#quit
```

Step 4 Save the configuration.

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

----End

Result

- VDSL user 0/2/1 can watch the programs with IP addresses 224.1.1.1 and 224.1.1.2 that are provided by ISP 1.
- VDSL user 0/4/1 can watch the programs with IP addresses 224.1.1.3 and 224.1.1.4 that are provided by ISP 2.

Configuration File

```
vlan 10 smart
multicast-vlan 10
```

```
igmp match mode disable
igmp match group ip 224.1.1.1 to-ip 224.1.1.2
igmp uplink-port 0/19/0
igmp mode proxy
quit
vlan 20 smart
igmp match mode disable
igmp match group ip 224.1.1.3 to-ip 224.1.1.4
igmp uplink-port 0/19/0
igmp mode proxy
quit
interface vdsl 0/2
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
interface vdsl 0/4
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
port vlan 10 0/19 0
port vlan 20 0/19 0
service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr 2
service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr 2
btv
igmp user add service-port 100 auth log enable
igmp user add service-port 101 auth log enable
multicast-vlan 10
igmp multicast-vlan member service-port 100
multicast-vlan 20
igmp multicast-vlan member service-port 101
quit
save
```

17.3 Example: Configuring the VoIP Service

This topic describes how to configure the H.248-based, MGCP-based, and SIP-based VoIP services respectively.

17.3.1 Example: Configuring the VoIP Service (H.248-based)

This topic describes an example for configuring the H.248-based VoIP service.

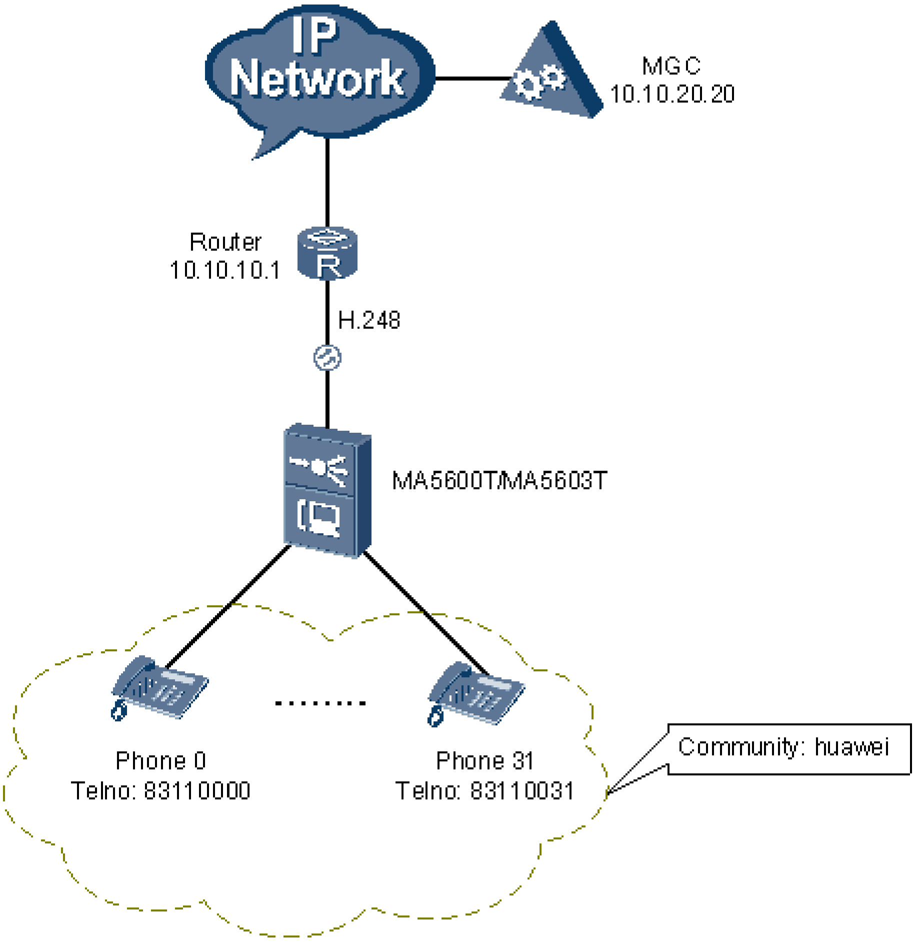
Service Requirements

In an office located in China, the MA5600T/MA5603T that adopts the H.248 protocol is newly deployed. Data plan and configuration, however, are not performed on the MGC (softswitch) connected to the MA5600T/MA5603T. The MA5600T/MA5603T is required to provide the following VoIP services:

- The common phone services are provisioned to 32 users (phones 0-31).
- The polarity-reversal accounting is adopted.

Figure 17-10 shows an example network for configuring the H.248-based VoIP service.

Figure 17-10 Example network for configuring the H.248-based VoIP service



Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T to the MGC must be configured to ensure that the MA5600T/MA5603T and the MGC are reachable from each other.
- Electronic switch 0 must be in **location-1** (indicating that the system goes upstream through only the upstream board). Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported). For details about how to configure the electronic switch, see **electro-switch**.

  NOTE

  - The SCUN and SCUH control boards do not support electronic switch.
  - The control board SCUL does not provide the upstream port and the system goes upstream through only the upstream board.

Data Plan

After the service requirements are further confirmed and analyzed with the service provider, the data plan is made by considering the interconnection with the MGC and according to the data plan described in **10.1 Configuring the VoIP Service (H.248-based or MGCP-based)**. **Table 17-3** provides the data plan for configuring the H.248-based VoIP service.

Table 17-3 Data plan for configuring the H.248-based VoIP service

Item			Data
MG interface data (The data configuration on the MG interface must be the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the VoIP service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the upstream board. Therefore, port 0/19/0 is used as the upstream port of the VoIP service.
		Media and signaling IP addresses	These two IP addresses are both 10.10.10.10.
		Default IP address of the MG	Confirmed with the engineers of this service provider, the next hop IP address from MA5600T/MA5603T to the MGC is 10.10.10.1.
	Parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	Confirmed with the engineers of this service provider, the 32 users to be provisioned with the services are the first batch of users in the community named **huawei**, and later other users in this community will be provisioned with the same services gradually. The number of users in this community is 10,000. Considering that the number of users is large, the office assigns a VAG (VAG 0) to this community for better management. Therefore, the MG interface ID is 0
		Signaling port ID of the MG interface	The signaling port ID is 2944.
		IP address of the primary MGC to which the MG interface belongs	The service provider does not provide dual homing for its network. According to the network topology, the IP address of the primary MGC is 10.10.20.20, and the port ID is 2944, the same as the port ID on the MA5600T/MA5603T.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	The **text** coding mode is adopted.

Item			Data
		Transmission mode of the MG interface	UDP is adopted.
		Domain name of the MG interface	The message ID (MID) adopts the IP address (default), and may not be configured with the domain name.
		Device name of the MG interface	The MID adopts the IP address (default), and may not be configured with the device name.
	Digitmap of the MG interface		Special applications such as emergency calls and emergency standalone are not configured, and therefore the digitmap is not configured here.
	Software parameters of the MG interface		According to the Background Information in **(Optional) Configuring the Software Parameters of an MG Interface** and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the software parameters are not configured here.
	Ringing mode of the MG interface		Confirmed with the service provider, the value of the ringing parameter (corresponding to the users) defined on the MGC is 0 (value of *mgcpara*), and the users have no special requirements for the ringing mode. Therefore, the normal ringing with the break-make ratio of 1:4 is adopted.
	Terminal ID (TID) format of the MG interface		To differentiate users according to the TID, the service provider requires that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the slot ID/subrack ID/port ID of the user. Run the **display tid-template** command to query the default TID template. It is found that default TID template (template 6) can meet the requirements.
VoIP user data (The data configuration must be the	Slot for the voice service board		User access is implemented by the ASPB board in slot 0/3.

Item			Data
same as the data configuration on the MGC.)	**User data**	Phone number	The emergency standalone is not supported, and therefore the configuration of phone numbers is not required when the users are added. The MGC assigns phone numbers 83110000-83110031 to phones 0-31 respectively.
		TID	The terminal layering is supported, and therefore the manual allocation of TIDs is not required.
		User priority	The users are common users, and the user priority uses the default cat3.
		User type	The users are common users, and the users are of the default DEL type.
	System parameters		According to the Background Information in **(Optional) Configuring the System Parameters** and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the system parameters are not configured here.
	Overseas parameters		According to the Background Information in **(Optional) Configuring the Overseas Parameters** and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the overseas parameters are not configured here.
	PSTN port attributes		The polarity reversal accounting is adopted, and therefore the PSTN port to which the users belong needs to support the polarity reversal pulse. The other attributes of the PSTN port do not need to be modified.
	Ringing current attributes		There is no special requirement, and the configuration of the ringing current attributes is not required.

Procedure

Step 1 Add the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
huawei(config-if-vlanif20)#quit
```

Step 2 Configure the media and signaling IP address pools.

Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively, which facilitates the selection of media and signaling IP addresses used for the services from the IP address pools. According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the 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.

Step 3 Add an MG interface.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 0, and configure the interface attributes.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute mg-media-ip1 10.10.10.10 mgip
10.10.10.10 mgport 2944 primary-mgc-ip1 10.10.20.20
primary-mgc-port 2944 code text transfer udp
```

Step 4 Configure the ringing mapping of MG interface 0.

Configure the user ringing mode. According to the data plan, the break-make ratios of the cadence ringing and the initial ringing are both 1:4. Therefore, the value of parameter *cadence* is 0, and the value of parameter *initialring* is 4.

```
huawei(config-if-h248-0)#mg-ringmode add 0 0 4
```

Step 5 Configure the TID format of PSTN users on MG interface 0.

Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users needs to be **huawei**, and the TID template adopts layering template 6.

CAUTION

The MA5600T/MA5603T requires that the terminal prefixes of PSTN users, ISDN BRA users, and ISDN PRA users on the same H.248 interface are either the same or different. Note this when configuring the terminal prefix.

```
huawei(config-if-h248-0)#tid-format pstn prefix huawei template 6
```

Step 6 Enable the MG interface.

Reset the MG interface to make the MG interface register with the MGC (or to make the attributes of the MG interface take effect), so that the MG interface can work in the normal state. The MG interface can be enabled in different ways (see Parameters of the **reset** command). For a newly configure MG interface, enable the MG interface through cold start.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

Step 7 Query the running status of the MG interface.

After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface can work in the normal state.

```
huawei(config)#display if-h248 all
  -------------------------------------------------------------------------
  MGID   TransMode State    MGPort MGIP/DomainName MGCPort MGCIP/DomainName
  -------------------------------------------------------------------------
  0      UDP       Normal   2944   10.10.10.10     2944    10.10.20.20
  -------------------------------------------------------------------------
```

Step 8 Confirm the service board.

Confirm the ASPB board that carries services to ensure that the board can work in the normal state.

```
huawei(config)#board confirm 0/3
```

Step 9 Configure the PSTN user data.

Add POTS users (phones 0-31) to ensure that users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0
huawei(config-esl-user)#quit
```

Step 10 Configure the polarity reversal accounting function.

Configure the physical attributes of the PSTN port to which the users belong to support the polarity reversal pulse, so that the users can support the polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 11 Save the data.

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

----End

Result

After the interface data and the PSTN user data corresponding to the MG interface are configured on the MGC, check whether the VoIP services can be provisioned normally. In the normal state, phones 0-31 can make phone calls to each other:

- The caller can hear the dial tone after picking up the phone.

- When the caller dials the phone number of the callee, the phone of the callee can ring normally, and the caller can hear the ring back tone.
- The caller and the callee can communicate with each other successfully.
- After the callee hangs up the phone, the caller can hear the busy tone.

Configuration File

The following describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported directly.

Configure the upstream VLAN interface.

```
vlan 20 standard
port vlan 20 0/19 0
interface vlanif 20
ip address 10.10.10.10 24
quit
```

Configure the media and signaling IP address pools.

```
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
quit
```

Add an MG interface and configure the attributes of the MG interface. The MG interface must be configured manually, and the configuration profile cannot be directly imported.

```
interface h248 0
if-h248 attribute mg-media-ip1 10.10.10.10 mgip 10.10.10.10 mgport 2944 primary-
mgc-ip1 10.10.20.20
 primary-mgc-port 2944 code text transfer udp
```

Configure the ringing mapping of the MG interface.

```
mg-ringmode add 0 0 4
```

Configure the TID format of the PSTN user on the MG interface.

```
tid-format pstn prefix huawei template 6
```

Enable the MG interface. The MG interface must be enabled manually, and the configuration profile cannot be directly imported.

```
reset coldstart
quit
```

Query the running status of the MG interface.

```
display if-h248 all
```

Confirm the service board.

```
board confirm 0/3
```

Configure the PSTN user data.

```
esl user
mgpstnuser batadd 0/3/0 0/3/31 0
quit
```

Configure the polarity reversal accounting function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse enable
quit
```

Save the data.

```
save
```

17.3.2 Example: Configuring the VoIP Service (MGCP-based)

This topic describes how to configure the MGCP-based VoIP service.

Service Requirements

In an office located in China, the MA5600T/MA5603T that adopts the MGCP protocol is newly deployed. Data plan and configuration, however, are not performed on the MGC (softswitch) connected to the MA5600T/MA5603T. The MA5600T/MA5603T is required to provide the following VoIP services:

- The common phone services are provisioned to 32 users (phones 0-31).
- The polarity-reversal accounting is adopted.

After the service requirements are further confirmed and analyzed with the service provider, the data plan is made by considering the interconnection with the MGC and according to the data plan described in **10.1 Configuring the VoIP Service (H.248-based or MGCP-based)**. **Table 17-4** provides the data plan for configuring the MGCP-based VoIP service.

Table 17-4 Data plan for configuring the MGCP-based VoIP service

Item			Data
MG interface data (The data configuration must be the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the VoIP service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the control board. Therefore, port 0/19/0 is used as the upstream port of the VoIP service.
		Media and signaling IP address	These two IP addresses are both 10.10.10.10. **CAUTION** The MGCP interface on the MA5600T/MA5603T does not support the isolation of media streams and signaling flows. Therefore, when the MGCP protocol is used, the media IP address pool and the signaling IP address pool must be the same. When the H.248 or SIP protocol is used, the media IP address pool and the signaling IP address pool can be the same or different.
		Default IP address of the MG	Confirmed with the engineers of this service provider, the next hop IP address from MA5600T/MA5603T to the MGC is 10.10.10.1.

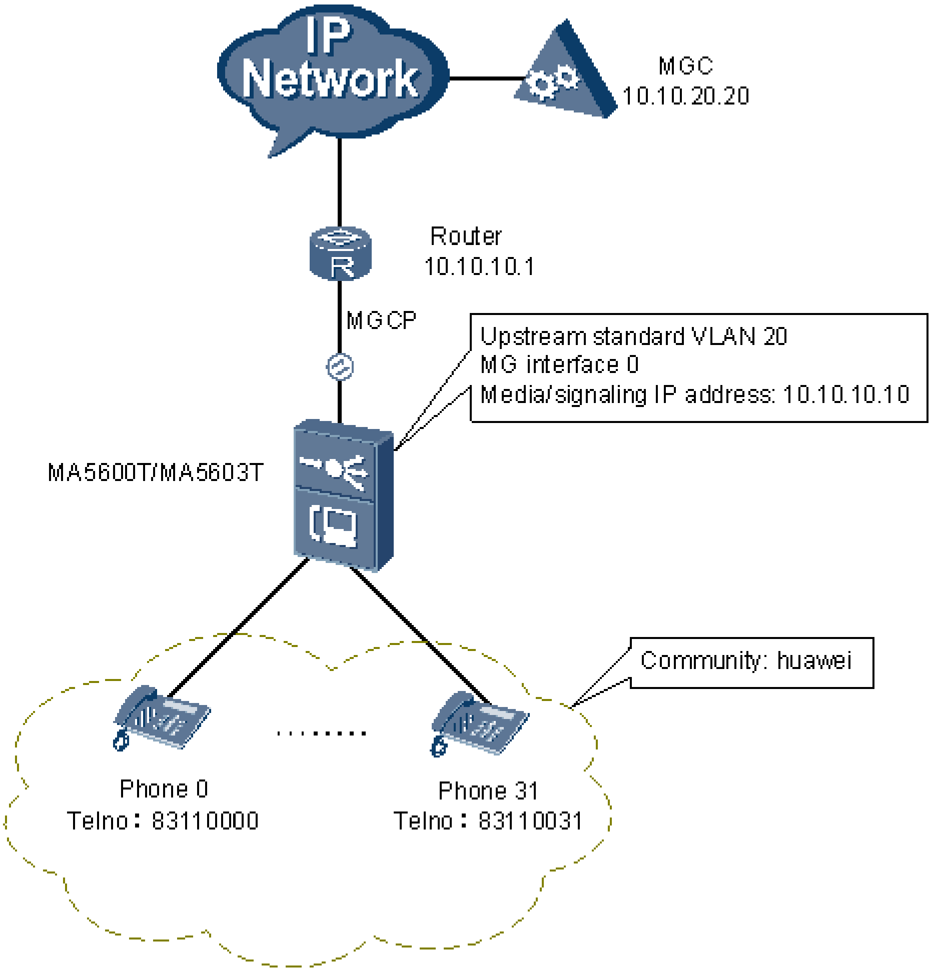
Item			Data
	Parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	Confirmed with the engineers of this service provider, the 32 users to be provisioned with the services are the first batch of users in the community named **huawei**, and later other users will be provisioned with the same services gradually. The number of users in this community is 10,000. Considering that the number of users is large, the service provider assigns a VAG (VAG 0) to this community for better management. Therefore, the MG interface ID is 0.
		Signaling port ID of the MG interface	The signaling port ID is 2727.
		IP address of the primary MGC to which the MG interface belongs	The service provider does not provide dual homing for its network. According to the network topology, the IP address of the primary MGC is 10.10.20.20, and the port ID is 2727, the same as the port ID on the MA5600T/MA5603T.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	For the MG interface that supports MGCP, the default coding mode is the **text** coding mode. This parameter can be queried, but cannot be configured.
		Transmission mode of the MG interface	For the MG interface that supports MGCP, the default transmission mode is UDP. This parameter can be queried, but cannot be configured.
		Domain name of the MG interface	The community name **huawei** is adopted.
	Digitmap of the MG interface		Special applications such as emergency calls and emergency standalone are not configured, and therefore the digitmap is not configured.

Item			Data
	Software parameters of the MG interface		According to the Background Information in **(Optional) Configuring the Software Parameters of an MG Interface** and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the software parameters are not configured here.
	Ringing mode of the MG interface		Confirmed with the service provider, the value of the ringing parameter (corresponding to the users) defined on the MGC is 0 (value of *mgcpara*), and the users have no special requirements for the ringing mode. Therefore, the normal ringing with the break-make ratio of 1:4 is adopted.
	Terminal ID (TID) format of the MG interface		To differentiate users according to the TID, the service provider requires that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the slot ID/subrack ID/ port ID of the user. Run the **display tid-template** command to query the default TID template. It is found that default TID template 6 can meet the requirements.
VoIP user data (The data configuration must be the same as the data configuration on the MGC.)	Slot of the voice service board		User access is implemented by the ASPB board in slot 0/3.
	User data	Phone number	MGCP does not support emergency standalone, and therefore the phone number does not need to be configured when the user is added. The MGC assigns phone numbers 83110000-83110031 to phones 0-31 respectively.
		TID	The terminal layering is supported, and therefore the manual allocation of TIDs is not required.
		User priority	The users are common users, and the user priority uses default cat3.
		User type	The users are common users, and the users are of the default DEL type.

Item		Data
	System parameters	According to the Background Information in **(Optional) Configuring the System Parameters** and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the system parameters are not configured here.
	Overseas parameters	According to the Background Information in **(Optional) Configuring the Overseas Parameters** and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the overseas parameters are not configured here.
	PSTN port attributes	The polarity reversal accounting is adopted, and therefore the PSTN port to which the users belong needs to support the polarity reversal pulse. The other attributes of the PSTN port do not need to be modified.
	Ringing current attributes	There is no special requirement, and the configuration of the ringing current attributes is not required.

Figure 17-11 shows an example network for configuring the MGCP-based VoIP service.

Figure 17-11 Example network for configuring the MGCP-based VoIP service



Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T to the MGC must be configured to ensure that the MA5600T/MA5603T and the MGC are reachable from each other.
- Electronic switch 0 must be in **location-1** (indicating that the system goes upstream through only the upstream board). Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported). For details about how to configure the electronic switch, see **electro-switch**.

  NOTE

  - The SCUN and SCUH control boards do not support electronic switch.
  - The control board SCUL does not provide the upstream port and the system goes upstream through only the upstream board.
- The POTS service board, namely the ASPB board, must be inserted into the planned slot, and the RUN ALM LED of the board must be green and must be on for 1s and off for 1s repeatedly.

Procedure

Step 1 Add the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
huawei(config-if-vlanif20)#quit
```

Step 2 Configure the media and signaling IP address pools.

According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

Step 3 Add an MG interface.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 0, and configure the interface attributes.

```
huawei(config)#interface mgcp 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#if-mgcp attribute mgip 10.10.10.10 mgport 2727 mgcip_1 
10.10.20.20 mgcport_1 2727 domainName huawei
```

Step 4 Configure the ringing mapping of MG interface 0.

Configure the ringing mode of the MG interface. According to the data plan, the break-make ratios of the cadence ringing and the initial ringing are both 1:4. Therefore, the value of parameter *cadence* is 0, and the value of parameter *initialring* is 4.

```
huawei(config-if-mgcp-0)#mg-ringmode add 0 0 4
```

Step 5 Configure the TID format of PSTN users on MG interface 0.

Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users needs to be **huawei**, and the TID template adopts layering template 6.

```
huawei(config-if-mgcp-0)#tid-format pstn prefix huawei template 6
```

Step 6 Enable the MG interface.

Reset the MG interface to make the MG interface register with the MGC (or to make the attributes of the MG interface take effect), so that the MG interface can work in the normal state.

```
huawei(config-if-mgcp-0)#reset
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#quit
```

Step 7 Query the running status of the MG interface.

After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface can work in the normal state.

```
huawei(config)#display if-mgcp all
  --------------------------------------------------------------------------
  MGID     State          MGPort MGIP           MGCPort MGCIP/DomainName
  --------------------------------------------------------------------------
  0        Normal         2727   10.10.10.10    2727    10.10.20.20
  --------------------------------------------------------------------------
```

Step 8 Configure the PSTN user data.

Add POTS users (phones 0-31) to ensure that users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0
huawei(config-esl-user)#quit
```

Step 9 Configure the polarity reversal accounting function.

Configure the physical attributes of the PSTN port to which the users belong to support the polarity reversal pulse, so that the users can support the polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 10 Save the data.

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

----End

Result

After the interface data and the PSTN user data corresponding to the MG interface are configured on the MGC, check whether the VoIP services can be provisioned normally. In the normal state, phones 0-31 can make phone calls to each other:

- The caller can hear the dial tone after picking up the phone.
- When the caller dials the phone number of the callee, the phone of the callee can ring normally, and the caller can hear the ring back tone.
- The caller and the callee can communicate with each other successfully.
- After the callee hangs up the phone, the caller can hear the busy tone.

Configuration File

The following describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported directly.

Configure the upstream VLAN interface.

```
vlan 20 standard
port vlan 20 0/19 0
interface vlanif 20
ip address 10.10.10.10 24
quit
```

Configure the media and signaling IP address pools.

```
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
quit
```

Add an MG interface and configure the attributes of the MG interface. The MG interface must be configured manually, and the configuration profile cannot be directly imported.

```
interface mgcp 0
if-mgcp attribute mgip 10.10.10.10 mgport 2727 mgcip_1 10.10.20.20 mgcport_1 2727
domainName huawei
```

Configure the ringing mapping of the MG interface.

```
mg-ringmode add 0 0 4
```

Configure the TID format of the PSTN user on the MG interface.

```
tid-format pstn prefix huawei template 6
quit
```

Enable the MG interface. The MG interface must be enabled manually, and the configuration profile cannot be directly imported.

```
reset
```

Query the running status of the MG interface.

```
display if-mgcp all
```

Confirm the service board.

```
board confirm 0/3
```

Configure the PSTN user data.

```
esl user
mgpstnuser batadd 0/3/0 0/3/31 0
quit
```

Configure the polarity reversal accounting function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse enable
```

Save the data.

```
quit
save
```

17.3.3 Example: Configuring the VoIP PSTN Service (SIP)

This topic describes the configuration example of the VoIP PSTN service based on sip protocol.

Service Requirements

In an office located in China, the MA5600T/MA5603T that adopts the SIP protocol is newly deployed. Data plan and configuration, however, are not performed on the IMS (softswitch) connected to the MA5600T/MA5603T. The MA5600T/MA5603T is required to provide the following VoIP services:

- The common phone services are provisioned to 128 users (phones 0-127).
- The polarity-reversal accounting is adopted.

After the service requirements are further confirmed and analyzed with the office, the data plan is made by considering the interconnection with the IMS and according to the data plan described in **10.2 Configuring the VoIP Service (SIP-based)**. **Table 17-5** provides the data plan for configuring the SIP-based VoIP service.

In this example, the device runs in China. The default configurations of system parameters and the overseas feature parameters meet the standard and the application requirements. Therefore, you do not need to configure these parameters.

Table 17-5 provides the data plan for configuring the VoIP PSTN service (SIP).

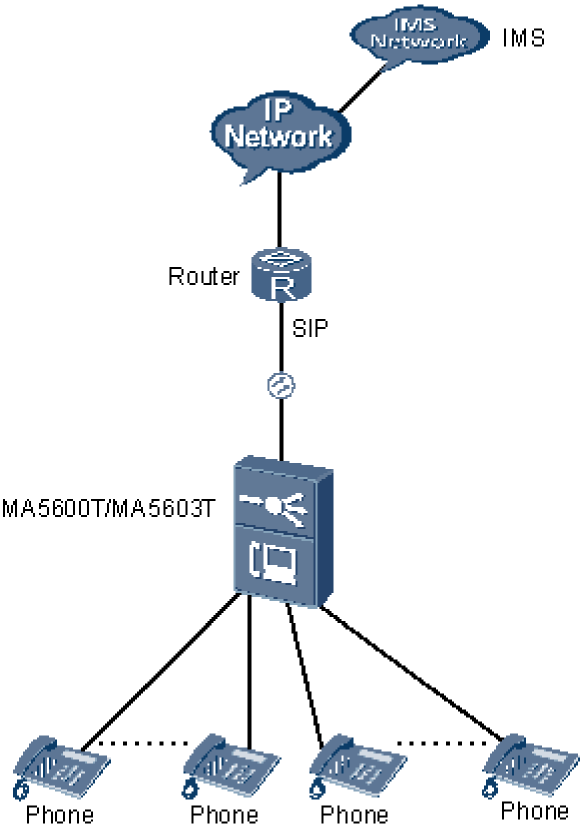
Table 17-5 Data plan for configuring the VoIP PSTN service (SIP)

Item			Data
SIP interface data (The data configuration on the SIP interface must be the same as the data configuration on the IMS.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the VoIP service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the GIU board. Therefore, port 0/19/0 is used as the upstream port of the VoIP service.
		Media and signaling IP addresses	These two IP addresses are both 10.10.10.10/24.
	SIP interface (SIP) **NOTE** The parameters of the SIP interface must be the same as the parameters on the softswitch. SIP has many negotiation parameters, and the parameters here are mandatory.	The SIP interface ID	0 It is the SIP interface ID used for the VoIP service to be configured, which determines the virtual access gateway (VAG) specified for the user.
		Signaling port ID of the SIP interface	5060
		IP address of the primary softswitch to which the SIP interface belongs	IP address: 10.10.10.20/24 Port ID: 5060 When dual homing is configured, the IP address and the port ID of the secondary softswitch must also be configured.
		Port ID of the primary softswitch to which the SIP interface belongs	
		Coding mode of the SIP interface	text
		Transmission mode of the SIP interface	UDP The transmission mode is selected according to the requirements on the softswitch. Generally, UDP is adopted.
		Home domain of the SIP interface	huawei

Item			Data
		Index of the profile used by the SIP interface	1
VoIP user data (The data configuration must be the same as the data configuration on the IMS.)	Slots that the boards reside in Voice service board (ASPB)		User access is implemented by the ASPB board in slot 0/2, 0/3.
	PSTN user data in slot 0/2	Numbers of Phone 0-Phone 63	83110000-83110063
		User priority	Phone 0: Cat2; Phone 1-Phone 63: Cat3 (default)
		User authentication	PSTN user whose port is 0/2/0, and telephone number is 83110000. ● Username: user83110000 ● Password: password mode, value: pwd83110000
	PSTN user data in slot 0/3	Numbers of Phone 64-Phone 127	88110000-88110063
		User type	Payphone
		PSTN port attributes	Polarity reversal pulse supported

Figure 17-12 shows an example network of the VoIP PSTN service (SIP).

Figure 17-12 Example network for configuring the VoIP PSTN service (SIP)



Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T to the IMS must be configured to ensure that the MA5600T/MA5603T and the IMS are reachable from each other.
- Electronic switch 0 must be in **location-1** (indicating that the system goes upstream through only the upstream board). Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported). For details about how to configure the electronic switch, see **electro-switch**.

  NOTE

  - The SCUN and SCUH control boards do not support electronic switch.
  - The control board SCUL does not provide the upstream port and the system goes upstream through only the upstream board.

Procedure

Step 1 Add the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
huawei(config-if-vlanif20)#quit
```

Step 2 Configure the media and signaling IP address pools.

Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively, which facilitates the selection of media and signaling IP addresses used for the services from the IP address pools. According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the 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.

Step 3 Add an SIP interface.

Add an SIP interface to communicate with the IMS, which ensures that the IMS can control the call connection through the SIP interface. According to the data plan, add SIP interface 0, and configure the interface attributes.

- Signaling/Media IP address: 10.10.10.10
- Coding mode: text
- Signaling port ID: 5060
- Transfer mode: UDP
- IP address of the primary IMS: 10.10.10.20
- Signaling port ID of the primary IMS: 5060Media IP address 1: 17.10.10.10
- Homing domain name of SIP interface: huawei
- SIP profile ID: 1

```
huawei(config)#interface sip 0
  Are you sure to add SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.10
 signal-ip 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 10.10.10.20
primary-proxy-port
5060 home-domain huawei sipprofile-index 1
```

Step 4 Configure the ringing mapping of SIP interface 0.

Configure the user ringing mode. The break-make ratios of the cadence ringing and the initial ringing are both 1:4. Therefore, the value of parameter *cadence* is 0, and the value of parameter *initialring* is 4.

```
huawei(config-if-sip-0)#ringmode add 0 ringname cadencering 0 initialring 4
```

Step 5 Enable the SIP interface.

Reset the SIP interface to make the SIP interface register with the IMS (or to make the attributes of the SIP interface take effect), so that the SIP interface can work in the normal state.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#quit
```

Step 6 Query the running status of the SIP interface.

After the SIP interface is interconnected with the IMS, the SIP interface should be in the normal state, indicating that the SIP interface can work in the normal state.

```
huawei(config)#display if-sip all
 -----------------------------------------------------------------------------
  MGID     Trans State     MGPort MGIP            ProxyPort ProxyIP/DomainName
  -----------------------------------------------------------------------------
  0        UDP   Normal     5060   10.10.10.10      5060      10.10.10.20/huawei
  -----------------------------------------------------------------------------
```

Step 7 Configure the PSTN subscriber data.

1. Configure the PSTN user data (Phone 0-Phone 63) in slot 0/2.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/2/0 0/2/63 0 telno 83110000
   ```

2. Configure the calling priority of the PSTN user in port 0/2/0 as Cat2.

   ```
   huawei(config-esl-user)#sippstnuser attribute set 0/2/0 priority cat2
   ```

3. Configure the PSTN user data (Phone 64-Phone 127) in slot 0/3.

   ```
   huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/63 0 telno 88110000
   ```

4. Configure the authentication data of the PSTN user in port 0/2/0.

   ```
   huawei(config-esl-user)#sippstnuser auth set 0/2/0 telno 83110000 password-
   mode password
     User Name(<=64 characters, "-" indicates deletion):user83110000
     User Password(<=64 characters, "-" indicates deletion):    //Input the
   password pwd8311000
   ```

   NOTE

   Considering users safety, the IMS may require user authentication. You can run the **sippstnuser auth set** command to configure the user authentication data, including user name, password mode and password. The authentication data should be consistent with that of IMS side.

5. Configure the PSTN user type in slot 0/3.

   ```
   huawei(config-esl-user)#sippstnuser attribute batset 0/3/0 0/3/63 potslinetype
   PayPhone
   huawei(config-esl-user)#quit
   ```

Step 8 Configure the PSTN port attributes.

Configure the PSTN port in slot 0/3 so that the port supports the polarity reversal.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/63 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 9 Save the data.

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

----End

Result

After the interface data and the PSTN user data corresponding to the SIP interface are configured on the IMS, check whether the VoIP services can be provisioned normally. In the normal state, users of Phone 0-Phone 127 can communicate with each other successfully.

- The calling party can hear the dialing tone after picking up the phone.
- When the calling party dials the phone number of the called party, the phone of the called party can ring normally, and the calling party can hear the ring-back tone.
- The calling party and the called party can communicate in the normal state.
- After the called party hooks on, the calling party can hear the busy tone.

Configuration File

The following describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported directly.

Configure the upstream VLAN interface.

```
vlan 20 standard
port vlan 20 0/19 0
interface vlanif 20
ip address 10.10.10.10 24
quit
```

Configure the media and signaling IP address pools.

```
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
```

Add an SIP interface and configure the attributes of the SIP interface.

```
if-sip attribute basic media-ip 10.10.10.10
 signal-ip 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 10.10.10.20
 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
```

Configure the ringing mapping of the SIP interface.

```
ringmode add 0 ringname cadencering 0 initialring 4
```

Enable the SIP interface.

```
reset
quit
```

Query the running status of the SIP interface.

```
display if-sip all
```

Confirm the service board.

```
board confirm 0/2
board confirm 0/3
```

Configure the PSTN user data.

```
esl user
sippstnuser batadd 0/2/00/2/63 0 telno 83110000
sippstnuser attribute set 0/2/0 priority cat2
sippstnuser auth set 0/2/0 telno 83110000 password-mode password
sippstnuser batadd 0/3/0 0/3/63 0 telno 88110000
sippstnuser attribute batset 0/3/0 0/3/63 potslinetype PayPhone
quit
```

Configure the polarity reversal accounting function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/63 reverse-pole-pulse enable
quit
```

Save the data.

```
save
```

17.3.4 Example: Configuring the VoIP Service (H.248-based and SIP-based)

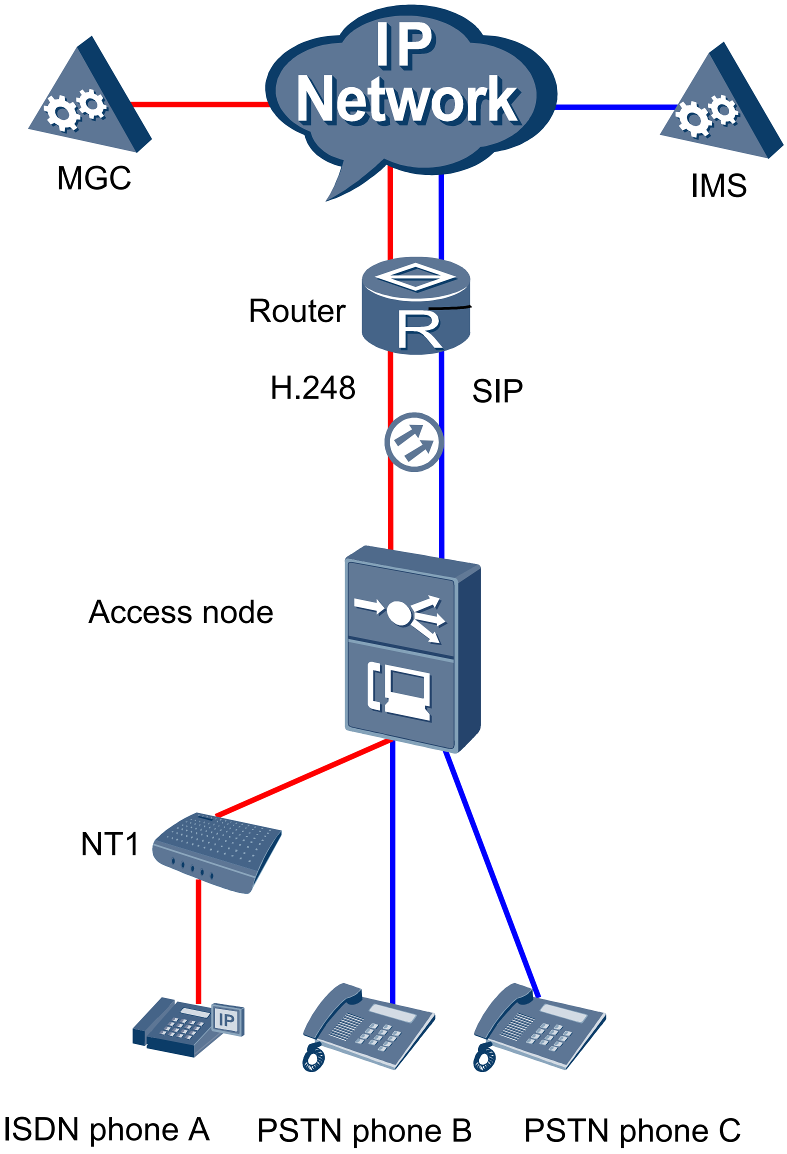
This topic describes an example for configuring the H.248-based and SIP-based VoIP service. The MA5600T/MA5603T supports the H.248-based VoIP service and the SIP-based VoIP service at the same time.

Service Requirements

- The MA5600T/MA5603T upstream to NGN network for ISDN service by adopting the H.248 protocol. The MA5600T/MA5603T upstream to IMS network for PSTN service by adopting the SIP protocol.
- ISDN Phone A is connected to the MA5600T/MA5603T through the NT1, and the ISDN digital phone supports the P2P function.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- The Phone B and Phone C are PSTN users, the user priority is **Cat2**.
- After the configuration is completed, normal calls can be made between two phone sets.

Figure 17-13 shows an example network of the VoIP service that based the SIP protocol and H.248 protocol.

Figure 17-13 the network of the VoIP service that based the SIP protocol and H.248 protocol.



Prerequisite

- The MA5600T/MA5603T upstream to IMS network adopting the SIP protocol and upstream to NGN network by adopting the H.248 protocol.
- The MA5600T/MA5603T must use the H.248 protocol to communicate with the MGC and use the SIP protocol to communicate with the IMS.
- The H.248 interface and the system parameters must be configured. For the related operations, see **10.1.1 Configuring an MG Interface** and **(Optional) Configuring the System Parameters**. The H.248 interface must be in the normal state.
- The SIP interface and the system parameters must be configured. For the related operations, see **10.2.1 Configuring an SIP Interface** and **(Optional) Configuring the System Parameters**. The SIP interface must be in the normal state.

- The system must be configured with the ISDN service board, that is, the DSRD board or DSRE board.
- The system must be configured with the PSTN service board, that is, the ASRB board or ASPB board.
- The ISDN digital phone must support the P2P function.
- The terminal endpoint identifier of the ISDN digital phone must be 0.

Data Plan

Table 17-6 provides the data plan .

Table 17-6 Data plan

Item		Data
The data plan of the ISDN BRA service based H.248 protocol		
H.248 interface ID		0
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)

Item		Data
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
ISDN BRA port	Subrack ID/ Slot ID/Port ID	0/2/0, 0/3/0
	IUA interface ID	8, 9
	Working mode	P2P
	TID	100, 110
	Phone number	12345601, 12345602
	Automatic deactivation	Disabled
	Activation mode	Stable activation
The data plan of the PSTN service based SIP protocol		
SIP interface ID		0
PSTN port (The data configuration must be the same as the data configuration on the IMS.)	Frame/slot/port	0/3/0
	Numbers of Phone	83110000, 83110001
	User priority	Cat2
	User type	Payphone
	PSTN port attributes	Polarity reversal pulse supported

Procedure

- Configure the H.248-based ISDN service
  1. Add the ISDN service board.

     According to the data plan, add a ISDN board to slot0/2.

     ```
     huawei(config)#board add 0/2 H802DSRD
     huawei(config)#board confirm 0/2
     ```

  2. Configure the working mode of the ISDN BRA port.

     In the BRA port mode, configure the working mode of the ISDN BRA port to P2P, configure the activation mode to stable activation, and disable automatic activation.

     ```
     huawei(config)#braport
     ```

```
huawei(config-braport)#braport attribute set 0/2/0 workmode p2p
activemode stable-active autodeactive disable
huawei(config-braport)#quit
```

3. Add an IUA link set and IUA links.

   In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable
trafficmode override
iid-map 2 pendingtime 1 cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
huawei(config-sigtran)#quit
```

   NOTE

   All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

4. Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid
100 telno 12345601
huawei(config-esl-user)#quit
```

CAUTION

Each ISDN BRA user occupies two TIDs. You need to input only the first TID when adding an ISDN BRA user.

- When the TID profile to which the ISDN BRA user of the MG interface is bound is not a layering profile, the TID must be configured and must differ from the TID of the existing ISDN BRA user by an integer multiple of 2.
- When the TID profile to which the ISDN BRA user of the MG interface is bound is a layering profile, the configuration of the TID is optional because the system automatically allocates the TID.

- Configure the SIP-based PSTN service

1. Add the ASPB service board.

   According to the data plan, add a ASPB board to slot0/3.

```
huawei(config)#board add 0/3 ASP
huawei(config)#board confirm 0/3
```

2. Configure the PSTN subscriber data.

   According to the data plan, configure a telephone number and priority of the PSTN user.

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/1 0 telno 83110000
huawei(config-esl-user)#sippstnuser attribute set 0/3/0 priority cat2
huawei(config-esl-user)#sippstnuser attribute set 0/3/1 priority cat2
huawei(config-esl-user)#quit
```

3. Configure the PSTN port attributes.

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

4. Save the data.

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

----End

Result

After the configuration is completed, users of ports 0/2/0, 0/3/0, and 0/3/1 can call each other successfully.

Configuration File

```
board add 0/2 H802DSRD
board confirm 0/2
braport
braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive
disable
quit
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime 1 cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
quit
esl user
mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid 100 telno 12345601
quit
board add 0/3 ASP
board confirm 0/3
esl user
sippstnuser batadd 0/3/00/3/1 0 telno 83110000
sippstnuser attribute set 0/3/0 priority cat2
sippstnuser attribute set 0/3/1 priority cat2
quit
pstnport
pstnport attribute batset 0/3/0 0/3/1 reverse-pole-pulse enable
quit
save
```

17.3.5 Example: Configuring the P2P ISDN BRA Service

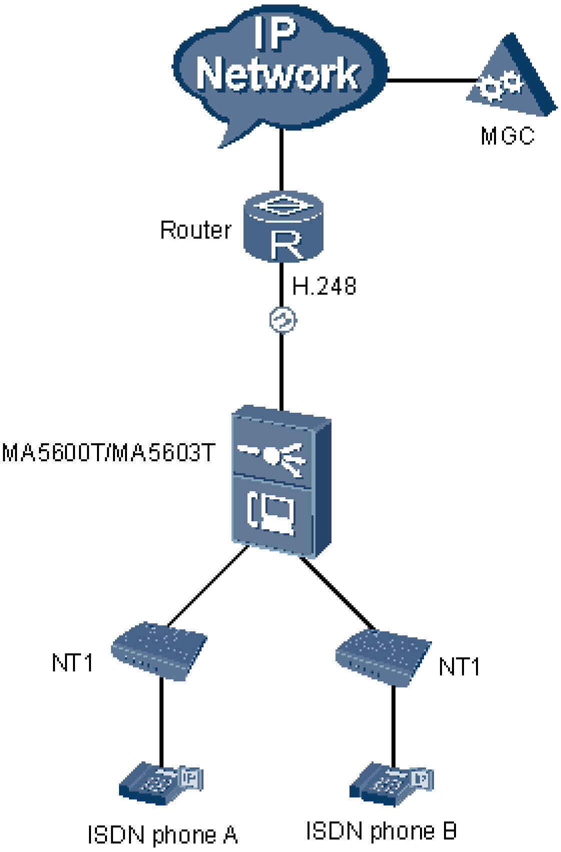
This topic describes how to configure the P2P ISDN BRA service on the MA5600T/MA5603T, which is applicable to the scenario where one NT1 is connected to only one terminal.

Service Requirements

- ISDN Phone A is connected to the MA5600T/MA5603T through the NT1, and the ISDN digital phone supports the P2P function.
- ISDN Phone B is connected to the MA5600T/MA5603T through the NT1, and the ISDN digital phone supports the P2P function.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- After the configuration is completed, normal calls can be made between two phone sets.

Figure 17-14 shows an example network of the P2P ISDN BRA service.

Figure 17-14 Example network of the P2P ISDN BRA service



Prerequisite

- The MG interface and the system parameters must be configured. For the related operations, see **10.1.1 Configuring an MG Interface** and **(Optional) Configuring the System Parameters**. The MG interface must be in the normal state.
- The ISDN digital phone must support the P2P function.
- The system must be configured with the ISDN service board, that is, the DSRD board.
- The terminal endpoint identifier of the ISDN digital phone must be 0.

Data Plan

Table 17-7 provides the data plan for configuring the P2P ISDN BRA service.

Table 17-7 Data plan for configuring the P2P ISDN BRA service

Item		Data
MG interface ID		0
IUA link set parameter	IUA link set ID	1

Item		Data
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
ISDN BRA port	Subrack ID/ Slot ID/Port ID	0/2/0, 0/3/0
	IUA interface ID	8, 9
	Working mode	P2P
	TID	100, 110
	Phone number	12345601, 12345602

Item		Data
	Automatic deactivation	Disabled
	Activation mode	Stable activation

Procedure

Step 1 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2P, configure the activation mode to stable activation, and disable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/2/0 workmode p2p activemode stable-
active autodeactive disable
huawei(config-braport)#braport attribute set 0/3/0 workmode p2p activemode stable-
active autodeactive disable
huawei(config-braport)#quit
```

Step 2 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
huawei(config-sigtran)#quit
```

NOTE

All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

Step 3 Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid 100 telno
12345601
huawei(config-esl-user)#mgbrauser add 0/3/0 0 1 interfaceid 9 terminalid 110 telno
12345602
huawei(config-esl-user)#quit
```

CAUTION

Each ISDN BRA user occupies two TIDs. You need to input only the first TID when adding an ISDN BRA user.

- When the TID profile to which the ISDN BRA user of the MG interface is bound is not a layering profile, the TID must be configured and must differ from the TID of the existing ISDN BRA user by an integer multiple of 2.
- When the TID profile to which the ISDN BRA user of the MG interface is bound is a layering profile, the configuration of the TID is optional because the system automatically allocates the TID.

Step 4 Save the data.

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

----End

Result

After the configuration is completed, two ISDN BRA users of ports 0/2/0 and 0/3/0 can call each other successfully.

Configuration File

```
board add 0/2 H802DSRD
board add 0/3 H802DSRD
board confirm 0/2
board confirm 0/3
braport
braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive
disable
braport attribute set 0/3/0 workmode p2p activemode stable-active autodeactive
disable
quit
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3quit
esl user
mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid 100 telno 12345601
mgbrauser add 0/3/0 0 1 interfaceid 9 terminalid 110 telno 12345602
quit
save
```

17.3.6 Example: Configuring the P2P ISDN BRA Service (Based on the SIP Protocol)

This topic describes how to configure the P2P ISDN BRA service on the MA5600T/MA5603T, which is applicable to the scenario where one NT1 is connected to only one terminal.

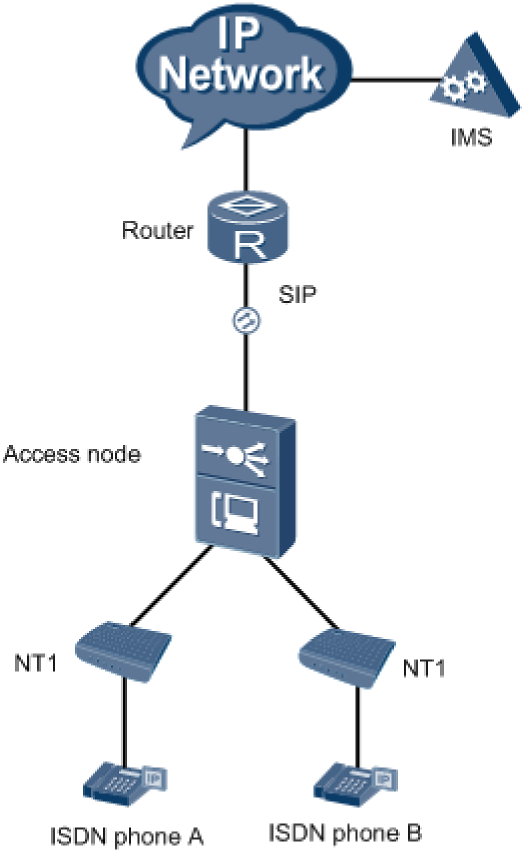
Service Requirements

- ISDN Phone A is connected to the MA5600T/MA5603T through the NT1, and the ISDN digital phone supports the P2P function.

- ISDN Phone B is connected to the MA5600T/MA5603T through the NT1, and the ISDN digital phone supports the P2P function.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- After the configuration is completed, normal calls can be made between two phone sets.

Figure 17-15 shows an example network of the P2P ISDN BRA service.

Figure 17-15 Example network of the P2P ISDN BRA service



Prerequisite

- The MA5600T/MA5603T must use the SIP protocol to communicate with the IMS.
- The MG interface and the system parameters must be configured. For the related operations, see **10.2.1 Configuring an SIP Interface** and **(Optional) Configuring the System Parameters**. The MG interface must be in the normal state.
- The ISDN digital phone must support the P2P function.
- The system must be configured with the ISDN service board, that is, the DSRD board or the DSRE board .
- The terminal endpoint identifier of the ISDN digital phone must be 0.

Data Plan

Table 17-8 provides the data plan for configuring the P2P ISDN BRA service.

Table 17-8 Data plan for configuring the P2P ISDN BRA service

Item		Data
MG interface ID		0
ISDN BRA port	Subrack ID/ Slot ID/Port ID	0/2/0, 0/3/0
	Working mode	P2P
	Phone number	12345601, 12345602
	Automatic deactivation	Disabled
	Activation mode	Stable activation

Procedure

Step 1 Add the ISDN service board.

According to the data plan, add two ISDN boards to slots 0/2 and 0/3.

```
huawei(config)#board add 0/2 H802DSRD
huawei(config)#board add 0/3 H802DSRD
huawei(config)#board confirm 0/2
huawei(config)#board confirm 0/3
```

Step 2 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2P, configure the activation mode to stable activation, and disable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/2/0 workmode p2p activemode stable-
active autodeactive disable
huawei(config-braport)#braport attribute set 0/3/0 workmode p2p activemode stable-
active autodeactive disable
huawei(config-braport)#quit
```

Step 3 Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#sipbrauser add 0/2/0 0 telno 12345601
huawei(config-esl-user)#sipbrauser add 0/3/0 0 telno 12345602
huawei(config-esl-user)#quit
```

Step 4 Save the data.

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

----End

Result

After the configuration is completed, two ISDN BRA users of ports 0/2/0 and 0/3/0 can call each other successfully.

Configuration File

```
board add 0/2 H802DSRD
board add 0/3 H802DSRD
board confirm 0/2
board confirm 0/3
braport
braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive
disable
braport attribute set 0/3/0 workmode p2p activemode stable-active autodeactive
disable
quit
esl user
sipbrauser add 0/2/0 0 telno 12345601
sipbrauser add 0/3/0 0 telno 12345602
quit
save
```

17.3.7 Example: Configuring the P2MP ISDN BRA Service

This topic describes how to configure the P2MP ISDN BRA service on the MA5600T/MA5603T, which is applicable to the scenario where one NT1 is connected to multiple terminals.

Service Requirements

- Two ISDN digital phones are connected to the MA5600T/MA5603T through the same NT1.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T to provide a rate of 144 kbit/s, including two B channels and one D channel.

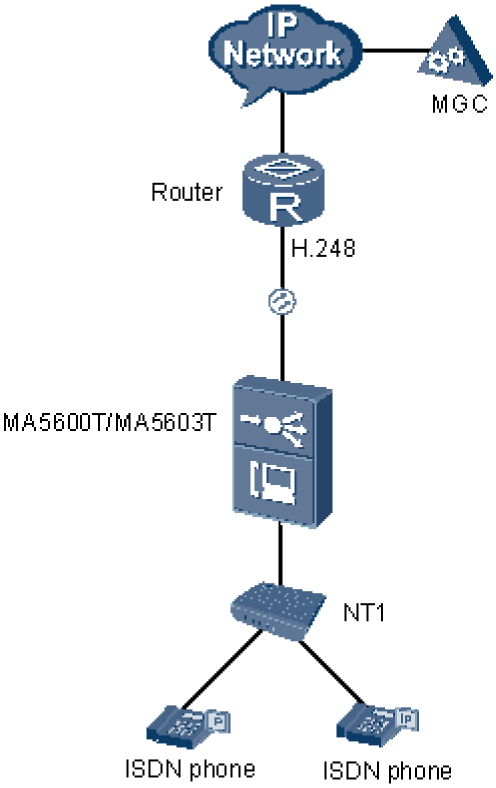
Prerequisite

- The MG interface and the system parameters must be configured. For the related operations, see **10.1.1 Configuring an MG Interface** and **(Optional) Configuring the System Parameters**. The MG interface must be in the normal state.

Networking

Figure 17-16 shows an example network of the P2MP ISDN BRA service.

Figure 17-16 Example network of the P2MP ISDN BRA service



Data Plan

Table 17-9 provides the data plan for configuring the P2MP ISDN BRA service.

Table 17-9 Data plan for the P2MP ISDN BRA service

Item		Data
MG interface ID		0
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable

Item		Data
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
ISDN BRA port	Subrack ID/Slot ID/Port ID	0/3/1
	IUA interface ID	10
	Working mode	P2MP
	TID	106
	Phone number	88880000

Procedure

Step 1 Add the ISDN service board.

According to the data plan, add an ISDN board to slot 0/3.

```
huawei(config)#board add 0/3 H802DSRD
huawei(config)#board confirm 0/3
```

Step 2 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2MP, configure the activation mode to stable activation, and enable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/3/1 workmode p2mp autodeactive
enable
```

Step 3 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config-braport)#quit
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
```

Step 4 Configure the ISDN BRA user data.

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/3/1 0 1 interfaceid 10 terminalid 106
telno 88880000
```

Step 5 Save the data.

```
huawei(config-esl-user)#quit
huawei(config)#save
```

----End

Result

After the configuration is completed, two ISDN BRA users of the NT1 connected to port 0/3/1 can make calls successfully.

Configuration File

```
board add 0/3 H802DSRD
board confirm 0/3
braport
braport attribute set 0/3/1 workmode p2mp autodeactive enable
quit
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
quit
esl user
mgbrauser add 0/3/1 0 1 interfaceid 10 terminalid 106  telno 88880000
quit
save
```

17.3.8 Example: Configuring the P2MP ISDN BRA Service(Based on the SIP Protocol)

This topic describes how to configure the P2MP ISDN BRA service on the MA5600T/MA5603T, which is applicable to the scenario where one NT1 is connected to multiple terminals.

Service Requirements

- Two ISDN digital phones are connected to the MA5600T/MA5603T through the same NT1.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- Normal calls can be made on both phones.

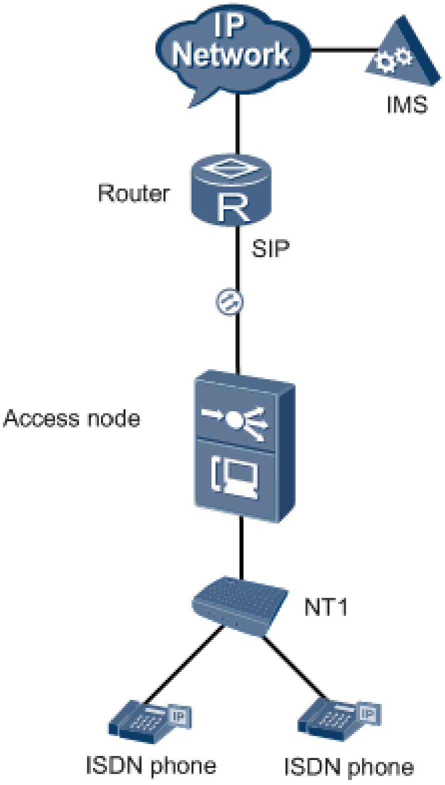
Prerequisite

- The MA5600T/MA5603T must use the SIP protocol to communicate with the IMS.
- The MG interface and the system parameters must be configured. For the related operations, see **10.2.1 Configuring an SIP Interface** and **(Optional) Configuring the System Parameters**. The MG interface must be in the normal state.
- The system must be configured with the ISDN service board, that is, the DSRD board or the DSRE board .

Networking

Figure 17-17 shows an example network of the P2MP ISDN BRA service.

Figure 17-17 Example network of the P2MP ISDN BRA service



Data Plan

Table 17-10 provides the data plan for configuring the P2MP ISDN BRA service.

Table 17-10 Data plan for the P2MP ISDN BRA service

Item	Data
MG interface ID	0

Item		Data
ISDN BRA port	Subrack ID/Slot ID/Port ID	0/3/1
	Working mode	P2MP
	Phone number	88880000

Procedure

Step 1 Add the ISDN service board.

According to the data plan, add an ISDN board to slot 0/3.

```
huawei(config)#board add 0/3 H802DSRD
huawei(config)#board confirm 0/3
```

Step 2 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2MP, configure the activation mode to stable activation, and enable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/3/1 workmode p2mp autodeactive
enable
huawei(config-braport)#quit
```

Step 3 Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#sipbrauser add 0/3/1 0 telno 88880000
huawei(config-esl-user)#quit
```

Step 4 Save the data.

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

----End

Result

After the configuration is completed, two ISDN BRA users of the NT1 connected to port 0/3/1 can make calls successfully.

Configuration File

```
board add 0/3 H802DSRD
board confirm 0/3
braport
braport attribute set 0/3/1 workmode p2mp autodeactive enable
quit
esl user
sipbrauser add 0/3/1 0 telno 88880000
quit
save
```

17.3.9 Example: Configuring the ISDN PRA Service

This topic is applicable to the scenario where the ISDN users are connected to the MA5600T/MA5603T through the ISDN primary rate interface (PRI).

Prerequisite

- The PSTN user (Phone B in the example network) must be configured and can communicate with other users in the normal state. For the configuration method, see **17.3.1 Example: Configuring the VoIP Service (H.248-based)**.
- Users of the PBX must be configured and can communicate with each other in the normal state.
- The system must be configured with the EDTB board.

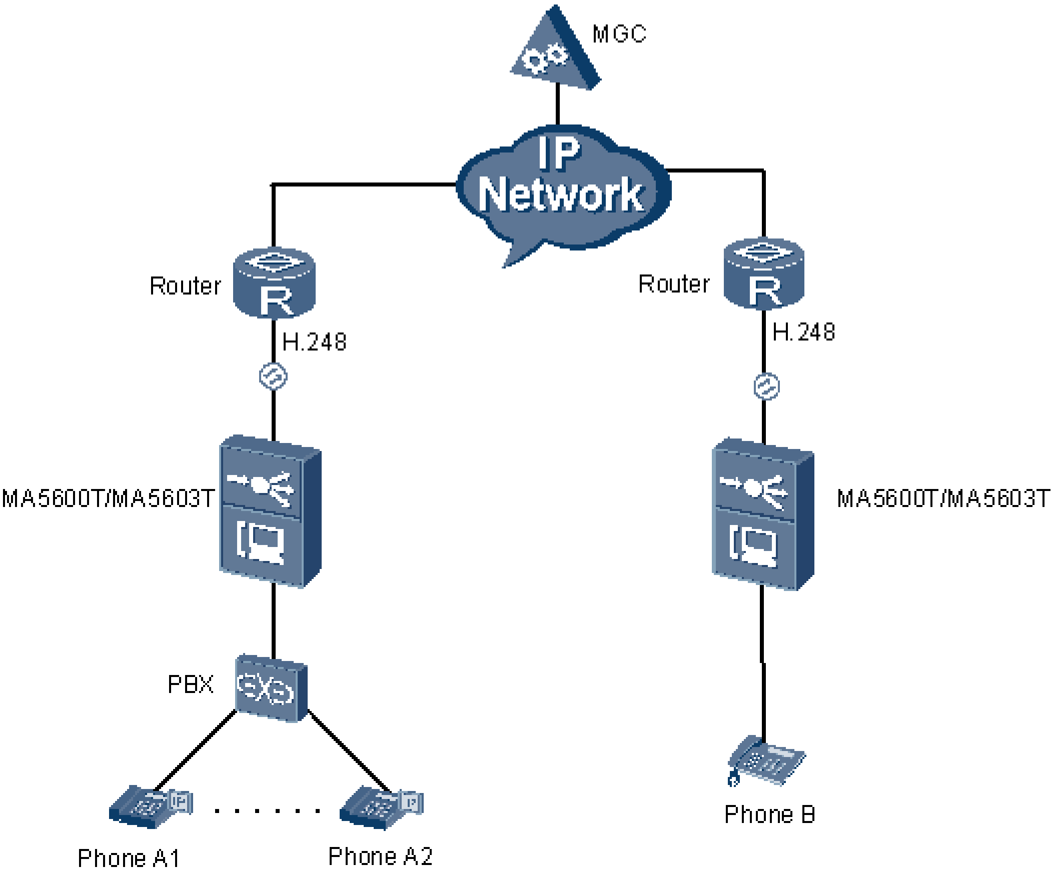
Service Requirements

- The PBX is connected to the MA5600T/MA5603T through the ISDN PRI. PRI supports a data rate of 2048 kbit/s, including 30 B channels and one D channel. The rate of both the B channel and the D channel is 64 kbit/s.
- After the configuration is completed, users of the PBX can make calls successfully and can communicate with users outside the PBX in the normal state.

Networking

Figure 17-18 shows an example of the ISDN PRA service.

Figure 17-18 Example of the ISDN PRA service



Data Plan

Table 17-11 provides the data plan for configuring the ISDN PRA service.

Table 17-11 Data plan for configuring the ISDN PRA service

Item		Data
MG interface ID		0
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
ISDN PRA port	Subrack ID/Slot ID/Port ID	0/2/0
	IUA interface ID	1
	TID	512

Procedure

Step 1 Add the EDTB board.

According to the data plan, add an ISDN PRA service board to slot 0/2.

```
huawei(config)#board add 0/2 h801EDTB
```

Step 2 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
```

NOTE

All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

Step 3 Configure the ISDN PRA user data.

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgprauser add 0/2/0 0 1 interfaceid 1 terminalid 512
```

CAUTION

Each ISDN PRA user occupies 32 TIDs. You need to input only the first TID when adding an ISDN PRA user.

- When the TID profile to which the ISDN PRA user of the MG interface is bound is not a layering profile, the TID must be configured and cannot be within the configured TID range.
- When the TID profile to which the ISDN PRA user of the MG interface is bound is a layering profile, the configuration of the TID parameter is not available because the system automatically allocates the TID.

Step 4 Save the data.

```
huawei(config-esl-user)#quit
huawei(config)#save
```

----End

Result

After the configuration is completed, all the users of the PBX can communicate with Phone B in the normal state.

Configuration File

```
board add 0/2 h801EDTB
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
```

```
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
quit
esl user
mgprauser add 0/2/0 0 1 interfaceid 1 terminalid 512
quit
save
```

17.3.10 Example: Configuring the ISDN PRA Service (Based on the SIP Protocol)

This topic is applicable to the scenario where the ISDN users are connected to the MA5600T/MA5603T through the ISDN primary rate interface (PRI).

Prerequisite

- The MA5600T/MA5603T must use the SIP protocol to communicate with the IMS.
- The MG interface and the system parameters must be configured. For the related operations, see **10.2.1 Configuring an SIP Interface** and **(Optional) Configuring the System Parameters**. The MG interface must be in the normal state.
- The PSTN user (Phone B in the example network) must be configured and can communicate with other users in the normal state. For the configuration method, see **17.3.3 Example: Configuring the VoIP PSTN Service (SIP)**.
- Users of the PBX must be configured and can communicate with each other in the normal state.
- The system must be configured with the EDTB board.

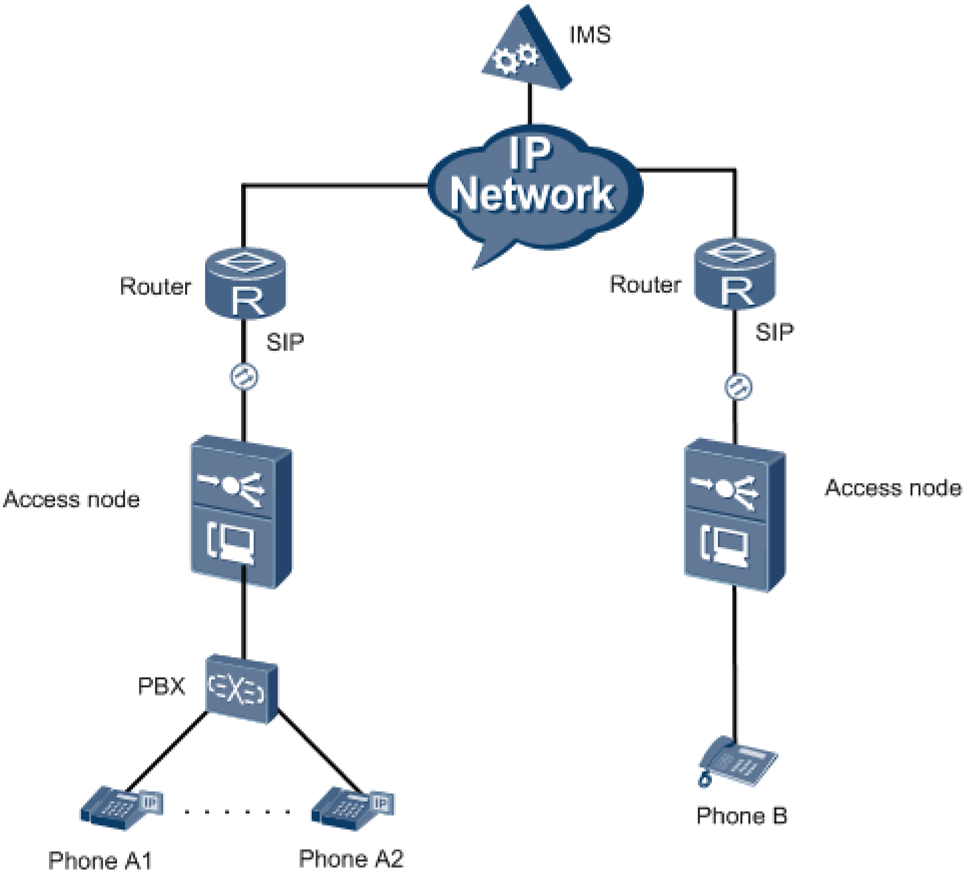
Service Requirements

- The PBX is connected to the MA5600T/MA5603T through the ISDN PRI. PRI supports a data rate of 2048 kbit/s, including 30 B channels and one D channel. The rate of both the B channel and the D channel is 64 kbit/s.
- After the configuration is completed, users of the PBX can make calls successfully and can communicate with users outside the PBX in the normal state.

Networking

Figure 17-19 shows an example of the ISDN PRA service.

Figure 17-19 Example of the ISDN PRA service



Data Plan

Table 17-12 provides the data plan for configuring the ISDN PRA service.

Table 17-12 Data plan for configuring the ISDN PRA service

Item		Data
MG interface ID		0
ISDN PRA port	Subrack ID/Slot ID/Port ID	0/2/0
	Phone number	12345600

Procedure

Step 1 Add the EDTB board.

According to the data plan, add an ISDN PRA service board to slot 0/2.

```
huawei(config)#board add 0/2 H802EDTB
huawei(config)#board confirm 0/2 H802EDTB
```

Step 2 Configure the ISDN PRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#sipprauser add 0/2/0 0 telno 12345600
huawei(config-esl-user)#quit
```

Step 3 Save the data.

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

----End

Result

After the configuration is completed, all the users of the PBX can communicate with Phone B in the normal state.

Configuration File

```
board add 0/2 H802EDTB
board confirm 0/2 H802EDTB
esl user
sipprauser add 0/2/0 0 telno 12345600
quit
save
```

17.3.11 Example: Configuring TDM SHDSL for Carrying the PRA Service

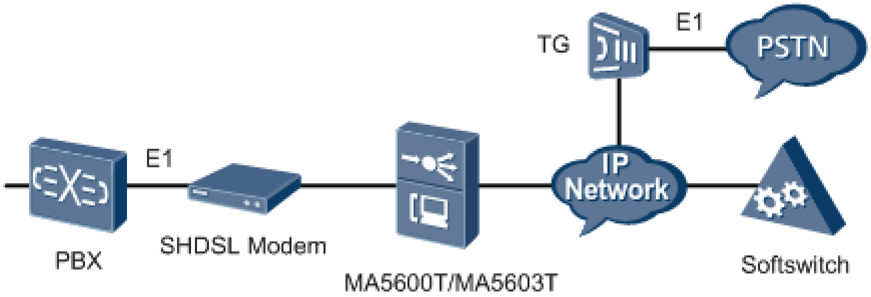
The MA5600T/MA5603T is connected to the PBX in the TDM SHDSL mode and then connected upstream to the IP network in the GE mode.

Service Requirements

- The PBX is connected to the IP network over a long distance to carry the PRA service.
- The user data is transparently transmitted on the MA5600T/MA5603T.

The following figure shows an example network of TDM SHDSL for carrying the PRA service.

Figure 17-20 Example network of TDM SHDSL for carrying the PRA service



Data Plan

The following table lists the data plan for configuring TDM SHDSL for carrying the PRA service.

Table 17-13 Data plan for configuring TDM SHDSL for carrying the PRA service

Item	Data
EDTB board	Working mode: voice Working sub-mode: service mode
Clock source	E1 line clock on port 0/3/0
SHDSL port	Port ID: 0/3/16
PRA user interface data	MGID: 0 IUA link set ID: 0 Terminal ID: 0

Prerequisite

- The H802EDTB board must be in position and must work in the normal state.
- An MG interface must be created and must communicate with the MGC in the normal state.
- An SHDSL modem must be correctly connected and the SHDSL port(s) must be activated.

Procedure

Step 1 (Optional) Configure the working mode of the board

Configure the working mode of the board to voice.

NOTE

The working sub-mode of the board can be configured only when the working mode of the board is configured to voice. By default, the working mode of the board is voice.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
```

Step 2 (Optional) Configure the working sub-mode of the board.

According to the service requirement, configure the working sub-mode of the board to service mode. By default, the working sub-mode of the board is service.

```
huawei(config-edt-0/3)#runmode service
```

Step 3 (Optional) Configure the clock source of the board.

Configure the E1 line clock on port 0/3/0 as the clock source.

NOTE

You can select the line clock or system clock as the clock source of the board according to your requirements. By default, the system clock is used as the clock source.

```
huawei(config-edt-0/3)#set clockmode line 0
```

Step 4 Configure the attributes of the SHDSL port.

Configure the signaling mode of SHDSL port 0/3/16 to CCS. PRA D channel signaling is transmitted in timeslot 16 and timeslot 0 is used for frame synchronization.

```
huawei(config-edt-0/3)#shdslport signal 16 CCS
huawei(config-edt-0/3)#quit
```

Step 5 Configure a PRA user.

```
huawei(config)#esl user
huawei(config-esl-user)#mgprauser add 0/3/16 0 0 terminalid 0
huawei(config-esl-user)#quit
```

Step 6 Save the data.

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

----End

Result

The phone set connected to the PBX can communicate with a phone set in the PSTN network in the normal state.

Configuration File

```
interface edt 0/3
board workmode voice
runmode service
set clockmode line 0
shdslport signal 16 CCS
quit
esl user
mgprauser add 0/3/16 0 0 terminalid 0
quit
save
```

17.3.12 Configuring VAGs

The purpose of configuring virtual access gateways (VAGs) is to simulate multiple AGs by using one AG, increasing the usage rate and flexibility of the device.

Example: Configuring the H.248/MGCP-based VAG Service

This topic describes how to configure the VAG service by creating two MG interfaces on the MA5600T/MA5603T and configuring PSTN users on the two MG interfaces. This topic is applicable to the scenario where multiple logical AGs are simulated on one physical AG.

Context

Configuring VAGs is literally to configure MG interfaces with different IDs on the same device, and to configure user ports homing to different MG interfaces. Pay attention to the following points:

- When the system uses the MGCP or H.248 protocol, up to eight MG interfaces with different IDs can be configured on the MA5600T/MA5603T, and each MG interface can be considered as a VAG.
- When configuring the parameters for interconnecting different MG interfaces with the MGC, make sure that the values of the following parameters of the MG interfaces are not the same. The values of at least one of the following parameters must be different on the MG interfaces.
  - Local IP address
  - Local port ID
  - Remote IP address
  - Remote port ID

Service Requirements

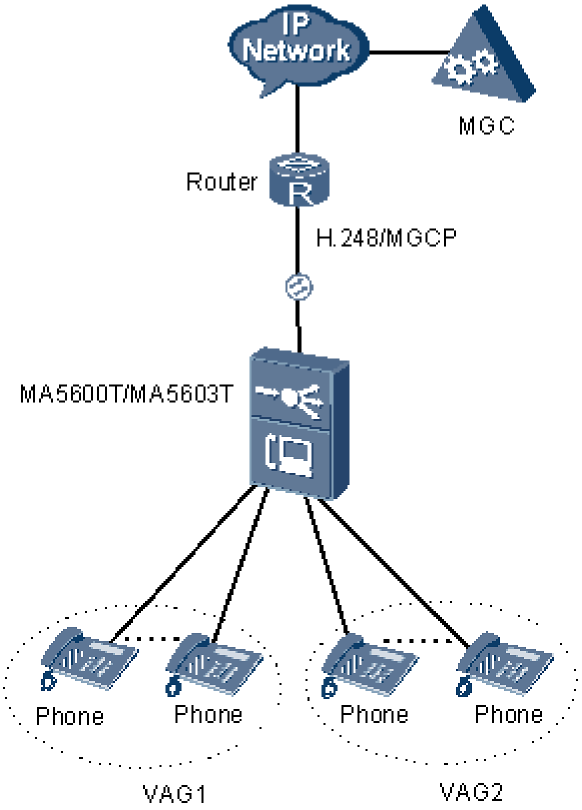
The service requirements are as follows:

- As shown in **Figure 17-21**, configure VAG1, and configure the users in slot 0/2 to belong to VAG1; configure VAG2, and configure the users in slot 0/3 to belong to VAG2.
- The MG communicates with the MGC through the H.248 protocol.
- Configure the data plan of VAG1 as listed in **Table 17-14**.
- The data plan of VAG2 is the same as that of VAG1 except for the following differences:
  - The media IP address and signaling IP address of VAG2 are 10.10.10.11.
  - The MGC assigns phone numbers 85110000-85110031 to phones 0-31 of VAG2.
- MG0 indicates VAG1 in the figure, and MG1 indicates VAG2 in the figure.

Networking

Figure 17-21 shows an example network of the VAG service.

Figure 17-21 Example network of the VAG service



Dataplan

Table 17-14 Data plan of VAG1

Item			Data
MG interface data (The data configuration must be the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the voice service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the control board. Therefore, port 0/19/0 is used as the upstream port of the voice service.
		Media IP address and signaling IP addresses	These two IP addresses are both 10.10.10.10.
		Default gateway IP address	The IP address of the next hop from the MA5600T/MA5603T to the MGC is 10.10.10.1.
	Attributes of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	0 and 1
		Signaling port ID of the MG interface	2944
		IP address of the primary MGC to which the MG interface belongs	The IP address of the primary MGC is 10.10.20.20, and the port ID is 2944, the same as the port ID on the MA5600T/MA5603T.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	**text** (indicates the text coding mode)
		Transmission mode of the MG interface	UDP

Item			Data
	(Optional) Configuring the TID Format of an MG Interface		To differentiate users according to the TID, the office requires that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the subrack ID/slot ID/port ID (F/S/P) of the user. Run the **display tid-template** command to query the default TID template. It is found that default TID template (template 6) can meet the requirements.
Voice user data (The data configuration must be the same as the data configuration on the MGC.)	Slot of the voice service board		User access is implemented by the ASPB board in slot 0/2.
	Configuring the PSTN User Data	Phone number	The emergency standalone is not supported, and therefore the phone numbers do not need to be configured when the users are added. The MGC assigns phone numbers 83110000-83110031 to phones 0-31.
		TID	The terminal layering is supported, and therefore the TIDs do not need to be allocated manually.

Procedure

- Configure VAG1.
  1. Add the upstream VLAN interface.

     According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

     ```
     huawei(config)#vlan 20 standard
     huawei(config)#port vlan 20 0/19 0
     huawei(config)#interface vlanif 20
     huawei(config-if-vlanif20)#ip address 10.10.10.10 24
     huawei(config-if-vlanif20)#quit
     ```

  2. Configure the media and signaling IP address pools.

     Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

     ```
     huawei(config)#voip
     huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
     ```

```
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

3. Add an MG interface.

   Add an MG interface for the MG to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 0, and configure the interface attributes.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute mg-media-ip1 10.10.10.10 mgip
10.10.10.10 mgport 2944 primary-mgc-ip1 10.10.20.20
primary-mgc-port 2944 code text transfer udp
```

4. Configure the TID template of the PSTN users on MG interface 0.

   Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users is **huawei**, and the TID template adopts layering template 6.

CAUTION

The MA5600T/MA5603T requires that the terminal prefixes of PSTN users, ISDN BRA users, and ISDN PRA users on the same H.248 interface be either the same or different. Note this when configuring the terminal prefix.

```
huawei(config-if-h248-0)#tid-format pstn prefix huawei template 6
```

5. Reset the MG interface.

   Reset the MG interface to make the MG interface register with the MGC (and to make the modified attributes of the MG interface take effect) so that the MG interface can work in the normal state. The MG interface can be started in different ways (see Parameters of the **reset** command). For a newly configured MG interface, enable the MG interface through cold start.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

6. Query the running status of the MG interface.

   After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface works in the normal state.

```
huawei(config)#display if-h248 all

------------------------------------------------------------------------
-----
  MGID     Trans State           MGPort MGIP           MGCPort MGCIP/
DomainName

------------------------------------------------------------------------
-----
  0        UDP   Normal          2944   10.10.10.10     2944
10.10.20.20

------------------------------------------------------------------------
-----
```

7. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

```
huawei(config)#board confirm 0/2
```

8. Configure the PSTN user data.

   Add POTS users (phones 0-31) so that the users can go online.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#mgpstnuser batadd 0/2/0 0/2/31 0
   huawei(config-esl-user)#quit
   ```

9. Save the data.

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

- Configure VAG2.

1. Add the upstream VLAN interface.

   According to the data plan, configure the secondary IP address of the Layer 3 interface to 10.10.10.11, which facilitates the configuration of the media and signaling IP address pools.

   In step **Step 1**, the VLAN is added and the IP address of the VLAN Layer 3 interface is configured. In this step, use the sub parameter to configure the secondary IP address of the VLAN. The secondary IP address is the same as the primary IP address in function. They are used for Layer 3 forwarding.

   ```
   huawei(config)#interface vlanif 20
   huawei(config-if-vlanif20)#ip address 10.10.10.11 24 sub
   huawei(config-if-vlanif20)#quit
   ```

2. Configure the media and signaling IP address pools.

   Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.10.10.11 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

   ```
   huawei(config)#voip
   huawei(config-voip)#ip address media 10.10.10.11 10.10.10.1
   huawei(config-voip)#ip address signaling 10.10.10.11
   huawei(config-voip)#quit
   ```

3. Add an MG interface.

   Add an MG interface for the MG to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 1, and configure the interface attributes.

   ```
   huawei(config)#interface h248 1
     Are you sure to add MG interface?(y/n)[n]:y
   huawei(config-if-h248-1)#if-h248 attribute mg-media-ip1 10.10.10.11 mgip
   10.10.10.11 mgport 2944 primary-mgc-ip1 10.10.20.20
   primary-mgc-port 2944 code text transfer udp
   ```

4. Configure the TID template of the PSTN users on MG interface 1.

   Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users is **huawei**, and the TID template adopts layering template 6.

⚠ **CAUTION**

The MA5600T/MA5603T requires that the terminal prefixes of PSTN users, ISDN BRA users, and ISDN PRA users on the same H.248 interface be either the same or different. Note this when configuring the terminal prefix.

```
huawei(config-if-h248-1)#tid-format pstn prefix huawei template 6
```

5. Reset the MG interface.

   Reset the MG interface to make the MG interface register with the MGC (and to make the modified attributes of the MG interface take effect) so that the MG interface can work in the normal state. The MG interface can be started in different ways (see Parameters of the **reset** command). For a newly configured MG interface, enable the MG interface through cold start.

```
huawei(config-if-h248-1)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-1)#quit
```

6. Query the running status of the MG interface.

   After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface works in the normal state.

```
huawei(config)#display if-h248 all

-----------------------------------------------------------------------
-----
  MGID     Trans State           MGPort MGIP            MGCPort MGCIP/
DomainName

-----------------------------------------------------------------------
-----
   0        UDP   Normal          2944   10.10.10.10     2944
10.10.20.2
   1        UDP   Normal          2944   10.10.10.11     2944
10.10.20.20

-----------------------------------------------------------------------
-----
```

7. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

```
huawei(config)#board confirm 0/3
```

8. Configure the PSTN user data.

   Add POTS users (phones 0-31) so that the users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 1
huawei(config-esl-user)#quit
```

9. Save the data.

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

----End

Result

1. When MG0 communicates with the MGC in the normal state, phones 0-31 belonging to MG0 can communicate with each other.
2. When MG1 communicates with the MGC in the normal state, phones 0-31 belonging to MG1 can communicate with each other.
3. When MG0 and MG1 communicate with the MGC in the normal state, phones 0-31 belonging to MG0 and phones 0-31 belonging to MG1 can communicate with each other.

Example: Configuring the SIP-based VAG Service

This topic describes how to configure and verify the VAG service by creating two SIP interfaces on the MA5600T/MA5603T and configuring PSTN users on the two SIP interfaces. This topic is applicable to the scenario where multiple logical AGs are simulated on one physical SIP AG.

Context

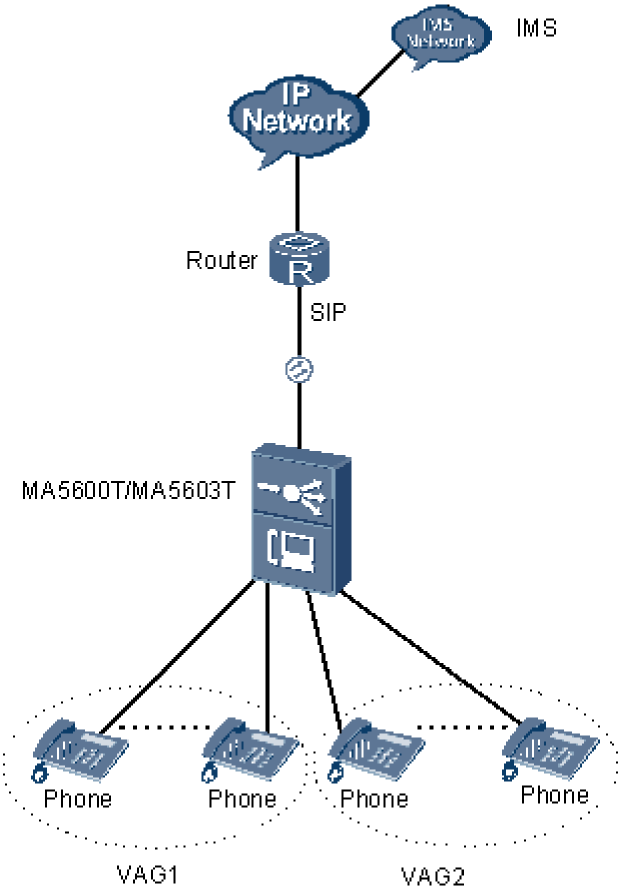
Configuring VAGs is literally to configure SIP interfaces with different IDs on the same device, and to configure user ports homing to different SIP interfaces. Pay attention to the following points:

- When the system uses the SIP protocol, up to eight SIP interfaces with different IDs can be configured on the MA5600T/MA5603T, and each SIP interface can be considered as a VAG.
- When configuring the parameters for interconnecting different SIP interfaces with the IMS, make sure that the values of the following parameters of the SIP interfaces are not completely the same. The values of at least one of the following parameters must be different on the SIP interfaces.
  - Local IP address
  - Local port ID
  - Remote IP address
  - Remote port ID

Service Requirements

Figure 17-22 shows an example network of the SIP-based VAG service.

Figure 17-22 Example network of the SIP-based VAG service



Data Plan

The service requirements are as follows:

- As shown in **Figure 17-22**, configure VAG1, and configure the users in slot 0/2 to belong to VAG1; configure VAG2, and configure the users in slot 0/3 to belong to VAG2.
- The MA5600T/MA5603T communicates with the IMS through the SIP protocol.
- Configure the data plan of VAG1 as listed in **Table 17-15**.
- The data plan of VAG2 is the same as that of VAG1 except for the following differences:
  - The media IP address and signaling IP address of VAG2 are 10.20.10.11.
  - The IMS assigns phone numbers 85000000-85000031 to phones 0-31 of VAG2.
- SIP interface 0 indicates VAG1 in the figure, and SIP interface 1 indicates VAG2 in the figure.

Table 17-15 Data plan of VAG1

Item			Remarks
SIP interface data (The data configuration must be the same as the data configuration on the IMS.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN 30 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the control board. Therefore, port 0/19/0 is used as the upstream port of the voice service.
		Media IP address and signaling IP addresses	These two IP addresses are both 10.20.10.10.
		Default gateway IP address	The IP address of the next hop from the MA5600T/MA5603T to the IMS core network device is 10.20.10.1.
	Attributes of the SIP interface **NOTE** Parameters listed here are mandatory, which means that the SIP interface fails to be enabled if these parameters are not configured.	SIP interface ID	0 and 1
		Signaling port ID of the SIP interface	5060
		IP address of the primary IMS core network device to which the SIP interface belongs	10.20.20.100
		Port ID of the primary IMS core network device to which the SIP interface belongs	5060
		Transmission mode of the SIP interface	UDP
		Homing domain name of the SIP interface	huawei
		Index of the profile used by the SIP interface	Default profile (profile 1)
Voice user data (The data configuration must be the	Slot of the voice service board		The ASPB service board in slot 0/2

Item		Remarks
same as the data configuration on the IMS.)	Phone number	80000000-80000031

Procedure

- Configure VAG1.
  1. Add the upstream VLAN interface.

     According to the data plan, configure standard VLAN 30 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.20.10.10, which facilitates the configuration of the media and signaling IP address pools.

     ```
     huawei(config)#vlan 30 standard
     huawei(config)#port vlan 30 0/19 0
     huawei(config)#interface vlanif 30
     huawei(config-if-vlanif30)#ip address 10.20.10.10 24
     huawei(config-if-vlanif30)#quit
     ```

  2. Configure the media and signaling IP address pools.

     Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.20.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.20.10.1.

     ```
     huawei(config)#voip
     huawei(config-voip)#ip address media 10.20.10.10 10.20.10.1
     huawei(config-voip)#ip address signaling 10.20.10.10
     huawei(config-voip)#quit
     ```

  3. Configure a static route to the IMS.

     Make sure that the route between the local device and the IMS is reachable. The static route is used as an example.

     ```
     huawei(config)#ip route-static 10.20.0.0 255.255.0.0 10.20.10.1
     ```

  4. Add a SIP interface.

     According to the data plan, add SIP interface 0, and configure the interface attributes.

     ```
     huawei(config)#interface sip 0
       Are you sure to add the SIP interface?(y/n)[n]:y
     huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.20.10.10
     signal-ip
     10.20.10.10 signal-port 5060 transfer udp primary-proxy-ip1 10.20.20.100
     primary-proxy-port 5060
      home-domain huawei sipprofile-index 1
     ```

  5. Reset the SIP interface.

     Reset the SIP interface to make the SIP interface register with the IMS (and to make the modified attributes of the SIP interface take effect) so that the SIP interface can work in the normal state.

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

6. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

   ```
   huawei(config)#board confirm 0/2
   ```

7. Configure the PSTN user data.

   Add POTS users (phones 0-31) to VAG1 so that the users can go online.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/2/0 0/2/31 0 telno 80000000
   huawei(config-esl-user)#quit
   ```

8. Save the data.

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

- Configure VAG2.

1. Add the upstream VLAN interface.

   According to the data plan, configure the IP address of the Layer 3 interface to 10.20.10.11, which facilitates the configuration of the media and signaling IP address pools.

   When you need to connect the VLAN interface to multiple subnets and configure the secondary IP address, use **sub** parameter. The secondary IP address is the same as the primary IP address in function. They are used for Layer 3 forwarding.

   In step **Step 1**, the VLAN is added and the IP address of the VLAN Layer 3 interface is configured. In this step, use the sub parameter to configure the secondary IP address of the VLAN. The secondary IP address is the same as the primary IP address in function. They are used for Layer 3 forwarding.

   ```
   huawei(config)#interface vlanif 30
   huawei(config-if-vlanif30)#ip address 10.20.10.11 24 sub
   huawei(config-if-vlanif30)#quit
   ```

2. Configure the media and signaling IP address pools.

   Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.20.10.11 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.20.10.1.

   ```
   huawei(config)#voip
   huawei(config-voip)#ip address media 10.20.10.11 10.20.10.1
   huawei(config-voip)#ip address signaling 10.20.10.11
   huawei(config-voip)#quit
   ```

3. Configure a static route to the IMS.

   Make sure that the route between the local device and the IMS is reachable. The static route is used as an example. If the static route has been configured, skip this step.

   ```
   huawei(config)#ip route-static 10.20.0.0 255.255.0.0 10.20.10.1
   ```

4. Add a SIP interface.

   According to the data plan, add SIP interface 1, and configure the interface attributes.

   ```
   huawei(config)#interface sip 1
     Are you sure to add the SIP interface?(y/n)[n]:y
   ```

```
huawei(config-if-sip-1)#if-sip attribute basic media-ip 10.20.10.11
signal-ip
10.20.10.11 signal-port 5060 transfer udp primary-proxy-ip1 10.20.20.100
primary-proxy-port 5060
 home-domain huawei sipprofile-index 1
```

5. Reset the SIP interface.

   Reset the SIP interface to make the SIP interface register with the IMS (and to make the modified attributes of the SIP interface take effect) so that the SIP interface can work in the normal state.

```
huawei(config-if-sip-1)#reset
    Are you sure to reset SIP interface?(y/n)[n]:y
```

6. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

```
huawei(config)#board confirm 0/3
```

7. Configure the PSTN user data.

   Add POTS users (phones 0-31) to VAG2 so that the users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/31 1 telno 85000000
huawei(config-esl-user)#quit
```

8. Save the data.

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

----End

Result

After the configuration:

- Users of VAG1 can communicate with each other.
- Users of VAG2 can communicate with each other.
- Users of VAG1 and VAG2 can communicate with each other.

17.4 Example: Configuring the Triple Play

This topic describes how to configure the Triple Play on the MA5600T/MA5603T.

Triple play is a service provisioning mode in which integrated services can be provided to a user. Currently, the prevailing integrated services include the high-speed Internet access service, voice over IP (VoIP) service, and IPTV service.

The early broadband access provides only the high-speed Internet access service. As the Internet is rapidly developing, it can offer much richer services, such as video (IPTV) services. The development of multiple access modes such as ADSL2+ and VDSL2 access, and the improvement of broadband access also lay a solid foundation for provisioning the video service.

PVC Modes for Triple Play Implementation

MA5600T/MA5603T supports the triple play implemented in single-PVC multiple services and multi-PVC multiple services modes.

PVC Mode	Implementation	Application Scenario
Single-PVC for single service	Single-PVC for single service is a triple play mode in which a PVC is adopted for carrying one type of service.	This mode provides only the Internet access service and is used only in early days.
Multi-PVC for multiple services	Multi-PVC for multiple services is a triple play mode in which multiple PVCs are adopted for carrying multiple services from the MA5600T/MA5603T to each DSL user terminal. ● On the user side, three PVCs are used for carrying VoIP, IPTV, and Internet services, and each xDSL port must be configured with at least three PVCs. ● At the network end, three VLANs are created for the upstream interface to carry different types of services.	The home gateway differentiates services based on PVCs. This mode is adopted to utilize the previously-configured services and previously-deployed user terminals.
Single-PVC for multiple services	Single-PVC for multiple services is a triple play mode in which a single PVC is adopted for carrying multiple services from the MA5600T/MA5603T to each DSL user terminal. The MA5600T/MA5603T can differentiate services by the following means: ● Ethernet type (IPoE/PPPoE) ● User-side VLAN ID ● User-side 802.1p value ● 802.1p value + VLAN ID carried in the Ethernet packet ● Ethernet type (IPoE/PPPoE) + VLAN ID	The home gateway differentiates services based on Ethernet parameters such as such as the VLAN ID or the 802.1p priority. This mode is recommended if the home gateway supports the preceding function.

Service Priorities and Bandwidth

The different services have different request on the bandwidth and priority.

- Because the bandwidth and delay of the VoIP service are low, the priority of the VoIP service is the highest among the triple play services.
- Because the bandwidth occupied by the IPTV service is relatively high, and the bit error ratio/packet loss ratio is relatively low, the priority of the IPTV service is lower than that of the VoIP service, but is higher than that of the Internet access service.
- Because common Internet access services, such as web browsing, require neither a strong real-time performance nor a low packet loss ratio, the priority of the high-speed Internet access service is the lowest among the triple play services.

Traffic Management for the Triple Play Services

Traffic management for the triple play includes two modes of rate limitations: stream-based and user (xDSL port)-based. These two modes are implemented on different layers, and therefore can be used together. When implementing the user (xDSL port)-based rate limitation, ensure that the rate limit for the user (xDSL port) must be higher than the aggregated rate limits for all services of the user.

- The stream-based rate limitation

  The stream-based rate limitation is planned based on services, for example, the bandwidth is planned based on the IPTV HD program and the IPTV SD program.
- The user (xDSL port)-based rate limitation

  The user (xDSL port)-based rate limitation is planned based on physical information, such as line quality and number of users per port. The bandwidth for each user is managed in a unified way: Every users' VoIP, IPTV, and Internet services share one user bandwidth, the bandwidth is preferentially allocated to the service with higher priority, and one service burst can hold the total user bandwidth when the other two services carry no traffic.

17.4.1 Configuration Example of the Triple Play (Multi-PVC for Multiple Services)

This topic describes how to configure the triple play in the multi-PVC for multiple services mode. The user home gateway is connected to multiple terminals to implement the access of multiple services such as Internet access service, VoIP service, and IPTV service. Carriers can adopt this mode when they want to use the existing operation, maintenance, and management system for the triple play services.

Prerequisites

- Network devices and lines must be in the normal state.
- The system is working properly.
- The home gateway has been configured. Specifically, permanent virtual channels (PVCs) have been configured on the home gateway for different services.
- The asymmetric digital subscriber line 2 plus (ADSL2+) line template and alarm template that need to be bound to ports have been configured. For details about how to configure the ADSL2+ line template or alarm template, see **4.1.1 Configuring an ADSL2+ Template**.

Service Requirements

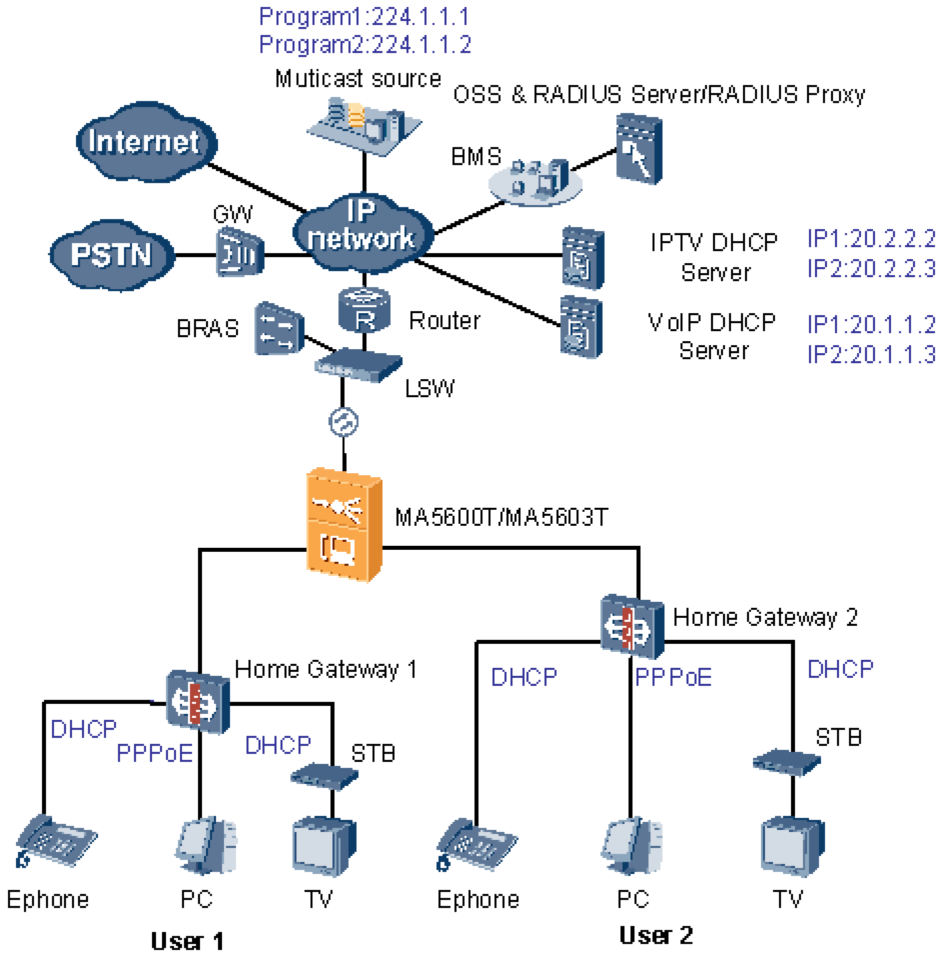
ADSL2+ user 1 and ADSL2+ user 2 are connected to the MA5600T/MA5603T to implement the triple play.

- The PC user accesses the Internet properly.
- The VoIP user makes calls properly.
- The IPTV user watches programs properly.
- After receiving different traffic streams, the MA5600T/MA5603T provides different QoS guarantees to the traffic streams according to the traffic priorities of the PVC.

Networking

Figure 17-23 shows an example network of the triple play service in the multi-PVC for multiple services mode. The Internet service is provided in the PPPoE mode. The VoIP service and the IPTV service are provided in the DHCP mode, obtaining IP addresses from the DHCP server in the standard DHCP mode.

Figure 17-23 Example network of the triple play service in the multi-PVC for multiple services mode



Data Plan

Table 17-16 shows the key data for configuring the triple play in multi-PVC for multiple services mode on the MA5600T/MA5603T.

Table 17-16 Data plan for configuring the triple play in multi-PVC for multiple services mode

Configuration Item	Data			Remarks
	Internet access	**VoIP**	**IPTV**	
Upstream port	0/19 0			-
ADSL2+ port	- User 1: 0/2/1 - User 2: 0/3/1			-

Configuration Item	Data			Remarks
VLAN	● VLAN ID: 2 ● VLAN type: smart	● VLAN ID: 3 ● VLAN type: smart	● VLAN ID: 4 ● VLAN type: smart	-
Traffic profile	● Index: 7 ● CIR: 2 Mbit/s ● Default packet 802.1p priority: 1 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 8 ● CIR: 1 Mbit/s ● Default packet 802.1p priority: 6 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 9 ● No rate limitation ● Default packet 802.1p priority: 5 ● Priority scheduling policy of downstream packets: Local-Setting	As VoIP, IPTV, and Internet services access from the same port, the 802.1p priorities for each service must be configured. These three services are prioritized in descending order as follows: VoIP, IPTV, Internet access.
Service port	● VPI: 0 ● VCI: 37	● VPI: 0 ● VCI: 36	● Index: 100 and 101 ● VPI: 0 ● VCI: 35	The three services have different VCIs.
DHCP relay	-	● Number of the DHCP server group: 1 ● IP address of DHCP server group 1: 20.1.1.2 ● IP address of DHCP server group 2: 20.1.1.3 ● IP address of the VLAN Layer 3 interface: 10.1.1.1/24	● Number of the DHCP server group: 2 ● IP address of DHCP server group 1: 20.2.2.2 ● IP address of DHCP server group 2: 20.2.2.3 ● IP address of the VLAN Layer 3 interface: 10.2.2.1/24	-

Configuration Item	Data			Remarks
Multicast	-	-	● Multicast mode: IGMP Proxy ● Profile 0 of multicast user 2: the right to watch only program BTV-1 ● Multicast upstream port: 0/19/0 ● Multicast IP address of program BTV-1: 224.1.1.1; program source IP address: 10.10.10.10 ● Multicast IP address of program BTV-2: 224.1.1.2; program source IP address: 10.10.10.10	-

Procedure

- Configure the Internet service.
  1. Create a VLAN and add an upstream port to the VLAN.
     ```
     huawei(config)#vlan 2 smart
     huawei(config)#port vlan 2 0/19 0
     ```
  2. Add a traffic profile.
     ```
     huawei(config)#traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
     ```
  3. Add a service port to the VLAN.

     Add a service port to the VLAN 2 and use the traffic profile 7 added in the preceding step.
     ```
     huawei(config)#service-port vlan 2 adsl 0/2/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 2 adsl 0/3/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
     ```
  4. Save the data.
     ```
     huawei(config)#save
     ```
- Configure the VoIP service.

1. Create a VLAN and add an upstream port to the VLAN.

   ```
   huawei(config)#vlan 3 smart
   huawei(config)#port vlan 3 0/19 0
   ```

2. Add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
   ```

3. Add a service port to the VLAN.

   Add a service port to the VLAN 3 and use the traffic profile 8 added in the preceding step.

   ```
   huawei(config)#service-port vlan 3 adsl 0/2/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
   huawei(config)#service-port vlan 3 adsl 0/3/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
   ```

4. Configure the DHCP relay.

   Configure the IP addresses of DHCP server 1 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 1.

   ```
   huawei(config)#dhcp mode layer-3 standard
   huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1 3
   huawei(config)#interface vlanif 3
   huawei(config-if-vlanif3)#ip address 10.1.1.1 24
   huawei(config-if-vlanif3)#dhcp-server 1
   huawei(config-if-vlanif3)#quit
   ```

5. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add an upstream port to the VLAN.

   ```
   huawei(config)#vlan 4 smart
   huawei(config)#port vlan 4 0/19 0
   ```

2. Add a traffic profile.

   ```
   huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy local-Setting
   ```

3. Add a service port to the VLAN.

   CAUTION

   On the MA5600T/MA5603T, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

   Add a service port to VLAN 4 and use traffic profile 9.

   ```
   huawei(config)#service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
   huawei(config)#service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
   ```

4. Configure the DHCP relay.

   Configure the IP address of DHCP server 2 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 2.

   ```
   huawei(config)#dhcp mode layer-3 standard
   huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
   huawei(config)#interface vlanif 4
   huawei(config-if-vlanif4)#ip address 10.2.2.1 24
   ```

```
huawei(config-if-vlanif4)#dhcp-server 2
huawei(config-if-vlanif4)#quit
```

5. Configure the multicast data.

   Configure the multicast mode, authority profile, multicast upstream port, and multicast program. Add multicast user 1 and multicast user 2 to multicast VLAN 4.

```
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4)#igmp uplink-port 0/19/0
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp program add name BTV-1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4)#igmp program add name BTV-2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add service-port 100 no-auth
huawei(config-btv)#igmp user add service-port 101 auth
huawei(config-btv)#igmp user bind-profile service-port 101 profile-name
profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4)#quit
```

6. Save the data.

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

----End

Result

After the related upstream device and downstream device are configured, the triple play service (Internet, VoIP, and IPTV services) is available.

- Internet: user 1 and user 2 can access the Internet through PPPoE dialup.
- VoIP: user 1 and user 2 can call each other.
- IPTV: user 1 can watch all the programs after being connected to port 0/2/1, and user 2 can watch only program BTV-1 after being connected to port 0/3/1.

Configuration File

Internet:

```
vlan 2 smart
port vlan 0/19 0
traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
service-port vlan 2 adsl 0/2/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
service-port vlan 2 adsl 0/3/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
save  //Save the configuration.
```

VoIP:

```
vlan 3 smart
port vlan 3 0/19 0
```

```
traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
service-port vlan 3 adsl 0/2/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
service-port vlan 3 adsl 0/3/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
interface vlanif 3
ip address 10.1.1.1 24
dhcp-server 1
quit
save  //Save the configuration.
```

IPTV:

```
vlan 4 smart
port vlan 4 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
dhcp mode layer-3 standard
dhcp-server 2 ip 20.2.2.2 20.2.2.3
interface vlanif 4
ip address 10.2.2.1 24
dhcp-server 2
quit
multicast-vlan 4
igmp mode proxy
igmp uplink-port 0/19/0
btv
igmp uplink-port-mode default
quit
multicast-vlan 4
igmp program add name BTV-1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.2 sourceip 10.10.10.10
btv
igmp profile profile-name profile0 program-name BTV-1 watch
igmp policy service-port 100 normal
igmp policy service-port 101 normal
igmp user add service-port 100 no-auth
igmp user add service-port 101 auth
igmp user bind-profile service-port 101 profile-name profile0
multicast-vlan 4
igmp multicast-vlan member service-port 100
igmp multicast-vlan member service-port 101
quit
save  //Save the configuration.
```

17.4.2 Configuration Example of the Triple Play (Single-PVC for Multiple Services) - Stream-based Rate Limitation

This topic describes how to configure the triple play in the single-PVC for multiple services mode. The user home gateway is connected to multiple terminals to implement the access of multiple services such as Internet access service, VoIP service, and IPTV service.

Prerequisites

- Network devices and lines must be in the normal state.
- The system is working properly.
- The home gateway has been configured. Specifically, virtual local area networks (VLANs) have been configured on the home gateway for different services.
- The asymmetric digital subscriber line 2 plus (ADSL2+) line template and alarm template that need to be bound to ports have been configured. For details about how to configure

the ADSL2+ line template or alarm template, see **4.1.1 Configuring an ADSL2+ Template**.

Service Requirements

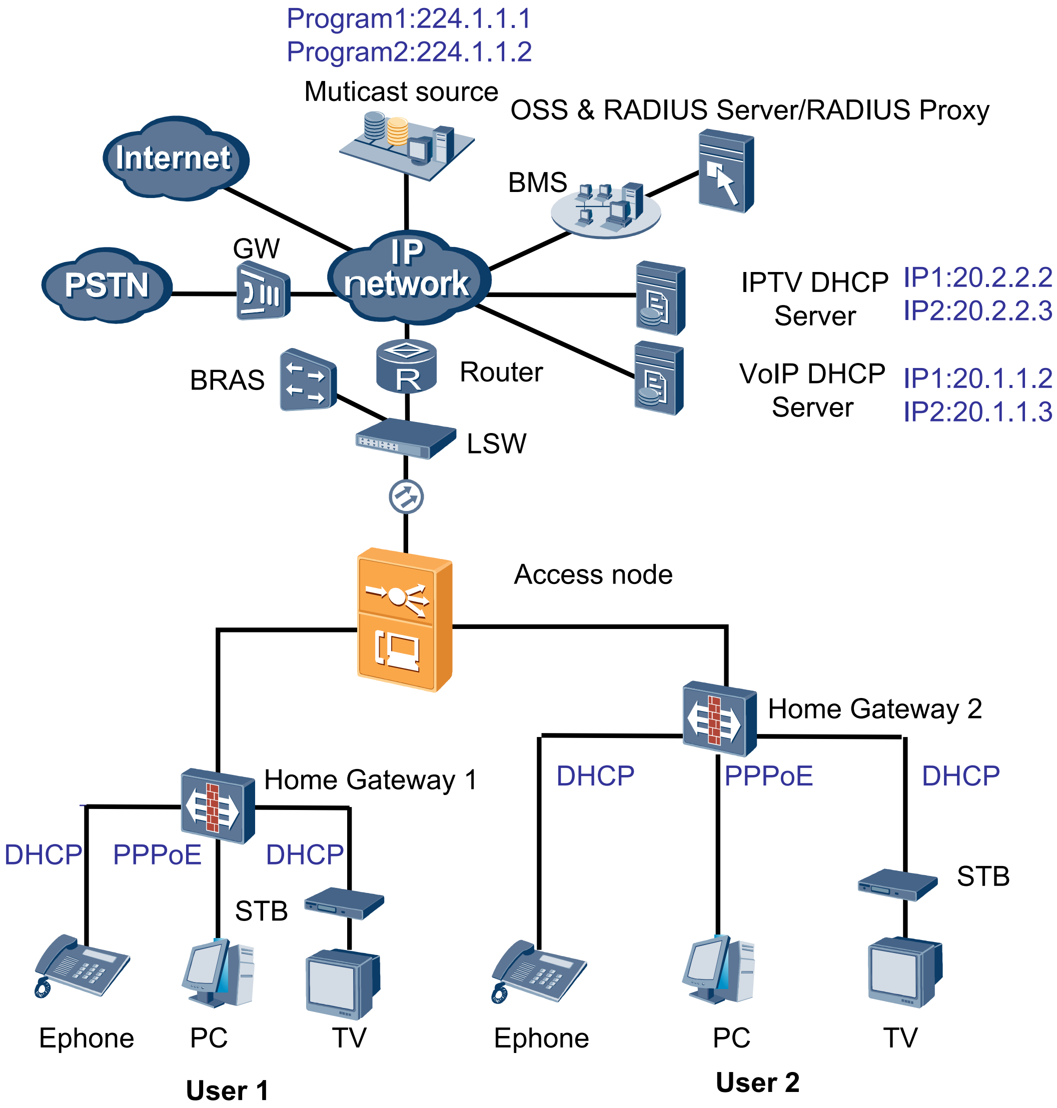
ADSL2+ user 1 and ADSL2+ user 2 are connected to the MA5600T/MA5603T to implement the triple play.

- The PC user accesses the Internet properly.
- The VoIP user makes calls properly.
- The IPTV user watches programs properly.
- After receiving different traffic streams through the same PVC, the MA5600T/MA5603T provides different QoS guarantees to the traffic streams according to the user-side VLANs.

Networking

Figure 17-24 shows an example network of the triple play service in the single-PVC for multiple services mode. The Internet service is accessed in the PPPoE mode. The VoIP service and the IPTV service are provided in the DHCP mode, obtaining IP addresses from the DHCP server in the standard DHCP mode.

Figure 17-24 Example network of the triple play service in the single-PVC for multiple services mode



Data Plan

Table 17-17 shows the key data for configuring the triple play in single-PVC for multiple services mode on the MA5600T/MA5603T.

Table 17-17 Data plan for configuring the triple play in single-PVC for multiple services mode (stream-based rate limitation)

Configuration Item	Data			Remarks
	Internet access	**VoIP**	**IPTV**	

Configuration Item	Data			Remarks
Upstream port	0/19 0			-
ADSL2+ port	● User 1: 0/2/1 ● User 2: 0/3/1			-
VLAN	● SVLAN ID: 2 ● SVLAN type: smart ● CVLAN ID: 20	● SVLAN ID: 3 ● SVLAN type: smart ● CVLAN ID: 30	● SVLAN ID: 4 ● SVLAN type: smart ● CVLAN ID: 40	-
Traffic profile	● Index: 7 ● CIR: 2 Mbit/s ● Default packet 802.1p priority: 1 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 8 ● CIR: 1 Mbit/s ● Default packet 802.1p priority: 6 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 9 ● No rate limitation ● Default packet 802.1p priority: 5 ● Priority scheduling policy of downstream packets: Local-Setting	As VoIP, IPTV, and Internet services access from the same port, the 802.1p priorities for each service must be configured. These three services are prioritized in descending order as follows: VoIP, IPTV, Internet access.
Service port	● VPI: 0 ● VCI: 35	● VPI: 0 ● VCI: 35	● Index: 100 and 101 ● VPI: 0 ● VCI: 35	The three services have different VCIs.

Configuration Item	Data			Remarks
DHCP relay	-	● Number of the DHCP server group: 1 ● IP address of DHCP server group 1: 20.1.1.2 ● IP address of DHCP server group 2: 20.1.1.3 ● IP address of the VLAN Layer 3 interface: 10.1.1.1/24	● Number of the DHCP server group: 2 ● IP address of DHCP server group 1: 20.2.2.2 ● IP address of DHCP server group 2: 20.2.2.3 ● IP address of the VLAN Layer 3 interface: 10.2.2.1/24	-
Multicast	-	-	● Multicast mode: IGMP Proxy ● Profile 0 of multicast user 2: the right to watch only program BTV-1 ● Multicast upstream port: 0/19/0 ● Multicast IP address of program BTV-1: 224.1.1.1; program source IP address: 10.10.10.10 ● Multicast IP address of program BTV-2: 224.1.1.2; program source IP address: 10.10.10.10	-

Procedure

- Configure the Internet service.

1. Create a VLAN and add an upstream port to the VLAN.

   ```
   huawei(config)#vlan 2 smart
   huawei(config)#port vlan 2 0/19 0
   ```

2. Add a traffic profile.

   ```
   huawei(config)#traffic table ip index 7 cir 2048 priority 1 priority-
   policy local-Setting
   ```

3. Add a service port to the VLAN.

   Add a service port to VLAN 2 and use the traffic profile added 7 in the preceding step.

   ```
   huawei(config)#service-port vlan 2 adsl 0/2/1 vpi 0 vci 35 multi-service
   user-vlan 20 rx-cttr 7 tx-cttr 7
   huawei(config)#service-port vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service
   user-vlan 20 rx-cttr 7 tx-cttr 7
   ```

4. Save the data.

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

- Configure the VoIP service.

1. Create a VLAN and add an upstream port to the VLAN.

   ```
   huawei(config)#vlan 3 smart
   huawei(config)#port vlan 3 0/19 0
   ```

2. Add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir 1024 priority 6 priority-
   policy local-Setting
   ```

3. Add a service port to the VLAN.

   Add a service port to the VLAN 3 and use the traffic profile 8 added in the preceding step.

   ```
   huawei(config)#service-port vlan 3 adsl 0/2/1 vpi 0 vci 35 multi-service
   user-vlan 30 rx-cttr 8 tx-cttr 8
   huawei(config)#service-port vlan 3 adsl 0/3/1 vpi 0 vci 35 multi-service
   user-vlan 30 rx-cttr 8 tx-cttr 8
   ```

   NOTE

   The video and voice services have stricter requirements on delay. You can run the **bind channel** command to bind them to a low delay channel. Currently, this command is available for only the VDSL port.

4. Configure the DHCP relay.

   Configure the IP addresses of DHCP server 1 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 1.

   ```
   huawei(config)#dhcp mode layer-3 standard
   huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1 3
   huawei(config)#interface vlanif 3
   huawei(config-if-vlanif3)#ip address 10.1.1.1 24
   huawei(config-if-vlanif3)#dhcp-server 1
   huawei(config-if-vlanif3)#quit
   ```

5. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add an upstream port to the VLAN.

   ```
   huawei(config)#vlan 4 smart
   huawei(config)#port vlan 4 0/19 0
   ```

2. Add a traffic profile.

   ```
   huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
   local-Setting
   ```

3. Add a service port to the VLAN.

   ⚠ **CAUTION**

   On the MA5600T/MA5603T, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

   Add a service port to VLAN 4 and use traffic profile 9.

```
huawei(config)#service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 multi-
service user-vlan 40 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 multi-
service user-vlan 40 rx-cttr 9 tx-cttr 9
```

4. Configure the DHCP relay.

   Configure the IP addresses of DHCP server 2 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 2.

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 10.2.2.1 24
huawei(config-if-vlanif4)#dhcp-server 2
huawei(config-if-vlanif4)#quit
```

5. Configure the multicast data.

   Configure the multicast mode, authority profile, multicast upstream port, and multicast program. Add multicast user 1 and multicast user 2 to multicast VLAN 4.

```
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4)#igmp uplink-port 0/19/0
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp program add name BTV-1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4)#igmp program add name BTV-2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add service-port 100 no-auth
huawei(config-btv)#igmp user add service-port 101 auth
huawei(config-btv)#igmp user bind-profile service-port 101 profile-name
profile0
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp multicast-vlan member port 0/2/1
huawei(config-mvlan4)#igmp multicast-vlan member port 0/3/1
huawei(config-mvlan4)#quit
```

6. Save the data.

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

----End

Result

After the related upstream device and downstream device are configured, the triple play service (Internet, VoIP, and IPTV services) is available.

- Internet: user 1 and user 2 can access the Internet through PPPoE dialup.
- VoIP: user 1 and user 2 can call each other.
- IPTV: user 1 can watch all the programs after being connected to port 0/2/1, and user 2 can watch only program BTV-1 after being connected to port 0/3/1.

Configuration File

Internet:

```
vlan 2 smart
port vlan 0/19 0
traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
service-port vlan 2 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-
cttr 7
service-port vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-
cttr 7
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
save
```

VoIP:

```
vlan 3 smart
port vlan 3 0/19 0
traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
service-port vlan 3 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-
cttr 8
service-port vlan 3 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-
cttr 8
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
interface vlanif 3
ip address 10.1.1.1 24
dhcp-server 1
quit
save
```

IPTV:

```
vlan 4 smart
port vlan 4 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 40 rx-cttr
9 tx-cttr 9
service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 40 rx-cttr
9 tx-cttr 9
dhcp mode layer-3 standard
dhcp-server 2 ip 20.2.2.2 20.2.2.3
interface vlanif 4
ip address 10.2.2.1 24
dhcp-server 2
quit
multicast-vlan 4
igmp mode proxy
igmp uplink-port 0/19/0
btv
igmp uplink-port-mode default
multicast-vlan 4
igmp program add name BTV-1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.2 sourceip 10.10.10.10
btv
igmp profile profile-name profile0 program-name BTV-1 watch
igmp policy service-port 100 normal
igmp policy service-port 101 normal
igmp user add service-port 100 no-auth
igmp user add service-port 101 auth
igmp user bind-profile service-port 101 profile-name profile0
```

```
multicast-vlan 4
igmp multicast-vlan member service-port 100
igmp multicast-vlan member service-port 101
quit
save
```

17.4.3 Configuration Example of the Triple Play Service (Single-PVC for Multiple Services) - User-based and Stream-based Rate Limitation

This topic describes how to configure the triple play service in the single-PVC for multiple services mode. The user home gateway is connected to multiple terminals to implement the access of multiple services such as Internet access, VoIP, and IPTV services and perform user-based and stream-based rate limitation.

Prerequisites

- Network devices and lines must be in the normal state.
- The system is working properly.
- The home gateway has been configured. Specifically, virtual local area networks (VLANs) have been configured on the home gateway for different services.
- The asymmetric digital subscriber line 2 plus (ADSL2+) line template and alarm template that need to be bound to ports have been configured. For details about how to configure the ADSL2+ line template or alarm template, see **4.1.1 Configuring an ADSL2+ Template**.

Service Requirements

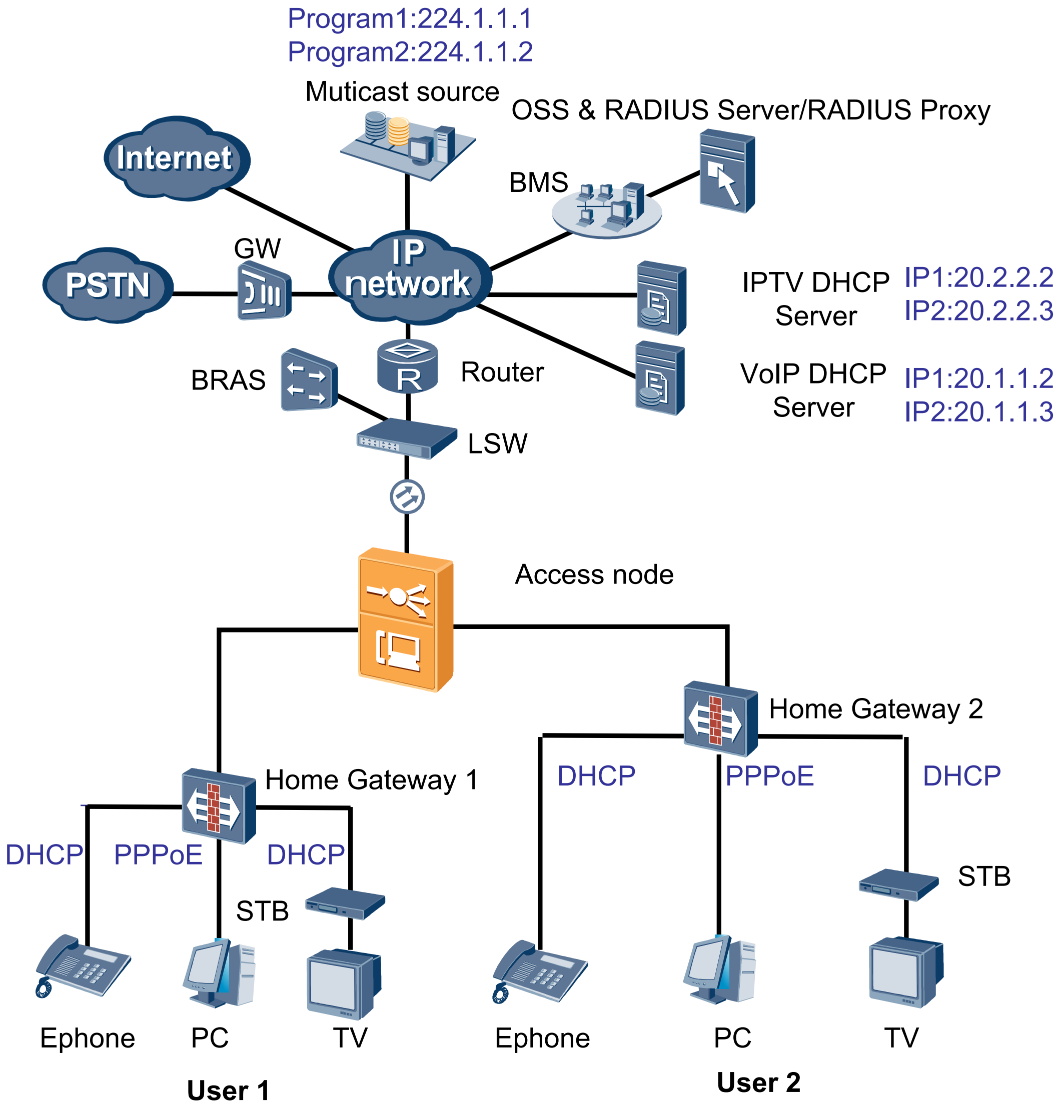
ADSL2+ user 1 and ADSL2+ user 2 are connected to the MA5600T/MA5603T to implement the triple play.

- The PC user accesses the Internet properly.
- The VoIP user makes calls properly.
- The IPTV user watches programs properly.
- The maximum bandwidth of each user is 10 Mbit/s, adopting user-based bandwidth management: The Internet access, VoIP, and IPTV services of each user share the same total bandwidth and the QoS scheduling is implemented. The service priorities are VoIP (the value is 6), IPTV (the value is 5), and Internet access (the value is 1) in descending order. If any two services carry no traffic, the third service can hold a burst of the total user bandwidth.
- After receiving different traffic streams through the same PVC, the MA5600T/MA5603T provides different QoS guarantees to the traffic streams according to the user-side VLANs.

Networking

Figure 17-25 shows an example network of the triple play in the single PVC for multiple services mode. The Internet service is accessed in the PPPoE mode. The VoIP service and the IPTV service are provided in the DHCP mode, obtaining IP addresses from the DHCP server in the standard DHCP mode.

Figure 17-25 Example network of the triple play service in the single-PVC for multiple services mode



Data Plan

Table 17-18 shows the key data for configuring the triple play in single-PVC for multiple services mode on the MA5600T/MA5603T.

Table 17-18 Data plan for configuring the triple play in single-PVC for multiple services mode (user-based and stream-based rate limitation)

Configuration Item	Data			Remarks
	Internet access	**VoIP**	**IPTV**	

Configuration Item	Data			Remarks
Upstream port	0/19 0			-
ADSL2+ port	● User 1: 0/2/0 ● User 2: 0/2/1 ● ADSL2+ channel profile – ID: 3 – Minimum upstream/downstream rates: 32 kbit/s – Minimum reserved upstream/downstream rate: 32 kbit/s – Maximum upstream rate: 4096 kbit/s – Maximum downstream rate: 10240 kbit/s ● ADSL2+ line template: – ID: 3 – Upstream/Downstream rate adaptation ratio of channel: 100 ● ADSL2+ line alarm template ID: 1			-
VLAN	● SVLAN ID: 2 ● SVLAN type: smart ● CVLAN ID: 20	● SVLAN ID: 3 ● SVLAN type: smart ● CVLAN ID: 30	● SVLAN ID: 4 ● SVLAN type: smart ● CVLAN ID: 40	-

Configuration Item	Data			Remarks
Traffic profile	● Index: 7 ● CIR: 2 Mbit/s ● PIR: 10 Mbit/s ● Default packet 802.1p priority: 1 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 8 ● CIR: 1 Mbit/s ● PIR: 10 Mbit/s ● Default packet 802.1p priority: 6 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 9 ● CIR: 4 Mbit/s ● PIR: 10 Mbit/s ● Default packet 802.1p priority: 5 ● Priority scheduling policy of downstream packets: Local-Setting	As VoIP, IPTV, and Internet services access from the same port, the 802.1p priorities for each service must be configured. These three services are prioritized in descending order as follows: VoIP, IPTV, Internet access. The PIR and maximum user bandwidth must be the same.
Service port	● VPI: 0 ● VCI: 35	● VPI: 0 ● VCI: 35	● Index: 100 and 101 ● VPI: 0 ● VCI: 35	The three services have different VCIs.
DHCP relay	-	● Number of the DHCP server group: 1 ● IP address of DHCP server group 1: 20.1.1.2 ● IP address of DHCP server group 2: 20.1.1.3 ● IP address of the VLAN Layer 3 interface: 10.1.1.1/24	● Number of the DHCP server group: 2 ● IP address of DHCP server group 1: 20.2.2.2 ● IP address of DHCP server group 2: 20.2.2.3 ● IP address of the VLAN Layer 3 interface: 10.2.2.1/24	-

Configuration Item	Data			Remarks
Multicast	-	-	● Multicast mode: IGMP Proxy ● Profile 0 of multicast user 2: the right to watch only program BTV-1 ● Multicast upstream port: 0/19/0 ● Multicast IP address of program BTV-1: 224.1.1.1; program source IP address: 10.10.10.10 ● Multicast IP address of program BTV-2: 224.1.1.2; program source IP address: 10.10.10.10	-

Procedure

- Configure user bandwidth management.

  For relevant background and configuration guide, see **Configuring User-based Rate Limitation**.

  1. Configure ADSL channel profile 3 with a minimum upstream/downstream transmission rate 32 kbit/s, a minimum upstream/downstream reserved rate 32 kbit/s, a maximum downstream transmission rate 10240 kbit/s and a maximum upstream transmission rate 4096 kbit/s.

     ```
     huawei(config)#adsl channel-profile quickadd 3 rate 32 32 10240 32 32
     4096
     ```

  2. Configure ADSL line template 3 by binding channel profile 3.

     ```
     huawei(config)#adsl line-template quickadd 3 channel1 3 100 100
     ```

- Bind ADSL line template 3 created in the previous step to ADSL ports 0/2/0 and 0/2/1. Activate the ports.

  ```
  huawei(config)#interface adsl 0/2
  huawei(config-if-adsl-0/2)#deactivate 0
  huawei(config-if-adsl-0/2)#deactivate 1
  huawei(config-if-adsl-0/2)#activate 0 template-index 3
  huawei(config-if-adsl-0/2)#activate 1 template-index 3
  huawei(config-if-adsl-0/2)#alarm-config 0 1
  ```

```
huawei(config-if-adsl-0/2)#alarm-config 1 1
huawei(config-if-adsl-0/2)#quit
```

- Configure the queue scheduling mode of the port.

  Configure the queue scheduling mode of the port to priority queuing (PQ).

  ```
  huawei(config)#queue-scheduler strict-priority
  ```

- Configure the Internet access service.

  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 2 smart
     huawei(config)#port vlan 2 0/19 0
     ```

  2. Configure a traffic profile.

     ```
     huawei(config)#traffic table ip index 7 cir 2048 pir 10240 priority 1
     priority-
     policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Create service virtual port, the S-VLAN ID to 2, the C-VLAN ID to 20, the VPI/VCI to 0/35 and use the traffic profile 7 added in the preceding step.

     ```
     huawei(config)#service-port vlan 2 adsl 0/2/0 vpi 0 vci 35
     multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 2 adsl 0/2/1 vpi 0 vci 35
     multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
     ```

  4. Save the data.

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

- Configure the VoIP service.

  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 3 smart
     huawei(config)#port vlan 3 0/19 0
     ```

  2. Configure a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir 1024 pir 10240 priority 6
     priority-policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Create service virtual port, the S-VLAN ID to 3, the C-VLAN ID to 30, the VPI/VCI to 0/35 and use the traffic profile 8added in the preceding step.

     ```
     huawei(config)#service-port vlan 3 adsl 0/2/0 vpi 0 vci 35
     multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
     huawei(config)#service-port vlan 3 adsl 0/2/1 vpi 0 vci 35
     multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
     ```

     NOTE

     The video and voice services have stricter requirements on delay. You can run the **bind channel** command to bind them to a low delay channel. Currently, this command is available for only the VDSL2 port.

  4. Configure the DHCP relay.

     Configure the IP addresses of DHCP server 1 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 1.

     ```
     huawei(config)#dhcp mode layer-3 standard
     huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1 3
     huawei(config)#interface vlanif 3
     huawei(config-if-vlanif3)#ip address 10.1.1.1 24
     huawei(config-if-vlanif3)#dhcp-server 1
     huawei(config-if-vlanif3)#quit
     ```

  5. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add an upstream port to the VLAN.

   ```
   huawei(config)#vlan 4 smart
   huawei(config)#port vlan 4 0/19 0
   ```

2. Configure a traffic profile.

   ```
   huawei(config)#traffic table ip index 9 cir 4096 pir 10240 priority 5
   priority-policy local-Setting
   ```

3. Add a service port to the VLAN.

   CAUTION

   On the MA5600T/MA5603T, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

   Create service virtual port, and use the traffic profile 9 added in the preceding step.

   ```
   huawei(config)#service-port 100 vlan 4 adsl 0/2/0 vpi 0 vci 35
   multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
   huawei(config)#service-port 101 vlan 4 adsl 0/2/1 vpi 0 vci 35
   multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
   ```

4. Configure the DHCP relay.

   Configure the IP addresses of DHCP server 2 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 2.

   ```
   huawei(config)#dhcp mode layer-3 standard
   huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
   huawei(config)#interface vlanif 4
   huawei(config-if-vlanif4)#ip address 10.2.2.1 24
   huawei(config-if-vlanif4)#dhcp-server 2
   huawei(config-if-vlanif4)#quit
   ```

5. Configure the multicast data.

   Configure the multicast mode, authority profile, multicast upstream port, and multicast program. Add multicast user 1 and multicast user 2 to multicast VLAN 4.

   ```
   huawei(config)#multicast-vlan 4
   huawei(config-mvlan4)#igmp mode proxy
     Are you sure to change IGMP mode?(y/n)[n]:y
   huawei(config-mvlan4)#igmp uplink-port 0/19/0
   huawei(config-mvlan4)#btv
   huawei(config-btv)#igmp uplink-port-mode default
   Are you sure to change the uplink port mode?(y/n)[n]:y
   huawei(config-btv)#quit
   huawei(config)#multicast-vlan 4
   huawei(config-mvlan4)#igmp program add name BTV-1 ip 224.1.1.1 sourceip
   10.10.10.10
   huawei(config-mvlan4)#igmp program add name BTV-2 ip 224.1.1.2 sourceip
   10.10.10.10
   huawei(config-mvlan4)#btv
   huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
   watch
   huawei(config-btv)#igmp policy service-port 100 normal
   huawei(config-btv)#igmp policy service-port 101 normal
   huawei(config-btv)#igmp user add port service-port 100 auth
   huawei(config-btv)#igmp user add port service-port 101 auth
   huawei(config-btv)#igmp user bind-profile service-port 100 profile-name
   profile0
   huawei(config-btv)#multicast-vlan 4
   huawei(config-mvlan4)#igmp multicast-vlan member service-port 100
   ```

```
huawei(config-mvlan4)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4)#quit
```

6. Save the data.

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

----End

Result

After the relevant upstream device and downstream device are configured, the triple play service (Internet access, VoIP, and IPTV services) is available. If any two services carry no traffic, the third service can hold a burst of the total user bandwidth.

- Internet: user 1 and user 2 can access the Internet through PPPoE dialup.
- VoIP: user 1 and user 2 can call each other.
- IPTV: user 1 can watch all the programs after being connected to port 0/2/0, and user 2 can watch only program BTV-1 after being connected to port 0/2/1.

Configuration File

```
adsl channel-profile quickadd 3 rate 32 32 10240 32 32 4096
adsl line-template quickadd 3 channel1 3 100 100
queue-scheduler strict-priority
interface adsl 0/2
deactivate 0
deactivate 1
activate 0 template-index 3
activate 1 template-index 3
alarm-config 0 1
alarm-config 1 1
quit
```

Internet:

```
vlan 2 smart
port vlan 0/19 0
traffic table ip index 7 cir 10240 priority 1 priority-policy local-Setting
service-port vlan 2 adsl 0/2/0
vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
service-port vlan 2 adsl 0/2/1
vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
save
```

VoIP:

```
vlan 3 smart
port vlan 3 0/19 0
traffic table ip index 8 cir 10240 priority 6 priority-policy local-Setting
service-port vlan 3 adsl 0/2/0
vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
service-port vlan 3 adsl 0/2/1
vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
interface vlanif 3
ip address 10.1.1.1 24
dhcp-server 1
quit
save
```

IPTV:

```
vlan 4 smart
port vlan 4 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 100 vlan 4 adsl  0/2/0
vpi 0 vci 35 multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
service-port 101 vlan 4 adsl 0/2/1
 vpi 0 vci 35 multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
dhcp mode layer-3 standard
dhcp-server 2 ip 20.2.2.2 20.2.2.3
interface vlanif 4
ip address 10.2.2.1 24
dhcp-server 2
quit
multicast-vlan 4
igmp mode proxy
igmp uplink-port 0/19/0
btv
igmp uplink-port-mode default
quit
multicast-vlan 4
igmp program add name BTV-1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.2 sourceip 10.10.10.10
btv
igmp profile profile-name profile0 program-name BTV-1 watch
igmp policy service-port 100 normal
igmp policy service-port 101 normal
igmp user add service-port 100 no-auth
igmp user add service-port 101 auth
igmp user bind-profile service-port 100 profile-name profile0
multicast-vlan 4
igmp multicast-vlan member service-port 100
igmp multicast-vlan member service-port 101
quit
save
```

18 Example: Configuring the Private Line Service

About This Chapter

A private line service refers to a service carried over a true or virtual private line on the public network for transparent transmission and for access of private network services. This topic describes how to configure the private line service.

Context

The MA5600T/MA5603T supports the following private line services:

- PWE3 private line service
- TDM SHDSL access service
- QinQ VLAN private line service

service, users are assigned specific timeslots of an E1 line, and therefore can share the bandwidth of the E1 line, hence saving the E1 line lease expense.

18.1 Example: Configuring the QinQ VLAN

The QinQ-VLAN-based private line service can achieve the interconnection and secure communication among branches in different areas within the enterprise private network.

Prerequisites

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

- An enterprise requires to achieve the interconnection and secure communication between its headquarters and the branches located in different areas through Layer 2 switching network, and to isolate the data of different departments.
- The access device uses xDSL or LAN access.

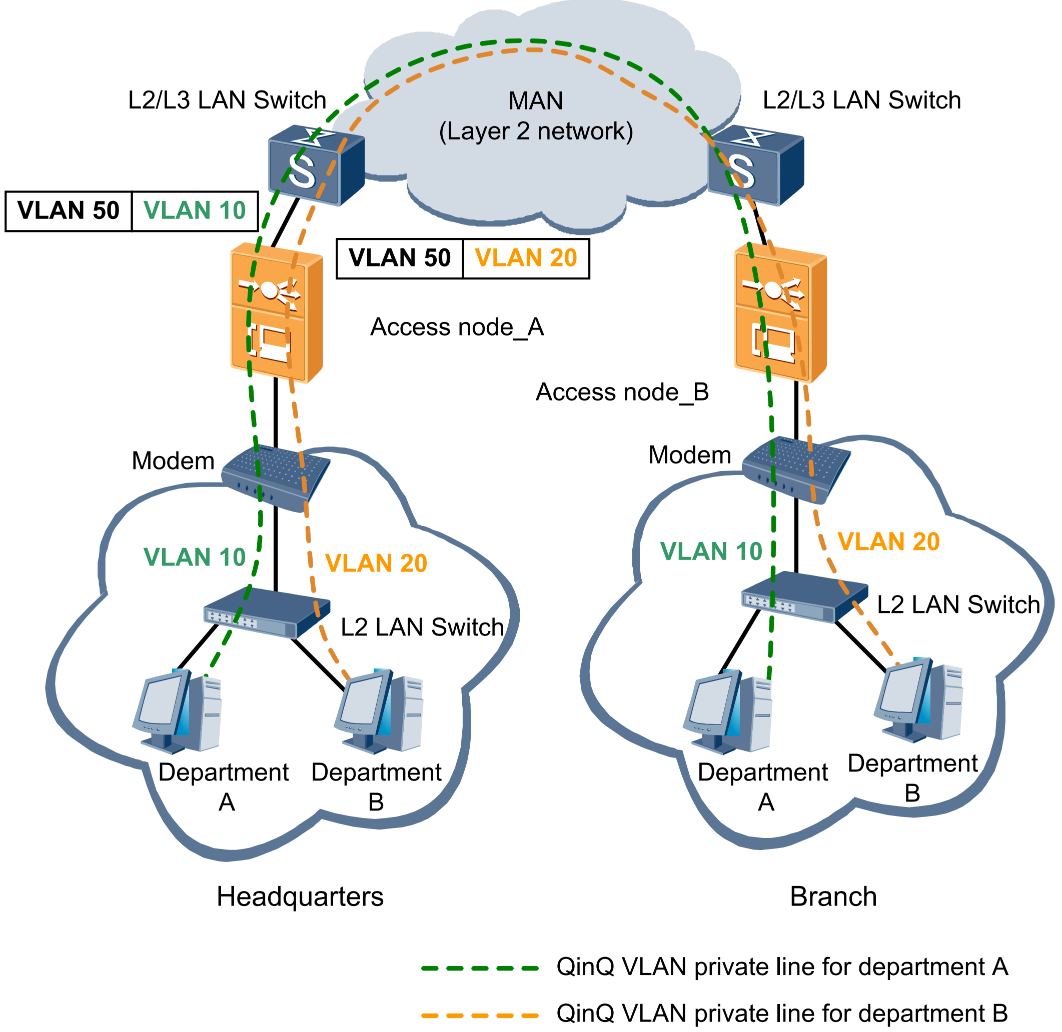
Networking

Figure 18-1 shows an example network for configuring the private line service.

The two branches of the enterprise are connected to the (metropolitan area network) MAN through the MA5600T/MA5603T. The upper-layer network must work in the Layer 2 mode, and must forward packets according to the VLAN and the MAC address.

On the MA5600T/MA5603T, the attribute of the upstream VLAN of user packets is configured as QinQ private line service. A VLAN tunnel is created in Layer 2/Layer 3 MAN for transmitting user data carrying the VLAN tag. Different VLAN IDs are used for different departments to achieve user isolation and data security. In this way, the service packets of the enterprise private network can be transparently transmitted through the public network, and the two branches can communicate with each other securely.

Figure 18-1 Example network for configuring the private line service



The configuration on MA5600T/MA5603T_A is the same as the configuration on MA5600T/MA5603T_B. The following uses the configuration on MA5600T/MA5603T_A and VDSL2 access as examples to describe how to configure the private line service implemented through a QinQ VLAN.

Data Plan

Table 18-1 lists the key data planning of the QinQ VLAN private line service on MA5600T/MA5603T_A.

Table 18-1 Data plan for configuring the QinQ VLAN private line service

Item	Data	Remarks
VLAN	● VLAN ID: 50 ● VLAN type: smart VLAN ● VLAN attribute: QinQ	The public network VLAN, namely outer VLAN, is configured here. The inner VLAN belongs to the enterprise private network, which can be planned by the enterprise self.
Transparent transmission of Layer 2 packets	Enable the transparent transmission of BPDUs.	This function is mainly used in the QinQ service to provide a transparent and secure data channel for the enterprise branches located in two places within the enterprise private network. After the transparent transmission of BPDUs is enabled, the Layer 2 protocol packets of a private network can be transparently transmitted through the public network.
Upstream port	0/19/0	-
Traffic profile	● Traffic profile ID: 10 ● CIR: 4 Mbit/s ● Priority copy policy: user-cos ● Default 802.1p priority of the packet: 4 ● Priority-based scheduling policy of the downstream packets: local-setting	The CIR depends on the user bandwidth requirement.
VDSL2 port	● VDSL2 port ID: 0/2/0 ● Default VDSL2 line profile: 1 ● Default VDSL2 alarm profile: 1	-
Service virtual port	● VLAN ID: 50 ● Service port: 0/2/0 ● VDSL channel mode: ATM ● VPI: 0 ● VCI: 35 ● ID of the traffic profile in Rx direction: 10 ● ID of the traffic profile in Tx direction: 10	● The VPI/VCI is the same as the management VPI/VCI on the peer modem. ● The traffic profile that meets the service requirement is used.

Procedure

Step 1 Create a VLAN.

The VLAN ID is 50, and the VLAN is a smart VLAN.

```
huawei(config)#vlan 50 smart
```

Step 2 Set the VLAN attribute to QinQ.

```
huawei(config)#vlan attrib 50 q-in-q
```

Step 3 Enable the transparent transmission of BPDUs.

Enable the transparent transmission of BPDUs so that the Layer 2 protocol packets of a private network can be transparently transmitted through the public network. By default, the transparent transmission of BPDUs is disabled.

```
huawei(config)#bpdu tunnel vlan 50 enable
```

Step 4 Add an upstream port to the VLAN.

Add upstream port 0/19/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/19 0
```

Step 5 Add a traffic profile.

The profile ID is 10, the CIR is 4 Mbit/s, and packets are scheduled according to the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 10 cir 4096 priority user-cos 4 priority-
policy
 local-Setting
```

Step 6 Activate the VDSL2 port and bind a profile to it.

Use the default VDSL2 line profile 1. Activate port 0/2/0 and bind alarm profile 1 to port 0/2/0.

NOTE

- By default, the VDSL port is in the activated state. Before binding a profile to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#deactivate 0
huawei(config-if-vdsl-0/2)#activate 0 template-index 1
huawei(config-if-vdsl-0/2)#alarm-config 0 1
huawei(config-if-vdsl-0/2)#quit
```

Step 7 Add a service port to the VLAN.

Add a service port to the VLAN 50, and use traffic profile 10 that meets the service requirements. The VPI and the VCI are 0 and 35 respectively, the same as those on the peer modem. The user port is 0/2/0. The VDSL channel is in ATM mode.

```
huawei(config)#service-port vlan 50 vdsl mode atm 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-
cttr 10
```

Step 8 Save the data.

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

----End

Result

After the configuration, the two branches of the enterprise can communicate with each other.

Configuration File

```
vlan 50 smart
vlan attrib 50 q-in-q
port vlan 50 0/19 0
bpdu tunnel vlan 50 enable
traffic table ip index 10 cir 4096 priority user-cos 4 priority-policy local-
Setting
interface vdsl 0/2
deactivate 0
activate 0 template-index 1
alarm-config 0 1
quit
service-port vlan 50 vdsl mode atm 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
save
```

18.2 Example: Configuring VLAN Stacking Multi-ISP Wholesale Access

In a Layer-2 switching metropolitan area network (MAN), there are multiple Internet service providers (ISPs). To provision the services provided by the ISP to the specified user group rapidly, the outer VLAN tags of VLAN stacking can be used to identify ISPs, while the inner VLAN tags to identify users. In this way, different user groups can be connected to the specified ISPs in batches through different outer VLAN tags to obtain services from the ISPs.

Prerequisites

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

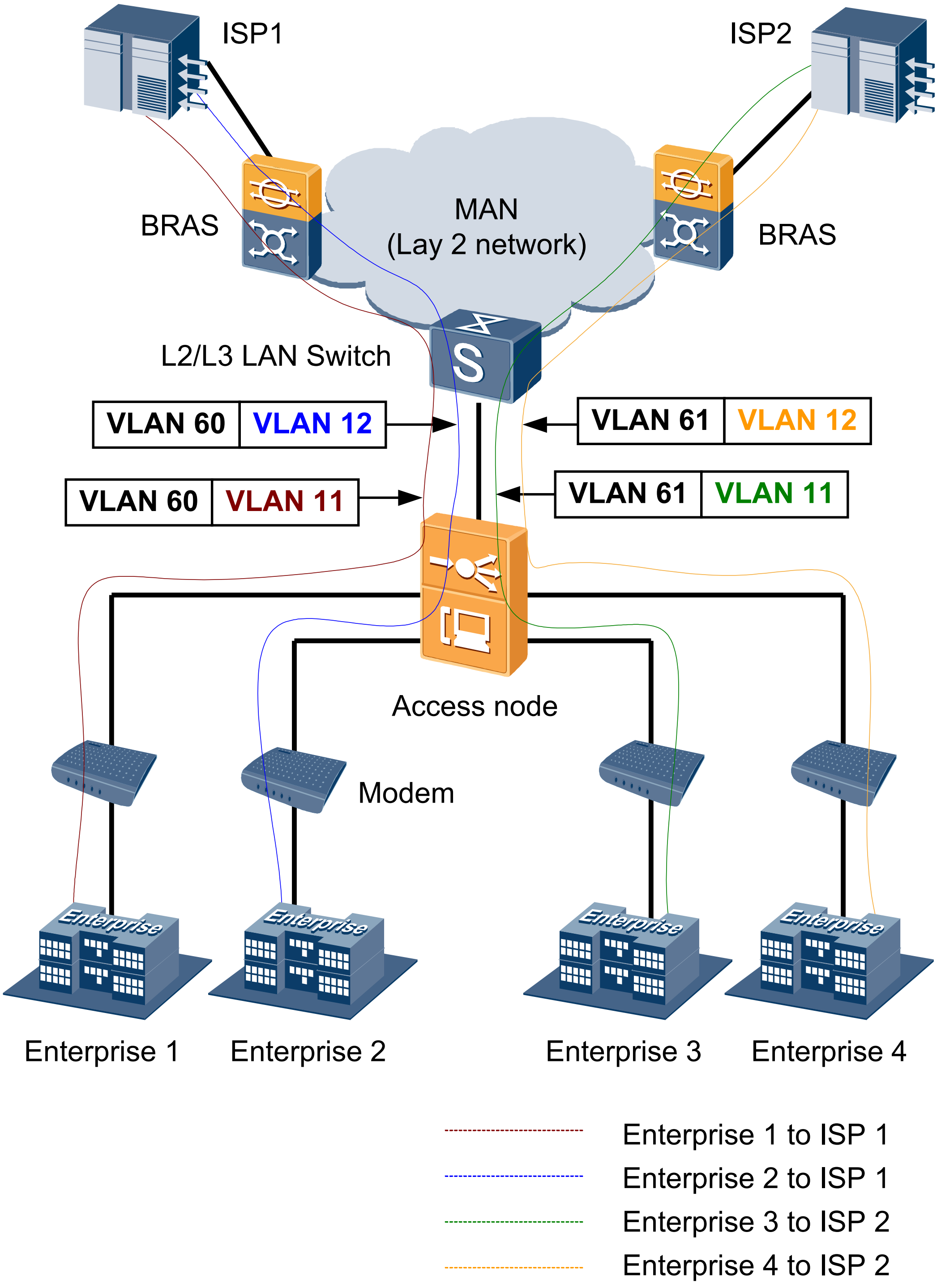
- The two ISPs in the Layer-2 switching MAN provide broadband services to enterprise users. Different enterprise user groups are bulk connected to the specified ISP to obtain services provided by the ISP.
- The access device uses xDSL or LAN access.

Networking

Figure 18-2 shows an example network for configuring the VLAN stacking multi-ISP wholesale access.

Enterprise 1 and 2 belong to ISP 1, and enterprise 3 and 4 belong to ISP 2. Based on the VLAN stacking feature. The upper-layer network must work in the Layer 2 mode, and must forward packets according to the VLAN and the MAC address. The MA5600T/MA5603T adds the outer VLAN tag to differentiate ISPs and inner VLAN tag to differentiate users and forwards the user packet to the Layer 2 network. Then the Layer 2/Layer 3 LAN switch forwards the user packets to the specified ISP BRAS based on the outer VLAN tag. The ISP BRAS removes the outer VLAN tag and identify the users based on the inner VLAN tag. After passing the authentication, the enterprise users can obtain various services provided by the ISP.

Figure 18-2 Example network for configuring the VLAN stacking multi-ISP wholesale access



Data Plan

Table 18-2 lists the key data planning of the VLAN stacking wholesale service on the MA5600T/MA5603T. The ADSL2+ access is used as an example.

Table 18-2 Data plan for configuring the VLAN stacking wholesale service

Item	Data	Remarks
VLAN	VLAN ID: ● ISP1: 60 – Enterprise user 1: 11 – Enterprise user 2: 12 ● ISP2: 61 – Enterprise user 3: 11 – Enterprise user 4: 12 ● VLAN type: smart VLAN ● VLAN attribute: stacking	The outer VLAN identifies the ISP, and inner VLAN identifies the user. The inner VLAN tags must be unique under the same ISP, but can be the same under different ISPs.
Upstream port	0/19/0	-
Traffic profile	● Traffic profile ID: 10 ● CIR: 2 Mbit/s ● Priority copy policy: user-cos ● Default 802.1p priority of the packet: 4 ● Priority-based scheduling policy of the downstream packets: local-setting	The CIR depends on the user bandwidth requirement.
ADSL2+ port	● ADSL2+ port ID – Enterprise user 1: 0/2/0 – Enterprise user 2: 0/2/1 – Enterprise user 3: 0/3/0 – Enterprise user 4: 0/3/1 ● Default ADSL2+ line profile: 1 ● Default ADSL2+ alarm profile: 1	-
Service virtual port	● Service port ID: – Enterprise user 1: 0 – Enterprise user 2: 1 – Enterprise user 3: 2 – Enterprise user 4: 3 ● VPI: 0 ● VCI: 35 ● ID of the traffic profile in Rx direction: 10 ● ID of the traffic profile in Tx direction: 10	● The VPI/VCI is the same as the management VPI/VCI on the peer modem. ● The traffic profile that meets the service requirement is used.

Procedure

Step 1 Create VLANs.

The outer VLAN IDs are 60 and 61, and the VLANs are smart VLANs.

```
huawei(config)#vlan 60-61 smart
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add VLANs? (y/n)[n]:y
```

Step 2 Set the VLAN attribute to stacking.

```
huawei(config)#vlan attrib 60-61 stacking
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to continue? (y/n)[n]:y
```

Step 3 Add an upstream port to the VLANs.

Add upstream port 0/19/0 to VLANs 60 and 61.

```
huawei(config)#port vlan 60-61 0/19 0
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the port VLAN(s) having been added is 2
```

Step 4 Add a traffic profile.

The profile ID is 10, the CIR is 2 Mbit/s, and packets are scheduled according to the priority specified in the traffic profile.

huawei(config)#**traffic table ip index 10 cir 2048 priority user-cos 4 priority-policy local-Setting**

Step 5 Activate the ADSL2+ port and bind a profile to it.

Use the default ADSL2+ line profile 1. Activate the ADSL2+ port and bind alarm profile 1 to the port. The following uses port 0/2/0 as an example. The configuration of the other three ADSL2+ ports are similar to that of port 0/2/0.

NOTE

- By default, the port is in the activated state. Before binding a profile to the port, you must deactivate the port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 1
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

Step 6 Add service ports to the VLANs.

Add service ports to the VLANs, and use traffic profile 10 that meets the service requirements. The VPI and the VCI are 0 and 35 respectively, the same as those on the peer modem.

```
huawei(config)#service-port 0 vlan 60 adsl 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr
10
huawei(config)#service-port 1 vlan 60 adsl 0/2/1 vpi 0 vci 35 rx-cttr 10 tx-cttr
10
huawei(config)#service-port 2 vlan 61 adsl 0/3/0 vpi 0 vci 35 rx-cttr 10 tx-cttr
10
huawei(config)#service-port 3 vlan 61 adsl 0/3/1 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
```

Step 7 Set the inner VLAN tags.

The inner VLAN tag identifies the user. Note that the inner VLAN tag must be unique in one ISP domain, and the inner VLAN tags can be the same in different ISP domains.

```
huawei(config)#stacking label service-port 0 11
huawei(config)#stacking label service-port 1 12
huawei(config)#stacking label service-port 2 11
huawei(config)#stacking label service-port 3 12
```

Step 8 Save the data.

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

----End

Result

- After passing the authentication by the ISP1 BRAS, enterprise 1 and enterprise 2 can obtain the service provided by ISP1.
- After passing the authentication by the ISP2 BRAS, enterprise 3 and enterprise 4 can obtain the service provided by ISP2.

Configuration File

```
vlan 60-61 smart
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add VLANs? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the added VLANs is 2

vlan attrib 60-61 stacking
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to continue? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the VLAN(s) which have been operated successfully is 2
port vlan 60-61 0/19 0
    It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the port VLAN(s) having been added is 2
traffic table ip index 100 cir 2048 priority user-cos 4 priority-policy local-
Setting
 service-port 0 vlan 60 adsl 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
service-port 1 vlan 60 adsl 0/2/1 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
service-port 2 vlan 61 adsl 0/3/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
service-port 3 vlan 61 adsl 0/3/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
stacking label service-port 0 11
stacking label service-port 1 12
stacking label service-port 2 11
stacking label service-port 3 12
save
```

18.3 Configuration Example of the PWE3 Private Line Service

This topic describes how to configure the MPLS PWE3 private line service using examples.

Context

For the PWE3 service model and network application, see **12.2 Configuring the PWE3 Private Line Service**.

PWE3 encapsulation may be performed in the following typical scenarios based on user-side service types and upstream network types.

User-Side Service	Upstream Network	Application
ATM	IP	Mainly used for the ATM network reconstruction. When the IP protocol is deployed for the transmission network and the ATM network evolves to the IP network, PWE3 encapsulation is recommended.
ATM	MPLS	Mainly used for the ATM network reconstruction. When the MPLS protocol is deployed for the transmission network and the ATM network evolves to the IP network, PWE3 encapsulation is recommended.
ETH	MPLS	Mainly used for private network data interaction between different enterprise branches.
TDM	IP	Mainly used to integrate the TDM circuit into the packet switched network (PSN) to provide more value-added services. When the IP protocol is deployed for the transmission network and the IP network provides simulated TDM services, PWE3 encapsulation is recommended.
TDM	MPLS	Mainly used to integrate the TDM circuit into the PSN to provide more value-added services. When the MPLS protocol is deployed for the transmission network and the IP network provides simulated TDM services, PWE3 encapsulation is recommended.

18.3.1 Example: Configuring ATM PWE3 to Implement Migration from ATM Network to IP Network

ATM PWE3 applies to ATM network reconstruction. If the IP protocol is used in the transport network, ATM PWE3 is recommended to migrate the ATM network to an IP network.

Service Requirements

- The original ATM DSLAM is replaced by the MA5600T/MA5603T and the upper-layer ATM BRAS remains.
- ATM service data is transparently transmitted across the network.
- The quality of service (QoS) such as traffic and priority, can be guaranteed for real-time ATM services.

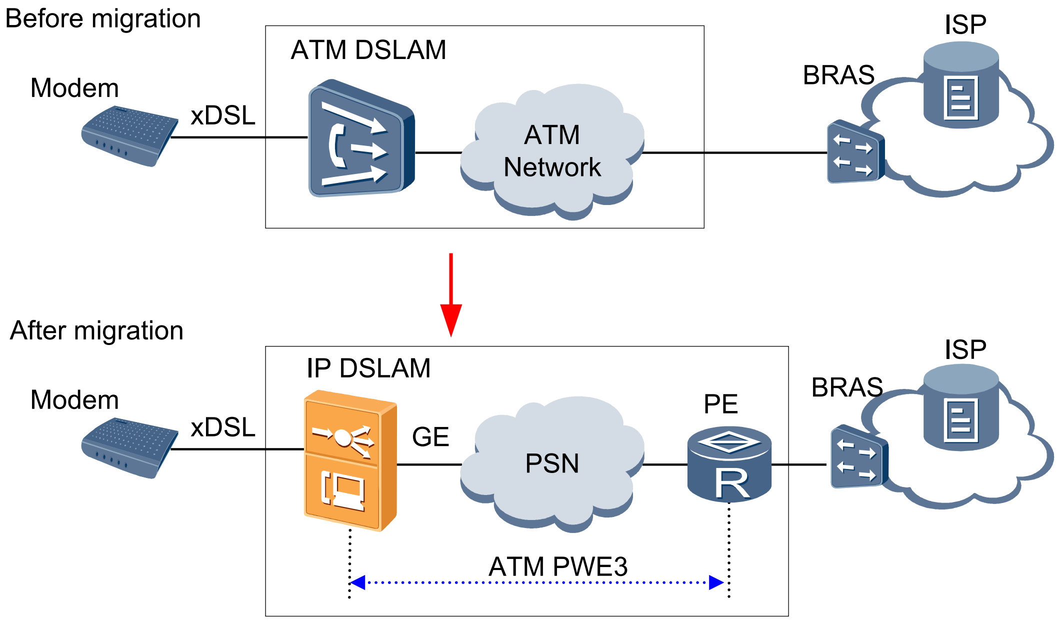
Networking

Figure 18-3 shows an example network of the ATM PWE3.

- Users access to MA5600T/MA5603T using xDSL service boards.

- The PW encapsulation mode is used to enable the transparent transmission of data over the IP network.
- PWs in the Ntol mode are used. Specifically, one PW is bound to multiple PVCs so that the same service from multiple users is carried by the same PW.
- In the upstream direction, the trTCM by CoS remarking based on PWs is used; in the downstream direction, the early drop based on CoS threshold is used. In this way, QoS can be guaranteed for various services.

Figure 18-3 Example network of the ATM PWE3



Prerequisite

- The xDSL board and the SPUB board must be in position and must work in the normal state.
- The static routing protocol or the OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised). For details, see **3.4 Configuring the Route**.

Context

For the principle and configuration of trTCM by CoS remarking, see **12.2.7 Configuring PW-based trTCM by CoS Remarking**.

The following ATM service types are available:

- Unspecified bit rate (UBR): UBR services support non-real-time applications, such as file transferring and Email. These applications have low requirements on delay or delay changes.
- Variable bit rate (VBR): VBR services can be further classified into real-time variable bit rate (rt-VBR) services and non-real-time variable bit rate (nrt-VBR) services. Both rt-VBR

and nrt-VBR services support changeable (burst) cell transmitting rate at the source end. The rt-VBR service type mainly applies to voice and video services.

- Constant bit rate (CBR): The CBR service type usually applies to real-time services that have high requirements on delay changes. Such services include voice, video, and circuit emulation services.

Data Plan

Table 18-3 lists the data plan for configuring the ATM PWE3.

Table 18-3 Key data plan for configuring the ATM PWE3

Item	Data	Remarks
MPLS	LSR ID: 5.5.5.5	The LSR ID must be the same as the IP address of the loopback interface on the device. To differentiate between the LSR ID and other IP addresses, set the LSR ID to a special unique value so that it identifies the device intuitively. The MPLS feature must be enabled for: 1. Global 2. L2VPN 3. VLAN and VLAN interfaces
VLAN	Smart VLAN: 300 IP address of the VLAN interface: 192.168.1.20 Upstream port: 0/19/1	VLAN and VLAN interfaces must be configured to enable MPLS forwarding.
PW parameters	Peer IP address: 7.7.7.7 PW type: ATM Nto1 VCC Control word: enabled (Optional) Maximum number of concatenated ATM cells: 4 (Optional) Maximum encapsulation delay of ATM cells: 10 ms PW type: static	The control word adds control information into service packets to rearrange the packets and to prevent packet disorder. ATM services must use the control word since they have high requirements on time sequence. Cell concatenation enables a PW packet to carry multiple ATM cells. In this way, the transmission efficiency of ATM cells over a PSN network and bandwidth utilization are improved.

Item	Data	Remarks
Tunnel	Tunnel ID: 20; tunnel interface ID: 20 Encapsulation protocol of the tunnel interface at the data link layer: MPLS IP Source IP address of the tunnel: 5.5.5.5 Destination IP address of the tunnel: 7.7.7.7	IP tunnels are used. Ingress and egress addresses of a tunnel are the LSR IDs of the local device and the peer PE device, respectively.
OSPF	OSPF process ID: 200; OSPF area ID: 1	Routes use the OSPF protocol.
PWE3 gateway	LSR ID: 7.7.7.7	It is the LSR ID of the peer PE device.

Table 18-4 Plan for configuring attributes of each type of service

Item	service Type			Remarks
	UBR	VBR	CBR	
Board Slot	0/2	0/3	0/4	Multiple services of the same type but from different users are deployed at different ports on the same board (in the same slot). By doing so, the same PW is used to carry multiple PVCs. This improves the transmission efficiency, reduces the number of PWs required, and facilitates the application of QoS policies. Services of different types are deployed on boards in different slots, isolating the services physically.
VPI/ VCI of Cells	0/35	0/35	0/35	Since the services belong to the same ISP, the VPI/VCI parameters of cells on PVCs at different ports are the same.
Binding PW ID	20	21	22	Services of different types are carried over different PWs, eliminating service interaction.

Item	service Type			Remarks
	UBR	VBR	CBR	
Initial Value for Ingress PVC in the PW	0/32	0/33	0/34	Since the VPI/VCI parameters of cells on PVCs at different ports are the same, the VPI/VCI parameters must be changed once before the cells on client-side PVCs are encapsulated into PWs. This ensures that the VPI/VCI parameters are unique for cells on each PVC in the PW.
Initial Value for Egress PVC in the PW	1/32	1/33	1/34	
Egress Label of the PW	8450	8451	8452	
Ingress Label of the PW	8460	8461	8462	
PW CAR	12288 Kbit/s	30720 Kbit/s	6144 Kbit/s	QoS policies: In the upstream direction, priorities of service packets are remarked by setting CAR and PIR for the PW and only yellow packets are identified (CAR < Rate < PIR).
User-CoS Priority	1	4	5	
CoS Priority After Remarking	0	2	5	
WRED Profile	ID: 5	ID: 5	ID: 5	QoS policies: In the downstream direction, the xDSL board sets CoS drop threshold globally to early drop yellow packets.

Item	service Type			Remarks
	UBR	VBR	CBR	
Traffic Profile	● CAR: OFF ● Color policy: cos-remark ● Downstream priority policy: tag-in-package	● CAR: OFF ● Color policy: cos-remark ● Downstream priority policy: tag-in-package	● CAR: OFF ● Color policy: cos-remark ● Downstream priority policy: tag-in-package	The traffic profile does no limit the rate. Instead the rate is limited using PWs.

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create upstream VLAN 300 and add upstream port 0/19/1 to VLAN 300.

```
huawei(config)#vlan 300 standard
 huawei(config)#port vlan 300 0/19 1
```

Step 2 Enable MPLS.

1. Configure the IP address of the loopback interface.

   Configure the IP address of loopback interface 0 to 5.5.5.5/32.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 5.5.5.5 32
huawei(config-if-loopback0)#quit
```

2. Configure the LSR ID of the MPLS and enable global MPLS function and Layer 2 VPN.

```
huawei(config)#mpls lsr-id 5.5.5.5
huawei(config)#mpls
huawei(config-mpls)#quit
huawei(config)#mpls l2vpn
```

3. Enable the MPLS function for VLAN 300, configure the IP address of the VLAN interface 300, and enable the MPLS function for it.

```
huawei(config)#mpls vlan 300
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#ip address 192.168.1.20 24
huawei(config-if-vlanif300)#mpls
huawei(config-if-vlanif300)#quit
```

Step 3 Configure a route.

PWE3 has no special requirement for the routing policy. Either a static route or an OSPF dynamic route can be configured. Because OSPF supports MPLS RSVP-TE extension, an OSPF dynamic route is recommended.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 200
huawei(config-ospf-1-area-0.0.0.200)#network 192.168.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.200)#network 5.5.5.5 0.0.0.0
huawei(config-ospf-1-area-0.0.0.200)#return
```

Step 4 Configure a PWE3 outer tunnel.

Configure the tunnel ID to 20 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS IP.

```
huawei#config
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls ip
```

Configure the source IP address of the tunnel to 5.5.5.5.

```
huawei(config-if-tunnel20)#source 5.5.5.5
```

Configure the destination IP address of the tunnel to 7.7.7.7.

```
huawei(config-if-tunnel20)#destination 7.7.7.7
```

Commit the configuration and quit the MPLS tunnel configuration.

```
huawei(config-if-tunnel20)#mpls ip commit
huawei(config-if-tunnel20)#quit
```

Step 5 Configure the tunnel policy.

Configure the policy name to atmpw-plcy.

```
huawei(config)#tunnel-policy atmpw-plcy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-atmpw-plcy)#tunnel select-seq ip load-balance-number
1
huawei(config-tunnel-policy-atmpw-plcy)#quit
```

Step 6 Configure the PW parameters.

NOTE

Take the configuration of PW 20 for example. To configure the PW 21 and PW 22 based on the data plan using the same steps.

1. Configure the PW ID to 20.
   ```
   huawei(config)#pw-para 20
   ```
2. Configure the LSR ID of the peer PWE3 gateway in the PW. Configure the LSR ID of the PWE3 gateway to 7.7.7.7.
   ```
   huawei(config-pw-para-20)#peer-address 7.7.7.7
   ```
3. Configure the PW type to ATM NTo1 VCC.
   ```
   huawei(config-pw-para-20)#pw-type atm nto1 vcc
   ```
4. Configure the PW to support the control word.
   ```
   huawei(config-pw-para-20)#control-word
   ```
5. (Optional) Set the maximum number of concatenated ATM cells to 4.
   ```
   huawei(config-pw-para-1)#max-atm-cells 4
   ```
6. (Optional) Set the maximum encapsulation delay of ATM cells to 10 ms.
   ```
   huawei(config-pw-para-1)#max-encapcell-delay 10
   ```
7. Configure the tunnel policy used by the PW.

   Configure the tunnel policy name to atmpw-plcy.

   ```
   huawei(config-pw-para-20)#tnl-policy atmpw-plcy huawei(config-pw-para-20)#quit
   ```

Step 7 Configure a traffic profile.

1. For UBR services, set the upstream/downstream traffic profile to 20, CIR to off (limiting rate only on BRAS), color policy to CoS, user-side packet mapping mode to outer-layer 802.1p, default 802.1p to 1, and priority policy to **tag-in-package**.

```
huawei(config)#traffic table ip index 20 cir off color-policy cos priority
user-cos 1 priority-policy tag-in-package
```

   NOTE

   - The color policy in the upstream and downstream traffic profiles must be the same.
   - If the color policy is cos-remark, the priority policy must be tag-in-package for the downstream direction.

2. For VBR services, set the upstream traffic profile to 21, CIR to off, color policy to CoS, user-side packet mapping mode to outer-layer 802.1p, default 802.1p to 4, and priority policy to **tag-in-package**.

```
huawei(config)#traffic table ip index 21 cir off color-policy cos priority
user-cos 4 priority-policy tag-in-package
```

3. For CBR services, set the upstream traffic profile to 22, CIR to off, color policy to CoS, user-side packet mapping mode to outer-layer 802.1p, default 802.1p to 5, and priority policy to **tag-in-package**.

```
huawei(config)#traffic table ip index 22 cir off color-policy cos priority
user-cos 5 priority-policy tag-in-package
```

Step 8 Create an ATM access service stream.

ATM cells must be encapsulated into ATM over Ethernet (AOE) packets before being carried by PWs. That is, create an ATM service stream.

- Create AOE service streams in batches for UBR services.

  The service board is in slot 0/2, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 20.

```
huawei(config)#multi-service-port vlan aoe board 2 vpi 0 vci 35 inbound
traffic-table index 20 outbound traffic-table index 20
```

- Create AOE service streams in batches for VBR services.

  The service board is in slot 0/3, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 21.

```
huawei(config)#multi-service-port vlan aoe board 3 vpi 0 vci 35 inbound
traffic-table index 21 outbound traffic-table index 21
```

- Create AOE service streams in batches for CBR services.

  The service board is in slot 0/4, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 22.

```
huawei(config)#multi-service-port vlan aoe board 4 vpi 0 vci 35 inbound
traffic-table index 22 outbound traffic-table index 22
```

Step 9 Bind the PVCs to PW 20 in batches to create an ATM PWE3 service.

Since the VPI/VCI parameters of cells on PVCs at different ports are the same, the VPI/VCI parameters must be changed once before the cells on client-side PVCs are encapsulated into PWs. This ensures that the VPI/VCI parameters are unique for cells on each PVC in the PW.

- Bind PVCs and PWs in batches for UBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 2 vpi 0 vci 35 from-outvpi 0 outvci
32
from-invpi 1 invci 32 pw 20 static transmit-label 8450 receive-label 8460
```

- Bind PVCs and PWs in batches for VBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 3 vpi 0 vci 35 from-outvpi 0 outvci
33
from-invpi 1 invci 33 pw 21 static transmit-label 8451 receive-label 8461
```

- Bind PVCs and PWs in batches for CBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 4 vpi 0 vci 35 from-outvpi 0 outvci
34
from-invpi 1 invci 34 pw 22 static transmit-label 8452 receive-label 8462
```

Step 10 Configure the WRED profile.

The index is 5. Configure the WRED profile so that green packets are not dropped, lower threshold for dropping yellow packets is 50, upper threshold for dropping yellow packets is 80, and the packet dropping percentage is 100.

```
huawei(config)#wred-profile index 5 green low-limit 100 high-limit 100
discard-probability 0 yellow low-limit 50 high-limit 80 discard-probability 100
```

Step 11 Configure queues and bind the WRED profile.

```
huawei(config)#queue-wred queue0 5 queue1 5 queue2 5 queue3 5 queue4 5 queue5 5
queue6 5 queue7 5
```

Step 12 Configure the priority remarking policy.

Remark the priority of yellow packets. Specifically, remark priority 1 (UBR service packets) to 0; priority 4 (VBR service packets) to 2, and priority 5 (CBR service packets) to 5.

```
huawei(config)#cos-remark cos1 0 cos4 2 cos5 5
```

Step 13 Configure the mapping between queues and 802.1p priorities.

Packets with 802.1p priorities 0 and 1 join queue 1; packets with 802.1p priorities 2 and 4 join queue 4; packets with 802.1p priority 5 join queue 5.

NOTE

Ensure that the packets with the CoS values before and after remarking join the same queue.

```
huawei(config)#cos-queue-map cos0 1 cos1 1 cos2 4 cos4 4 cos5 5
```

Step 14 Set committed rate in the PW upstream direction.

- Set CAR in the upstream direction of PW 20 to 12288 kbit/s.
  ```
  huawei(config)#mpls car-pw 20 cir 12288
  ```
- Set CAR in the upstream direction of PW 21 to 30720 kbit/s.
  ```
  huawei(config)#mpls car-pw 21 cir 30720
  ```
- Set CAR in the upstream direction of PW 22 to 6144 kbit/s.
  ```
  huawei(config)#mpls car-pw 22 cir 6144
  ```

----End

Result

- UBR, VBR, and CBR services can be migrated to an IP network smoothly. No change is required on the user side and users will not feel any change.
- Various services are scheduled based on their priorities. When a congestion occurs on the network, the quality of CBR services is guaranteed with precedence.
- When a congestion occurs at a port, the system first drops traffic of the burst bandwidth (bandwidth > peak value), ensuring the guaranteed bandwidth for each type of service.

Configuration File

```
vlan 300 smart
port vlan 300 0/19 1
interface loopback 0
ip address 5.5.5.5 32
quit
mpls lsr-id 5.5.5.5
mpls
quit
mpls l2vpn
```

```
mpls vlan 300
interface vlanif 300
ip address 192.168.1.20 24
mpls
quit
ospf 1
area 200
network 192.168.1.0 0.0.0.255
network 5.5.5.5 0.0.0.0
return
config
interface tunnel 20
tunnel-protocol mpls ip
destination 7.7.7.7
mpls ip commit
quit
tunnel-policy atmpw-plcy
tunnel select-seq ip load-balance-number 1
quit
pw-para 20
peer-address 7.7.7.7
pw-type atm nto1 vcc
control-word
max-atm-cells 4
max-encapcell-delay 10
tnl-policy atmpw-plcy
quit
traffic table ip index 20 cir off color-policy cos priority user
-cos 1 priority-policy tag-in-package
traffic table ip index 21 cir off color-policy cos priority user
-cos 4 priority-policy tag-in-package
traffic table ip index 22 cir off color-policy cos priority user
-cos 5 priority-policy tag-in-package
multi-service-port vlan aoe board 2 vpi 0 vci 35 inbound traffi
c-table index 20 outbound traffic-table index 20
multi-service-port vlan aoe board 3 vpi 0 vci 35 inbound traffi
c-table index 21 outbound traffic-table index 21
multi-service-port vlan aoe board 4 vpi 0 vci 35 inbound traffi
c-table index 22 outbound traffic-table index 22
multi-pw-ac-binding pvc board 2 vpi 0 vci 35 from-outvpi 0 outvci 32
from-invpi 1 invci 32 pw 20 static transmit-label 8450 receive-label 8460
multi-pw-ac-binding pvc board 3 vpi 0 vci 35 from-outvpi 0 outvci 33
from-invpi 1 invci 33 pw 21 static transmit-label 8451 receive-label 8461
multi-pw-ac-binding pvc board 4 vpi 0 vci 35 from-outvpi 0 outvci 34
from-invpi 1 invci 34 pw 22 static transmit-label 8452 receive-label 8462
wred-profile index 5 green low-limit 100 high-limit 100 discard-probability
 0 yellow low-limit 50 high-limit 80 discard-probability 100
queue-wred queue0 5 queue1 5 queue2 5 queue3 5 queue4 5 queue5 5
queue6 5 queue7 5
cos-remark cos1 0 cos4 2 cos5 5
cos-queue-map cos0 1 cos1 1 cos2 4 cos4 4 cos5 5
mpls car-pw 20 cir 12288
mpls car-pw 20 cir 30720
mpls car-pw 20 cir 6144
```

18.3.2 Example: Configuring the ATM PWE3 to Achieve emulated ATM Services on the MPLS Network

ATM PWE3 is mainly used in ATM network reconstruction. When the MPLS protocol is deployed for the transmission network and the ATM network evolves to the MPLS network, PWE3 encapsulation is recommended.

Service Requirements

- The xDSL service board (or AIUG board) of the MA5600T/MA5603T is used to provide the ATM service.
- The PW encapsulation mode is adopted so that data can be transparently transmitted in the MPLS network.

Prerequisite

- The xDSL board (or AIUG board) and the SPUB board must be in position and must work in the normal state.
- The static routing protocol or the OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised). For details, see **3.4 Configuring the Route**.

Context

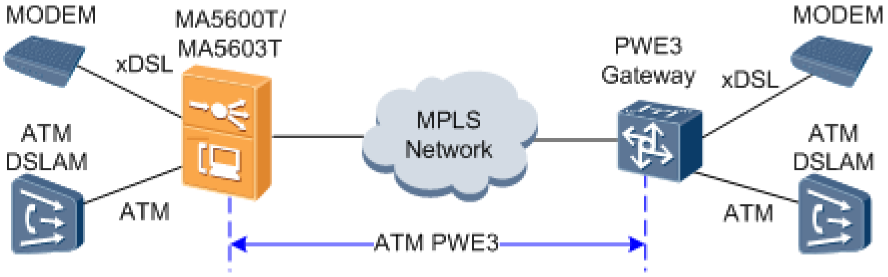
The implementation process of the ATM PWE3 (MPLS-based) is as follows:

1. The xDSL modem or ATM DSLAM transmits the ATM service to the xDSL or AIUG board of the MA5600T/MA5603T.
2. The control board sends ATM packets to the SPUB board.
3. After performing the PW and MPLS encapsulation for the packets, the SPUB board performs the MPLS packet header encapsulation and then sends them to the control board.
4. The control board performs the Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the MPLS network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores the ATM cells and sends them to the peer ATM device.

Networking

Figure 18-4 shows an example network of the ATM PWE3 (MPLS-based).

Figure 18-4 Example network of the ATM PWE3 (MPLS-based)



Data Plan

Table 18-5 lists the data plan for configuring the ATM PWE3 (MPLS-based).

Table 18-5 Data plan for configuring the ATM PWE3 (MPLS-based)

Item	Data
MPLS	LSR ID: 5.5.5.5 Global MPLS TE: enabled MPLS Layer 2 VPN: enabled VLAN MPLS RSVP-TE: enabled
VLAN	Standard VLAN for MPLS forwarding: 300 MPLS address of the VLAN interface: 192.2.2.20 Upstream port: 0/19/1
PW parameters	PW ID: 20 Peer IP address: 7.7.7.7 PW type: ATM Nto1 VCC PW in VPI/VCI: 0/35 PW out VPI/VCI: 8/35 PW type: static Control word: enabled PW out port: 8450 PW in port: 8460
Tunnel	Tunnel ID: 20; tunnel interface ID: 20 Encapsulation protocol of the tunnel interface at the data link layer: MPLS TE Tunnel signaling protocol: RSVP-TE
ATM service port	Port: 0/2/0 Emulation SVLAN: 3001 VPI/VCI: 0/35
OSPF	OSPF process ID: 200; OSPF area ID: 1 Enable MPLS TE for the OSPF area
PWE3 gateway	LSR ID: 7.7.7.7

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create upstream VLAN 300 and add upstream port 0/19/1 to VLAN 300.

```
huawei(config)#vlan 300 standard
 huawei(config)#port vlan 300 0/19 1
```

Step 2 Enable MPLS.

1. Configure the IP address of the loopback interface.

   Configure the IP address of loopback interface 0 to 5.5.5.5/32.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 5.5.5.5 32
huawei(config-if-loopback0)#quit
```

2. Configure the LSR ID of the MPLS and enable global MPLS TE and Layer 2 VPN.

```
huawei(config)#mpls lsr-id 5.5.5.5
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsvp-te
huawei(config-mpls)#quit
huawei(config)#mpls l2vpn
```

3. Enable the VLAN interface MPLS TE function and configure the IP address of the VLAN interface.

```
huawei(config)#mpls vlan 300
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#ip address 192.2.2.20 24
huawei(config-if-vlanif300)#mpls
huawei(config-if-vlanif300)#mpls te
huawei(config-if-vlanif300)#mpls rsvp-te
huawei(config-if-vlanif300)#quit
```

Step 3 Configure a route.

PWE3 has no special requirement for the routing policy. Either a static route or an OSPF dynamic route can be configured. Because OSPF supports MPLS RSVP-TE extension, an OSPF dynamic route is recommended.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#opaque-capability enable..//Enable the opaque capability
huawei(config-ospf-1)#area 200
huawei(config-ospf-1-area-0.0.0.200)#mpls-te enable standard-complying //Enable
MPLS TE for the OSPF area
huawei(config-ospf-1-area-0.0.0.200)#network 192.2.2.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.200)#network 5.5.5.5 0.0.0.0
huawei(config-ospf-1-area-0.0.0.200)#return
```

Step 4 Configure a PWE3 outer tunnel.

Configure the tunnel ID to 20 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS TE.

```
huawei#config
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls te
```

Configure the destination IP address of the tunnel to 7.7.7.7.

```
huawei(config-if-tunnel10)#destination 7.7.7.7
```

Configure the ID of the MPLS TE tunnel interface to 20. The tunnel ID and LSR ID uniquely identify an MPLS TE tunnel.

```
huawei(config-if-tunnel20)#mpls te tunnel-id 20
```

Configure the signaling protocol of the MPLS TE tunnel to RSVP-TE.

```
huawei(config-if-tunnel20)#mpls te signal-protocol rsvp-te
```

Configure the MPLS TE tunnel for being bound by a VPN instance.

```
huawei(config-if-tunnel20)#mpls te reserved-for-binding
```

Commit the configuration and quit the tunnel configuration.

```
huawei(config-if-tunnel20)#mpls te commit
huawei(config-if-tunnel20)#quit
```

Step 5 Configure the tunnel policy.

Configure the policy name to atmpw-plcy.

```
huawei(config)#tunnel-policy atmpw-plcy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-atmpw-plcy)#tunnel binding destination 7.7.7.7 te
tunnel 20
huawei(config-tunnel-policy-atmpw-plcy)#quit
```

Step 6 Configure the PW parameters.

NOTE

Take the configuration of PW 20 for example. To configure the PW 21 and PW 22 based on the data plan using the same steps.

1. Configure the PW ID to 20.
```
huawei(config)#pw-para 20
```
2. Configure the LSR ID of the peer PWE3 gateway in the PW. Configure the LSR ID of the PWE3 gateway to 7.7.7.7.
```
huawei(config-pw-para-20)#peer-address 7.7.7.7
```
3. Configure the PW type to ATM NTo1 VCC.
```
huawei(config-pw-para-20)#pw-type atm nto1 vcc
```
4. Configure the PW to support the control word.
```
huawei(config-pw-para-20)#control-word
```
5. (Optional) Set the maximum number of concatenated ATM cells to 4.
```
huawei(config-pw-para-1)#max-atm-cells 4
```
6. (Optional) Set the maximum encapsulation delay of ATM cells to 10 ms.
```
huawei(config-pw-para-1)#max-encapcell-delay 10
```
7. Configure the tunnel policy used by the PW.

   Configure the tunnel policy name to atmpw-plcy.
```
huawei(config-pw-para-20)#tnl-policy atmpw-plcy huawei(config-pw-para-20)#quit
```

Step 7 Create an ATM access service stream.

ATM cells must be encapsulated into ATM over Ethernet (AOE) packets before being carried by PWs. That is, create an ATM service stream.

- Create AOE service streams in batches for UBR services.

  The service board is in slot 0/2, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 20.
```
huawei(config)#multi-service-port vlan aoe board 2 vpi 0 vci 35 inbound
traffic-table index 20 outbound traffic-table index 20
```
- Create AOE service streams in batches for VBR services.

  The service board is in slot 0/3, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 21.
```
huawei(config)#multi-service-port vlan aoe board 3 vpi 0 vci 35 inbound
traffic-table index 21 outbound traffic-table index 21
```
- Create AOE service streams in batches for CBR services.

  The service board is in slot 0/4, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 22.
```
huawei(config)#multi-service-port vlan aoe board 4 vpi 0 vci 35 inbound
traffic-table index 22 outbound traffic-table index 22
```

Step 8 Bind the PVCs to PW 20 in batches to create an ATM PWE3 service.

Since the VPI/VCI parameters of cells on PVCs at different ports are the same, the VPI/VCI parameters must be changed once before the cells on client-side PVCs are encapsulated into PWs. This ensures that the VPI/VCI parameters are unique for cells on each PVC in the PW.

- Bind PVCs and PWs in batches for UBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 2 vpi 0 vci 35 from-outvpi 0 outvci 
32
from-invpi 1 invci 32 pw 20 static transmit-label 8450 receive-label 8460
```

- Bind PVCs and PWs in batches for VBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 3 vpi 0 vci 35 from-outvpi 0 outvci 
33
from-invpi 1 invci 33 pw 21 static transmit-label 8451 receive-label 8461
```

- Bind PVCs and PWs in batches for CBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 4 vpi 0 vci 35 from-outvpi 0 outvci 
34
from-invpi 1 invci 34 pw 22 static transmit-label 8452 receive-label 8462
```

Step 9 Query the PW status.

```
huawei(config)#display pw-ac-binding pvc 0/2/0 vpi 0 vci 35
  Total : 1  (Up/Down :    1/0           Static/LDP :    1/0)
  ---------------------------------------------------------------------------
  F/S/P            PW         PW    PROTO  RECEIVE TRNS    PW
  VPIVCI           ID         STATE TYPE   LABEL   LABEL   INDEX
  ---------------------------------------------------------------------------
   0/2/0 0 35      20         up    static 8460    8450    20
  ---------------------------------------------------------------------------
  Note  : F--Frame, S--Slot, P--Port
          *: Secondary
```

----End

Result

The ATM packets can be transparently transmitted in the MPLS network and the ATM-based services can be provided normally.

Configuration File

```
vlan 300 standard
port vlan 300 0/19 1
interface loopback 0
ip address 5.5.5.5 32
quit
mpls lsr-id 5.5.5.5
mpls
mpls te
mpls rsvp-te
quit
mpls l2vpn
mpls vlan 300
interface vlanif 300
ip address 192.2.2.20 24
mpls
mpls te
mpls rsvp-te
quit
ospf 1
opaque-capability enable
area 200
mpls-te enable standard-complying
network 192.2.2.0 0.0.0.255
network 5.5.5.5 0.0.0.0
return
config
interface tunnel 20
```

```
tunnel-protocol mpls te
destination 7.7.7.7
mpls te tunnel-id 20
mpls te signal-protocol rsvp-te
mpls te reserved-for-binding
mpls te commit
quit
tunnel-policy atmpw-plcy
tunnel binding destination 7.7.7.7 te tunnel 20
quit
pw-para 20
peer-address 7.7.7.7
pw-type atm nto1 vcc
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy atmpw-plcy
quit
service-port vlan aoe adsl 0/2/0 vpi 0 vci 35 rx-cttr 6 tx-cttr 6   //xDSL access
service-port vlan aoe atm 0/2/0 vpi 0 vci 35 rx-cttr 6 tx-cttr 6   //ATM access
pw-ac-bnding pvc 0/2/0 vpi 0 vci 35 outvpi 8 outvci 35 pw 20
static transmit-label 8450 receive-label 8460
```

18.3.3 Example: Configuring the ETH PWE3 to Emulate Ethernet Services on the MPLS Network

The MA5600T/MA5603T supports the PW encapsulation for ethernet packets and implements the ETH PWE3 emulation service after the MPLS encapsulation of the packets, providing the solution of emulation Ethernet private line service over the MPLS network.

Service Requirements

- The data interaction between enterprise branches in different regions is achieved through the metropolitan area network (MAN) that is running the MPLS protocol.
- The Ethernet service data of the enterprise private network is transparently transmitted so that the data security can be ensured.

Prerequisite

- The SPUB board must be in position and must work in the normal state.
- The static routing protocol or the OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised). For details, see **3.4 Configuring the Route**.

Context

The Ethernet packet-based data interaction between enterprise branches in different regions is achieved using the routers of the public network to forward the packets. If the public network uses the MPLS protocol, the Ethernet packets cannot be forwarded directly. In this case, the Ethernet packet forwarding can be achieved by using the ETH PWE3 technology. In addition, the ETH PWE3 technology can be deployed to achieve high security with low costs.

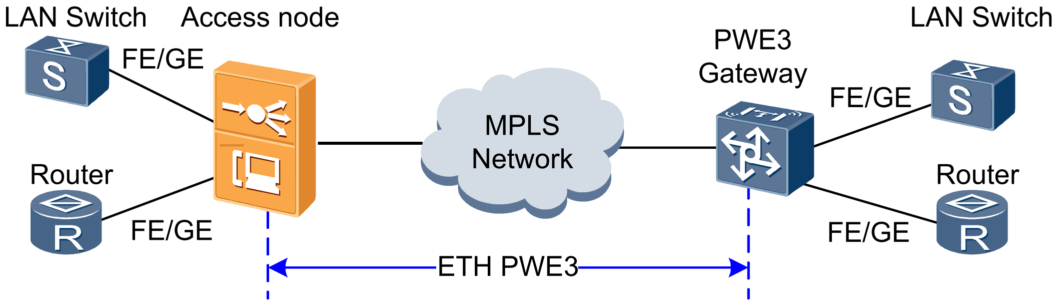
Networking

Figure 18-5 shows an example network of the ETH PWE3.

1. The Ethernet switch or router of the enterprise aggregates the private network data of the enterprise and sends the data to the ETH board of the MA5600T/MA5603T.

2. The control board sends ETH packets to the SPUB board.
3. After performing the PW and MPLS encapsulation for the packets, the SPUB board performs the ETH packet header encapsulation and then sends them to the control board.
4. The control board performs the Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the MPLS network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores ETH signals and sends them to the peer Ethernet switch or router.

Figure 18-5 Example network of the ETH PWE3



Data Plan

Table 18-6 lists the data plan for configuring the ETH PWE3.

Table 18-6 Data plan for configuring the ETH PWE3

Item	Data
MPLS	LSR ID: 5.5.5.5 Global MPLS TE: enabled MPLS Layer 2 VPN: enabled VLAN MPLS RSVP-TE: enabled
VLAN	Standard VLAN for MPLS forwarding: 200 IP address of the VLAN interface: 192.1.1.10 Upstream port: 0/19/0
PW parameters	PW ID: 10 Peer IP address: 6.6.6.6 PW type: ETH tagged Control word: enabled Out label: 8500 In label: 8600

Item	Data
Tunnel	Tunnel ID: 10; tunnel interface ID: 10 Encapsulation protocol of the tunnel interface at the data link layer: MPLS TE Tunnel signaling protocol: RSVP-TE
ETH service port	Port: 0/4/0 Emulation SVLAN: 3001 CVLAN: 20
OSPF	OSPF process ID: 100; OSPF area ID: 1 Enable MPLS TE for the OSPF area
PWE3 gateway	LSR ID: 6.6.6.6

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create upstream VLAN 200 and add upstream port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 standard
huawei(config)#port vlan 200 0/19 0
```

Step 2 Enable MPLS.

1. Configure the IP address of the loopback interface.

   Configure the IP address of loopback interface 0 to 5.5.5.5/32.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 5.5.5.5 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the LSR ID of the MPLS and enable global MPLS TE and Layer 2 VPN.

   ```
   huawei(config)#mpls lsr-id 5.5.5.5
   huawei(config)#mpls
   huawei(config-mpls)#mpls te
   huawei(config-mpls)#mpls rsvp-te
   huawei(config-mpls)#quit
   huawei(config)#mpls l2vpn
   ```

3. Enable the VLAN interface MPLS TE function and configure the IP address of the VLAN interface.

   ```
   huawei(config)#mpls vlan 200
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 192.1.1.10 24
   huawei(config-if-vlanif200)#mpls
   huawei(config-if-vlanif200)#mpls te
   huawei(config-if-vlanif200)#mpls rsvp-te
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure a route.

PWE3 has no special requirement for the routing policy. Either a static route or an OSPF dynamic route can be configured. Because OSPF supports MPLS RSVP-TE extension, an OSPF dynamic route is recommended.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#opaque-capability enable..//Enable the opaque capability
```

```
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#mpls-te enable standard-complying //Enable
MPLS TE for the OSPF area
huawei(config-ospf-1-area-0.0.0.100)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 5.5.5.5 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure a PWE3 outer tunnel.

Configure the tunnel ID to 10 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS TE.

```
huawei#config
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
```

Configure the destination IP address of the tunnel to 6.6.6.6.

```
huawei(config-if-tunnel10)#destination 6.6.6.6
```

Configure the ID of the MPLS TE tunnel interface to 10. The tunnel ID and LSR ID uniquely identify an MPLS TE tunnel.

```
huawei(config-if-tunnel10)#mpls te tunnel-id 10
```

Configure the signaling protocol of the MPLS TE tunnel to RSVP-TE.

```
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
```

Configure the MPLS TE tunnel for being bound by a VPN instance.

```
huawei(config-if-tunnel10)#mpls te reserved-for-binding
```

Commit the configuration and quit the tunnel configuration.

```
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

Step 5 Configure the tunnel policy.

Configure the policy name to ethpw-plcy.

```
huawei(config)#tunnel-policy ethpw-plcy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-ethpw-plcy)#tunnel binding destination 6.6.6.6 te
tunnel 10
huawei(config-tunnel-policy-ethpw-plcy)#quit
```

Step 6 Configure the PW parameters.

1. Configure the PW ID to 10.
   ```
   huawei(config)#pw-para 10
   ```
2. Configure the LSR ID of the peer PWE3 gateway in the PW. Configure the LSR ID of the PWE3 gateway to 6.6.6.6.
   ```
   huawei(config-pw-para-10)#peer-address 6.6.6.6
   ```
3. Configure the PW type to ethernet tagged.
   ```
   huawei(config-pw-para-10)#pw-type ethernet tagged
   ```
4. Configure the PW to support the control word.
   ```
   huawei(config-pw-para-10)#control-word
   ```
5. Enable the virtual circuit connectivity verification (VCCV) function.
   ```
   huawei(config-pw-para-10)#vccv cc cw alert ttl cv lsp-ping
   ```
6. Configure the tunnel policy used by the PW.

   Configure the tunnel policy name to ethpw-plcy.

```
huawei(config-pw-para-10)#tnl-policy etnpw-plcy
huawei(config-pw-para-10)#quit
```

Step 7 Create an Ethernet access service port.

Create a VLAN for the ETH emulation service (after ETH emulation, this VLAN will be restored by the peer ETH PWE3 gateway), and then create a service port for translating the CVLAN ID into the VLAN ID of the emulation service.

```
huawei(config)#vlan 3001
huawei(config)#service-port vlan 3001 eth 0/4/0 multi-service user-vlan 20 rx-cttr
6 tx-cttr 6
```

Step 8 Bind the VLAN to the PW to create the ETH PWE3 service.

Bind emulation SVLAN 3001 to PW 10, and set PW type to static PW, out label of the PW to 8500, and in label of the PW to 8600.

```
huawei(config)#pw-ac-binding vlan 3001 pw 10 static transmit-label 8500 receive-
label 8600
```

Step 9 Query the PW status.

```
huawei(config)#display pw-ac-binding vlan 3001
  Total : 1  (Up/Down :    1/0          Static/LDP :    1/0)
  ----------------------------------------------------------------------------
  VLAN             PW         PW    PROTO  RECEIVE TRNS     PW
  ID               ID         STATE TYPE   LABEL   LABEL    INDEX
  ----------------------------------------------------------------------------
   3001            10         up    static 8600    8500     10
  ----------------------------------------------------------------------------
```

----End

Result

The private network data of the enterprise can be transparently transmitted over the MPLS network, and all services in the private network can be provided normally.

Configuration File

```
vlan 200 smart
port vlan 200 0/19 0
interface loopback 0
ip address 5.5.5.5 32
quit
mpls lsr-id 5.5.5.5
mpls
mpls te
mpls rsvp-te
quit
mpls l2vpn
mpls vlan 200
interface vlanif 200
ip address 192.1.1.10 24
mpls
mpls te
mpls rsvp-te
quit
ospf 1
opaque-capability enable
area 100
mpls-te enable standard-complying
network 192.1.1.0 0.0.0.255
network 5.5.5.5 0.0.0.0
return
config
```

```
interface tunnel 10
tunnel-protocol mpls te
destination 6.6.6.6
mpls te tunnel-id 10
mpls te signal-protocol rsvp-te
mpls te reserved-for-binding
mpls te commit
quit
tunnel-policy ethpw-plcy
tunnel binding destination 6.6.6.6 te tunnel 10
quit
pw-para 10
peer-address 6.6.6.6
pw-type ethernet tagged
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy ethpw-plcy
quit
vlan 3001
service-port vlan 3001 eth 0/4/0 multi-service user-vlan 20 rx-cttr 6 tx-cttr 6
pw-ac-binding vlan 3001 pw 10 static transmit-label 8500 receive-label 8600
```

18.3.4 Example: Configuring the TDM PWE3 to Emulate TDM Services on the IP Network

The MA5600T/MA5603T supports SAToP encapsulation for non-frame E1 signals and implements the TDM PWE3 emulation service after IP-encapsulating the signals. In this way, the MA5600T/MA5603T provides emulated TDM private line service over the IP network.

Service Requirements

- To make full use of legacy TDM line and equipment, and replace legacy DDN network and ISDN PRI PBX convergence network.
- To perform MPLS over IP encapsulation on the E1 data aggregated by the Nx64k private line and ISDN PRI PBX, and transmit the data upstream as IP packets to the DDN network or SDH network.

Prerequisite

- The H802EDTB board and SPUB board are installed and work in the normal state.
- The working mode of the H802EDTB board is set to SAToP by running the **board workmode** command.
- A static route or dynamic route is successfully configured on each device over the network so that the IP routes between LSRs are reachable. For details, see **3.4 Configuring the Route**.

Context

The implementation process of TDM PWE3 is as follows:

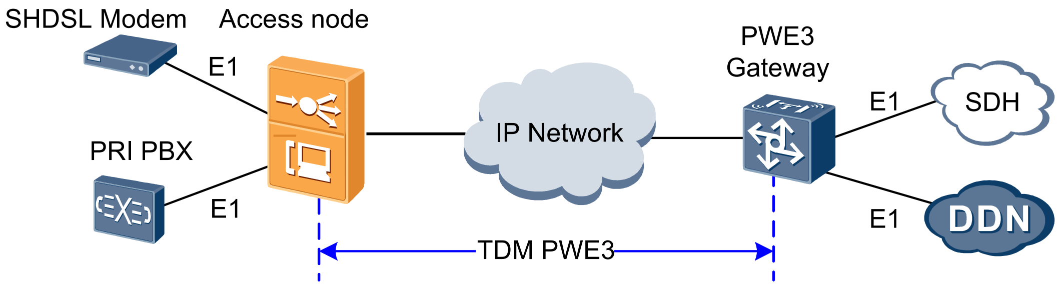
1. The data of the Nx64k private line service or ISDN PRI PBX service is converged and then transmitted to the H802EDTB board of the MA5600T/MA5603T.
2. After performing SAToP processing (adding CW control word and RTP header) on the E1 data, the H802EDTB board sends the data to the SPUB board through the control board.
3. After performing the PW and MPLS encapsulation on the packets, the SPUB board adds the ETH header to the packets, and then sends them to the control board.

4. The control board performs Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the PSN network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores the E1 signals from the packets and then sends them to the DDN network or SDH network.

Networking

Figure 18-6 shows an example network of TDM PWE3 (IP-based).

Figure 18-6 Example network of TDM PWE3 (IP-based)



Data Plan

Table 18-7 lists the data plan for configuring TDM PWE3 (IP-based).

Table 18-7 Data plan for configuring TDM PWE3 (IP-based)

Parameter	Data
H802EDTB board	Board slot: 0/3 E1 port: 0/3/1
SPUB board	Board slot: 0/5
MPLS	VLAN for MPLS forwarding: VLAN 4001 IP address of VLAN interface 4001: 10.50.50.50/24 MPLS LSR ID: 3.3.3.3 Global MPLS LDP: enabled MPLS Layer 2 VPN: enabled
PW parameters	PW ID: 2 Peer IP address: 9.9.9.9 Template type: TDM SAToP E1 PW load time: 125 µs Jitter buffer size: 2500 µs Control word: enabled RTP: enabled VCCV: enabled

Parameter	Data
Tunnel	Tunnel interface ID: 10 Tunnel ID: 10 Encapsulation protocol of the tunnel interface at the data link layer: IP Policy name: **ip_policy**
Tx clock of the E1 port	Network clock, recovered from PW2

Procedure

Step 1 Configure a loopback interface.

Set the ID of the loopback interface to 0 and its IP address to 3.3.3.3/32.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 3.3.3.3 32
huawei(config-if-loopback0)#quit
```

Step 2 Enable basic MPLS functions.

Set the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 3.3.3.3
```

Enable global MPLS.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host  //set up an LSP by triggering the LDP through
the host address
huawei(config-mpls)#quit
```

Enable Layer 2 VPN.

```
huawei(config)#mpls l2vpn
```

Enable global LDP.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

NOTE

- Only one session can exist between two LSRs and a local LDP session takes priority over a remote LDP session. To simplify the configuration, assume that the MA5600T/MA5603T is directly connected to the PTN. Hence, you need to enable only the LDP function (the local LDP session is automatically set up after the LDP function is enabled).
- If the MA5600T/MA5603T is not directly connected to the PTN, after the LDP function is enabled, run the **mpls ldp remote-peer** command to create an LDP remote peer and then enter the remote peer mode. Then, run the **remote-ip***ip-addr* command to specify the ID of the remote LSR.
- For detailed configurations, see **12.1.2 Configuring the LDP LSP**.

Step 3 Configure a VLAN and enable MPLS for the VLAN and the VLAN interface.

Add VLAN 4001 for forwarding MPLS packets and add an upstream port to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19/0
```

Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

Set the IP address of VLAN interface 4001 to 10.50.50.50/24 and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 4 Configure a route.

PWE3 has no special requirements for the routing policy. A static route, or dynamic RIP, or OSPF route can be configured. An OSPF dynamic route is recommended because OSPF supports MPLS RSVP-TE extension.

Set the OSPF process ID to 100 and OSPF area ID to 1. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 5 Configure a PWE3 outer tunnel.

Set the tunnel ID to 10 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS IP.

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls ip
```

Set the destination IP address of the tunnel to the LSR ID of the PTN 9.9.9.9.

```
huawei(config-if-tunnel10)#destination 9.9.9.9
```

Commit the configuration and then quit the MPLS tunnel mode:

```
huawei(config-if-tunnel10)#mpls ip commit
huawei(config-if-tunnel10)#quit
```

Step 6 Configure the tunnel policy.

Set the policy name to **ip_policy**.

```
huawei(config)#tunnel-policy ip_policy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-ip_policy)#tunnel select-seq ip load-balance-number 1
huawei(config-tunnel-policy-ip_policy)#quit
```

Step 7 Configure PW parameters.

1. Create PW 2 and enter the PW parameter mode.
   ```
   huawei(config)#pw-para 2
   ```
2. Configure the loopback interface IP address of the remote PTN device.

   Set the loopback interface IP address to 9.9.9.9.
   ```
   huawei(config-pw-para-2)#peer-address 9.9.9.9
   ```
3. Set the PW type to TDM SAToP E1.
   ```
   huawei(config-pw-para-2)#pw-type tdm satop e1
   ```
4. Configure the PW load time.

   Set the load time to 125 μs.

```
huawei(config-pw-para-2)#tdm-load-time satop e1 loadtime 125
```

5. Enable RTP. After RTP is enabled, PW packets of the TDM type contain the RTP control header. By default, RTP is disabled.

   NOTE

   The RTP configuration must be the same as that on the PTN.

   ```
   huawei(config-pw-para-2)#rtp enable
   ```

6. (Optional) Configure the jitter buffer size. The jitter buffer can effectively prevent jitter and latency. Only PW of the TDM type support the jitter buffer configuration. By default, the jitter buffer size is 2000 μs.

   NOTE

   The value range of the jitter buffer size is 500-32000 and the value must be an integer multiple of 125. Configure this value according to actual conditions. In this example, the jitter buffer size is set to 2500 μs.

   ```
   huawei(config-pw-para-2)#jitter-buffer buffer-size 2500
   ```

7. Configure the PW to support the control word.

   ```
   huawei(config-pw-para-2)#control-word
   ```

8. Enable virtual circuit connectivity verification (VCCV).

   ```
   huawei(config-pw-para-2)#vccv cc cw alert ttl cv lsp-ping
   ```

9. Configure the tunnel policy used by the PW parameters.

   Set the tunnel policy name to **ip-policy**.

   ```
   huawei(config-pw-para-2)#tnl-policy ip_policy
   huawei(config-pw-para-2)#quit
   ```

Step 8 Create a TDM connection.

Set the TDM connection ID to 1, type to PWE3, and ID of the E1 port on the H802EDTB board to 0/3/1.

```
huawei(config)#tdm-connect connectid 1 tdm pwe3-uplink 0/3 e1 0/3/1
```

Step 9 Bind the TDM connection to the PW to create the PW service of the TDM type.

Bind TDM connection 1 to PW2.

```
huawei(config)#pw-ac-binding tdm 1 pw 2
```

Step 10 Confirm that the PW is in the normal state.

On the OLT, run the **display pw** or **display pw-ac-binding** command to query the PW status. Confirm that the PW state is normal (**up**).

```
huawei(config)#display pw-ac-binding tdm 1
  Total : 1  (Up/Down :    1/0           Static/LDP :    0/1)
  ----------------------------------------------------------------------------
  TDM              PW         PW    PROTO  RECEIVE TRNS    PW
  ID               ID         STATE TYPE   LABEL   LABEL   INDEX
  ----------------------------------------------------------------------------
   1               2          up    LDP    ---     ---     2
  ----------------------------------------------------------------------------
  Note   : F--Frame, S--Slot, P--Port
          *: Secondary
```

Step 11 Configure clock synchronization on the E1 port.

Configure the recovery clock source of the H802EDTB board. In the recovery clock mode, the receive end recovers the clock of the transmit end according to the average arrival rate of the received SAToP packets. In this example, clock signals are extracted from PW2 to serve as the recovery clock of a board.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#adapt-clock-source clock-source 0 2
```

Configure the Tx clock of E1 port 0/3/1 on the H802EDTB board as the network-side clock. That is, configure the clock recovered from a TDM PW as the Tx clock of a port, implementing voice service synchronization.

```
huawei(config-edt-0/3)#clock-work 1 net
```

----End

Result

After a network is restructured, the long-term bit error ratio and latency meet the requirements for actual applications, the Nx64k private line service or ISDN PRI PBX service runs normally, and the operation method for end users is not changed.

Configuration File

```
interface loopback 0
ip address 3.3.3.3 32
quit
mpls lsr-id 3.3.3.3
mpls
lsp-trigger host
quit
mpls l2vpn
mpls ldp
quit
vlan 4001 smart
port vlan 4001 0/19/0
mpls vlan 4001
interface vlanif 4001
ip address 10.50.50.50 24
mpls
mpls ldp
quit
ospf 1
area 100
network 10.50.50.0 0.0.0.255
network 3.3.3.3 0.0.0.0
return
interface tunnel 10
tunnel-protocol mpls ip
destination 9.9.9.9
mpls ip commit
quit
tunnel-policy ip_policy
tunnel select-seq ip load-balance-number 1
quit
pw-para 2
peer-address 9.9.9.9
pw-type tdm satop e1
tdm-load-time satop e1 loadtime 125
rtp enable
jitter-buffer buffer-size 2500
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy ip_policy
quit
tdm-connect connectid 1 tdm pwe3-uplink 0/3 e1 0/3/1
pw-ac-binding tdm 1 pw 2
interface edt 0/3
adapt-clock-source clock-source 0 2
clock-work 1 net
```

18.3.5 Example: Configuring the TDM PWE3 to Emulate TDM Services on the MPLS Network

The MA5600T/MA5603T supports the SAToP encapsulation for non-frame E1 signals and implements the TDM PWE3 emulation service after MPLS-encapsulating the signals. In this way, the MA5600T/MA5603T provides emulated TDM private line service over the MPLS network.

Service Requirements

- To make full use of legacy TDM line and equipment, and replace legacy DDN network and ISDN PRI PBX convergence network.
- To perform MPLS over IP encapsulation on the E1 data aggregated by the Nx64k private line and ISDN PRI PBX, and transmit the data upstream as MPLS packets to the DDN network or SDH network.

Prerequisite

- The H802EDTB board and SPUB board are installed and work in the normal state.
- The working mode of the H802EDTB board is set to SAToP by running the **board workmode** command.
- A static route or dynamic route is successfully configured on each device over the network so that the IP routes between LSRs are reachable. For details, see **3.4 Configuring the Route**.

Context

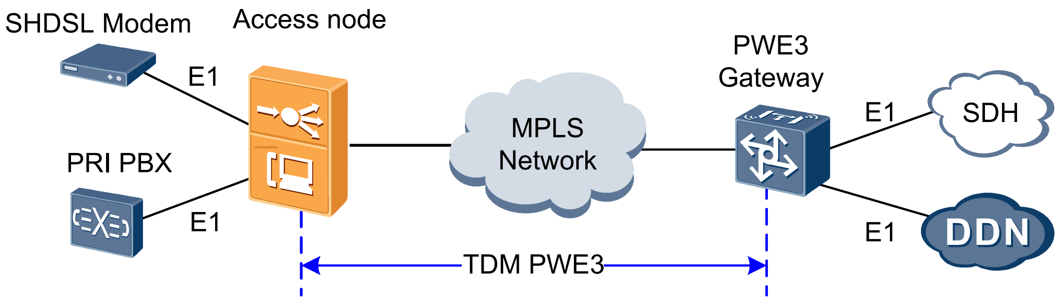
The implementation process of TDM PWE3 is as follows:

1. The data of the Nx64k private line service or ISDN PRI PBX service is converged and then transmitted to the H802EDTB board of the MA5600T/MA5603T.
2. After performing SAToP processing (adding CW control word and RTP header) on the E1 data, the H802EDTB board sends the data to the SPUB board through the control board.
3. After performing the PW and MPLS encapsulation on the packets, the SPUB board adds the ETH header to the packets, and then sends them to the control board.
4. The control board performs Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the PSN network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores the E1 signals from the packets and then sends them to the DDN network or SDH network.

Networking

Figure 18-7 shows an example network of TDM PWE3 (MPLS-based).

Figure 18-7 Example network of TDM PWE3 (MPLS-based)



Data Plan

Table 18-8 lists the data plan for configuring TDM PWE3 (MPLS-based).

Table 18-8 Data plan for configuring TDM PWE3 (MPLS-based)

Parameter	Data
H802EDTB board	Board slot: 0/4 E1 port: 0/4/5
SPUB board	Board slot: 0/5
MPLS	VLAN for MPLS forwarding: 4001 IP address of VLAN interface 4001: 10.50.50.50/24 MPLS LSR ID: 3.3.3.3 Global MPLS LDP: enabled MPLS LDP for VLANIF 4001: enabled MPLS Layer 2 VPN: enabled
PW parameters	PW ID: 3 Peer IP address: 10.10.10.10 PW type: TDM SAToP E1 PW load time: 125 μs Jitter buffer size: 2500 μs Control word: enabled RTP: enabled VCCV: enabled
Tx clock of the E1 port	Network clock, recovered from PW 3

Procedure

Step 1 Configure a loopback interface.

Set the ID of the loopback interface to 0 and its IP address to 3.3.3.3/32.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 3.3.3.3 32
huawei(config-if-loopback0)#quit
```

Step 2 Enable basic MPLS functions.

Set the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 3.3.3.3
```

Enable global MPLS.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host  //set up an LSP by triggering the LDP through
the host address
huawei(config-mpls)#quit
```

Enable Layer 2 VPN.

```
huawei(config)#mpls l2vpn
```

Enable global LDP.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

NOTE

- Only one session can exist between two LSRs and a local LDP session takes priority over a remote LDP session. To simplify the configuration, assume that the MA5600T/MA5603T is directly connected to the PTN. Hence, you need to enable only the LDP function (the local LDP session is automatically set up after the LDP function is enabled).
- If the MA5600T/MA5603T is not directly connected to the PTN, after the LDP function is enabled, run the **mpls ldp remote-peer** command to create an LDP remote peer and then enter the remote peer mode. Then, run the **remote-ip***ip-addr* command to specify the ID of the remote LSR.
- For detailed configurations, see **12.1.2 Configuring the LDP LSP**.

Step 3 Configure a VLAN and enable MPLS for the VLAN and the VLAN interface.

Add VLAN 4001 for forwarding MPLS packets and add an upstream port to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19/0
```

Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

Set the IP address of VLAN interface 4001 to 10.50.50.50/24 and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 4 Configure a route.

PWE3 has no special requirements for the routing policy. A static route, or dynamic RIP, or OSPF route can be configured. An OSPF dynamic route is recommended because OSPF supports MPLS RSVP-TE extension.

Set the OSPF process ID to 100 and OSPF area ID to 1. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 5 Configure PW parameters.

1. Create PW 3 and enter the PW parameter mode.
   ```
   huawei(config)#pw-para 3
   ```
2. Configure the loopback interface IP address of the remote PTN device in the PW.

   Set the loopback interface IP address to 10.10.10.10.
   ```
   huawei(config-pw-para-3)#peer-address 10.10.10.10
   ```
3. Set the PW type to TDM SAToP E1.
   ```
   huawei(config-pw-para-3)#pw-type tdm satop e1
   ```
4. Configure the PW load time.

   Set the load time to 125 μs.
   ```
   huawei(config-pw-para-3)#tdm-load-time satop e1 loadtime 125
   ```
5. (Optional) Enable RTP. After RTP is enabled, PW packets of the TDM type contain the RTP control header. By default, RTP is disabled.

   NOTE

   The RTP configuration must be the same as that on the PTN.
   ```
   huawei(config-pw-para-3)#rtp enable
   ```
6. (Optional) Configure the jitter buffer size. The jitter buffer can effectively prevent jitter and delay. Only PW parameters of the TDM type support the jitter buffer configuration. By default, the jitter buffer size is 2000 μs.

   NOTE

   The value range of the jitter buffer is 500-32000 and the value must be an integer multiple of 125. You can configure this value according to actual conditions. In this example, the jitter buffer size is set to 2500 μs.
   ```
   huawei(config-pw-para-3)#jitter-buffer buffer-size 2500
   ```
7. Configure the PW parameter to support the control word.
   ```
   huawei(config-pw-para-3)#control-word
   ```
8. Enable virtual circuit connectivity verification (VCCV).
   ```
   huawei(config-pw-para-3)#vccv cc cw alert ttl cv lsp-ping
   ```

Step 6 Create a TDM connection.

Set TDM connection ID to 2, type to PWE3, and ID of the E1 port of the H802EDTB board to 0/4/5.

```
huawei(config)#tdm-connect connectid 2 tdm pwe3-uplink 0/4 e1 0/4/5
```

Step 7 Bind the TDM connection to the PW to create the PW service of the TDM type.

Bind TDM connection 2 to PW 3.

```
huawei(config)#pw-ac-binding tdm 2 pw 3
```

Step 8 Confirm that the PW is in the normal state.

On the OLT, run the **display pw** or **display pw-ac-binding** command to query the PW status. Confirm that the PW state is normal (**up**).

```
huawei(config)#display pw-ac-binding tdm 2
  Total : 1  (Up/Down :    1/0          Static/LDP :    0/1)
  -----------------------------------------------------------------------------
  TDM              PW         PW    PROTO   RECEIVE TRNS    PW
  ID               ID         STATE TYPE    LABEL   LABEL   INDEX
```

```
 ----------------------------------------------------------------------------
  2              3          up    LDP    ---     ---     3
 ----------------------------------------------------------------------------
 Note  : F--Frame, S--Slot, P--Port
         *: Secondary
```

Step 9 Configure clock synchronization on the E1 port.

Configure the recovery clock source of the H802EDTB board. In the recovery clock mode, the receive end recovers the clock of the transmit end according to the average arrival rate of the received SAToP packets. In this example, clock signals are extracted from PW 3 to serve as the recovery clock of a board.

```
huawei(config)#interface edt 0/4
huawei(config-edt-0/4)#adapt-clock-source clock-source 0 3
```

Configure the Tx clock of E1 port 0/4/5 on the H802EDTB board as the network-side clock. That is, configure the clock recovered from a TDM PW as the Tx clock of a port, implementing voice service synchronization.

```
huawei(config-edt-0/4)#clock-work 5 net
```

----End

Result

After a network is restructured, the long-term bit error ratio and latency meet the requirements for actual applications, the Nx64k private line service or ISDN PRI PBX service runs normally, and the operation method for end users is not changed.

Configuration File

```
interface loopback 0
ip address 3.3.3.3 32
quit
mpls lsr-id 3.3.3.3
mpls
lsp-trigger host
quit
mpls l2vpn
mpls ldp
quit
vlan 4001 smart
port vlan 4001 0/19/0
mpls vlan 4001
interface vlanif 4001
ip address 10.50.50.50 24
mpls
mpls ldp
quit
ospf 1
area 100
network 10.50.50.0 0.0.0.255
network 3.3.3.3 0.0.0.0
return
pw-para 3
peer-address 10.10.10.10
pw-type tdm satop e1
tdm-load-time satop e1 loadtime 125
rtp enable
jitter-buffer buffer-size 2500
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy ip_policy
quit
tdm-connect connectid 1 tdm pwe3-uplink 0/4 e1 0/4/5
```

```
pw-ac-binding tdm 2 pw 3
interface edt 0/4
adapt-clock-source clock-source 0 3
clock-work 5 net
```

18.3.6 Configuring TDM E1/T1 Private Line Service

In the GPON FTTO networking scenario, ONUs access enterprise time division multiplexing (TDM) service in E1/T1 access mode, and transmits the data to the SDH network over the GPON network which supports long-distance transmission and high bandwidth. In this way, uniform deployment of E1/T1 service is achieved.

Service Requirements

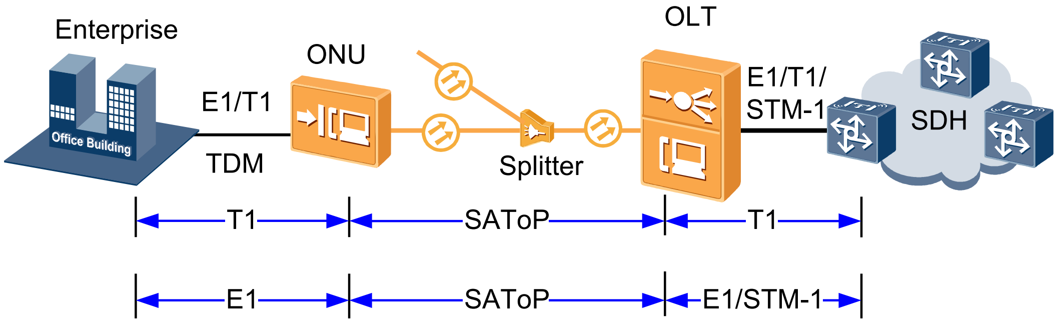
- Existing SDH resources are utilized efficiently. In this way, carriers' existing investments are protected and enterprise users in different regions are won.
- Services are received over optical fibers, reducing investment in copper cables between enterprises and the SDH network.
- The standardized user-side ports facilitate deployment and maintenance.

Application Scenario

As shown in **Figure 18-8**, the ONU accesses enterprise E1/T1 service through standardized hardware ports, and transmits data to the OLT over the GPON line after performing structure-agnostic time division multiplexing over packet (SAToP) encapsulation on the service. After receiving the signals, the OLT restores E1/T1 signals and transmits the signals to the SDH network.

- For carriers, with this networking, they can win enterprise users with GPON lines which support long-distance transmission and high bandwidth. With the trend of fiber-in and copper-out, deployment of GPON lines can reduce deployment costs of copper cables and support service expansion.
- For enterprise users, with GPON access, they can reduce fees spent in leasing lines.

Figure 18-8 E1/T1 access in SAToP mode



Prerequisite

Required hardware is ready.

- Control board on the OLT: SCUN+CKMC

- Upstream board on the OLT: EDTB (for E1/T1 upstream transmission)
- Service board on the OLT: GPBD
- ONU: MA5612 (configured with the E81A board) or MA5628

Data Plan

Table 18-9 and **Table 18-10** provide key data plans for the OLT and the ONU.

Table 18-9 Key data plan for the OLT

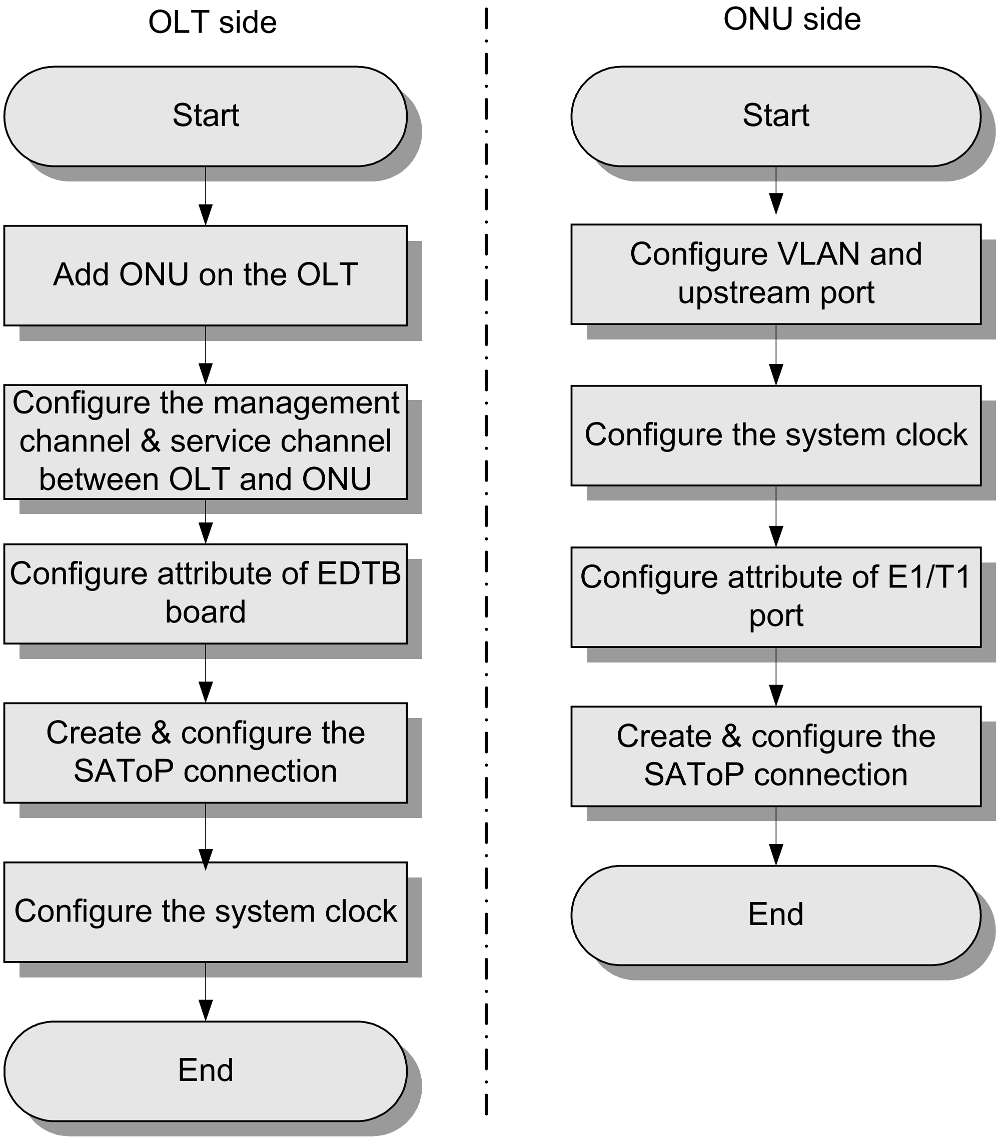
Configuration Item	Data	Remarks
GPON line attributes	DBA profile: type1. The fixed bandwidth is 64 Mbit/s. The default DBA bandwidth allocation mode at the GPON port is minimum bandwidth delay. ONU line profile ID: 10 ONU management mode: SNMP ONU ID: 1 ONU authentication mode: SN authentication GPON port: 0/3/1	The recommended bandwidth for each E1/T1 port is 8192 kbit/s, and 65536 kbit/s in total for eight ports.
EDTB	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: obtained dynamically Local UDP port number: 50050	MAC address configuration modes (the MAC address is statically configured or dynamically obtained) at two ends must be consistent to establish a connection. You are advised to set MAC address configuration mode to dynamic, which facilitates configuration and maintenance. The UDP port cannot be the port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.
VLAN ID and IP address	In-band management VLAN ID: 8 In-band management IP address: 192.168.50.10/24 Service VLAN ID: 100	To telnet to the ONU from the OLT and then configure the ONU, you must configure the in-band management VLANs and IP addresses of the OLT and the ONU on the OLT.
System clock	E1/T1 line clock: 0/5/0	The GPON network transmits clock information to the ONU.

Table 18-10 Key data plan for the ONU

Configuration Item	Data	Remarks
VLAN ID and IP address	In-band management VLAN ID: 8 In-band management IP address: 192.168.50.20/24 Service VLAN ID: 100	-
E1/T1 port	E1 port number: 0/1/0 Port working mode: ● E1: UDT ● T1: SDT Transmit clock of the port: system clock TDM virtual channel link (VCL) ID: 10 Board IP address: 10.10.50.20 Board MAC address: obtained dynamically Local UDP port number: 50050	The UDP port cannot be the port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Configuration Flowchart

The OLT/ONU configuration process is as follows.


OLT side
Start
Add ONU on the OLT
Configure the management channel & service channel between OLT and ONU
Configure attribute of EDTB board
Create & configure the SAToP connection
Configure the system clock
End
ONU side
Start
Configure VLAN and upstream port
Configure the system clock
Configure attribute of E1/T1 port
Create & configure the SAToP connection
End

Procedure

- Configure the OLT.
  1. Add an ONU.
     a. Configure a DBA profile.

        The profile name is tdm_64mbps and the type is Type1. The fixed bandwidth is 64 Mbit/s. Enable the bandwidth compensation function, and set the DBA bandwidth allocation mode to minimum bandwidth delay mode for GPON port 0/3/1.

```
huawei(config)#dba-profile add profile-name tdm_64mbps type1 fix
65536 bandwidth_compensate yes
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-
loop-delay
```

     b. Configure an ONU line profile.

Create GPON ONU line profile 10. Bind T-CONT 10 to the default DBA profile named dba-profile_1, and bind T-CONT 1 to the DBA profile named TDM.

```
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_64mbps
```

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

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 10 priority-
queue 0
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 1 priority-
queue 0
```

Configure the mapping between the GEM port and the ONU-side service to the VLAN mapping mode (default), map the service port of management VLAN 8 to GEM port 0, and map the SAToP traffic streams of VLAN 100 to GEM port 1.

```
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)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. Add an ONU.

```
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
```

d. Confirm that the ONU goes online normally.

```
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, 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.

2. Configure the management channel from the OLT to the ONU.

Create management VLAN 8, and set the in-band management IP address to 192.168.50.10/24 for the OLT.

```
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
```

Set 192.168.50.20/24 as the static IP address of the ONU and VLAN 8 (the same as that of the OLT) as the management VLAN of the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address
192.168.50.20 mask 255.255.255.0 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Configure an in-band 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 in-band 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
```

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.

3. Configure the service channel between the OLT and the ONU.

Set the service port ID to 1, SVLAN ID to 100, GEM port ID to 1, and CVLAN ID to 100. Rate limit 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)#vlan 100 smart
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
```

4. Configure EDTB board attributes.

   Set the board working mode to SAToP.

   ```
   huawei(config)#interface edt 0/5
   huawei(config-if-edt-0/5)#board workmode satop
   ```

   Configure the access mode and frame format.

   - For E1 access, run the following command:
     ```
     huawei(config-if-edt-0/5)#tdm access-mode E1
     ```
   - For T1 access, run the following commands:
     ```
     huawei(config-if-edt-0/5)#tdm access-mode T1
     huawei(config-if-edt-0/5)#frame-mode 0 esf
     ```

     NOTE

     The T1 frame format must be the same as that on the SDH side.

   Configure the IP address of the E1/T1 port on the EDTB board. The following uses port 0/5/0 as an example. Set the IP address to 10.10.50.10.

   ```
   huawei(config)#interface edt 0/5
   huawei(config-if-edt-0/5)#set ip-address 10.10.50.10
   huawei(config-if-edt-0/5)#quit
   ```

5. Create a SAToP connection.

   Create TDM VCL 10.

   - For E1 access, set the TDM VCL type to SAToP.
     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/5/0
     ```
   - For T1 access, set the TDM VCL type to CESoP. Set the timeslot to 0xfffffff.
     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 cesop 0/5/0 timeslot 0xffffff
     ```

   Create a SAToP connection at E1/T1 port 0/5/0. Set SVLAN to 100, local UDP port number to 50050, the remote IP address (the IP address of the E1/T1 access board on the ONU) to 10.10.50.20, and remote UDP port number to 50050. The remote MAC address is obtained dynamically.

   NOTE

   During an SAToP connection setup, the EDTB board requires that the local UDP port ID must be the same as the remote UDP port ID of the ONU. Actually, they have the following relationship: Local UDP + 50048 on the OLT side = Remote UDP on the ONU side.

   ```
   huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 2 remote-ip
   10.10.50.20 remote-udp 50050
   ```

   You can also create a SAToP connection by configuring the MAC address statically. Assume that the remote MAC address (the MAC address of the E1 access board on the ONU, which can be queried by running the **display cesop-mac-address** command on the ONU) is 00e0-fc01-0450. You can create a SAToP connection in static mode as follows:

   ```
   huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 2 remote-mac
    00e0-fc01-0450 remote-ip 10.10.50.20 remote-udp 50050
   ```

6. (Optional) Configure attributes of the SAToP connection.

   NOTE

   The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. In normal cases, use the system default values.

   - Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.

- Run the **cesop encap** command to set SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to set the buffer depth of the SAToP packet. The default buffer depth is 2000 us.
- Run the **cesop loadtime** command to set the load time of the SAToP packet. The default load time is 125 us.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

7. Configure the system clock.

   Use the E1/T1 line clock input from EDTB port 0/5/0 as the system clock 0. Set the priority to **0** (highest priority).

   ```
   huawei(config)#clock source 0 0/5/0
   huawei(config)#clock priority system 0
   ```

8. 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 upstream VLAN and upstream port of the ONU.

   Create upstream VLAN 100, and add upstream port 0/0/0 to VLAN 100.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/0 0
   ```

2. Configure the system clock.

   The system clock of the OLT is applied to the ONU through the PON port on the OLT, achieving clock synchronization between the OLT and the ONU.

   ```
   huawei(config)#clock source 0 0/0/0
   huawei(config)#clock priority system 0
   ```

3. Configure E1/T1 port attributes.

   Configure the IP address of TDM service board 0/1 as 10.10.50.20.

   ```
   huawei(config)#interface tdm 0/1
   huawei(config-if-tdm-0/1)#set ip-address 10.10.50.20
   ```

   Configure the port working mode and transmit clock.

   - For E1 access, set the working mode to UDT and the system clock as the transmit clock.

     ```
     huawei(config-if-tdm-0/1)#port 0 udt system
     ```

   - For T1 access, set the working mode to SDT, set the system clock as the transmit clock, and enable ESF check.

     ```
     huawei(config-if-tdm-0/1)#port 0 sdt system esf enable
     ```

4. Create a SAToP connection.

   Create TDM VCL 10.

   - For E1 access, set the TDM VCL type to SAToP.

     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/1/0
     ```

   - For T1 access, set the TDM VCL type to CESoP. Set the timeslot to 0xfffffff.

     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 cesop 0/1/0 timeslot 0xffffff
     ```

Create a SAToP connection at TDM port 0/1/0. Set SVLAN to 100, local UDP port number to 50050, the remote IP address (the IP address of the EDTB board on the OLT) to 10.10.50.10, and remote UDP port number to 50050. The remote MAC address is obtained dynamically.

```
huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 50050 remote-ip
10.10.50.10 remote-udp 50050
```

NOTE

You can also create a SAToP connection by configuring the MAC address statically. Assume that the remote MAC address (the MAC address of the EDTB board on the OLT) is 0800-3E32-5310. You can create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 50050 remote-mac
 0800-3E32-5310 remote-ip 10.10.50.10 remote-udp 50050
```

5. (Optional) Configure attributes of the SAToP connection.

   NOTE

   The attributes of the SAToP connection on the ONU must be consistent with those on the OLT. In normal cases, use the system default values.

   - Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
   - Run the **cesop encap** command to set SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
   - Run the **cesop jitter-buffer** command to set the buffer depth of the SAToP packet. The default buffer depth is 2000 us.
   - Run the **cesop loadtime** command to set the load time of the SAToP packet. The default load time is 125 us.
   - Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

6. Save the data.

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

----End

Result

1. Use the networking shown in **Figure 18-8**. Connect a test instrument to the upstream port of the OLT, and perform a local loopback at E1/T1 port 0/1/0 of the ONU using the **loopback 0 local** command. Use the test instrument to transmit packets continuously. The 12-hour BER should be less than 1E-9.
2. Services of an enterprise can be provisioned normally.

18.3.7 Configuring TDM E1/T1 Private Line Service (OLT Cascading)

In the GPON FTTO networking scenario, ONUs access enterprise time division multiplexing (TDM) service in E1/T1 access mode, and transmits the data to the SDH network in OLT cascading mode over the GPON network which supports long-distance transmission and high bandwidth. In this way, uniform deployment of E1/T1 service is achieved.

Service Requirements

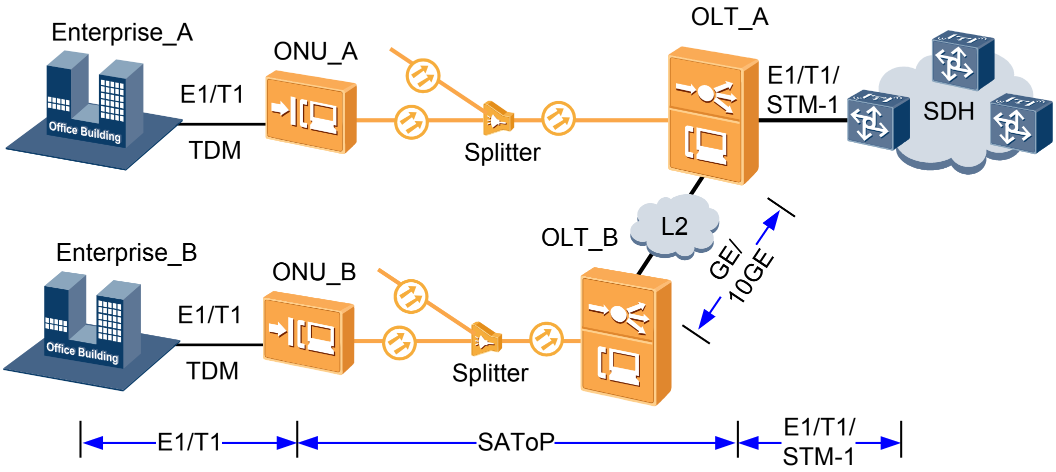
- Existing SDH resources are utilized efficiently. In this way, carriers' existing investments are protected, and enterprise users with no SDH resources in different regions are won.
- Services are received over optical fibers, reducing investment in copper cables between enterprises and the SDH network.
- The standardized user-side ports facilitate deployment and maintenance.

Application Scenario

As shown in **Figure 18-9**, a carrier's SDH network is migrated gradually. In a city, there are only some nodes (for example, OLT_A in the following figure) can transmit signals upstream to the SDH network through STM-1 ports, and other nodes (for example, OLT_B in the following figure) must access SDH resources through GE/10GE ports. In this scenario, ONU_B accesses the E1/T1 service in SAToP mode, and transmits the service to the OLT at the local site (OLT_B) over the GPON line. OLT_B transparently transmits the service to another OLT with SDH resources (OLT_A) through GE/10GE ports.

- For carriers, with this networking, they can win enterprise users who have no SDH resources with GPON lines which support long-distance transmission and high bandwidth. With the trend of fiber-in and copper-out, deployment of GPON lines can reduce deployment costs of copper cables and support service expansion.
- For enterprise users, with GPON access, they can reduce fees spent in leasing lines.

Figure 18-9 E1/T1 access in SAToP mode



Prerequisite

Required hardware is ready.

Equipment	Configuration
OLT_A	● Control board: SCUN+CKMC ● GPON service board: GPBD ● Upstream board: EDTB ● Cascaded service board: – GE port: GICK or OPGD – 10GE port: X2CS **NOTE** The E1/T1 service can also be transmitted from ONU_A to OLT_A in SAToP mode. For corresponding configurations, see **18.3.6 Configuring TDM E1/T1 Private Line Service**.
OLT_B (cascading)	● Control board: SCUN+CKMC ● GPON service board: GPBD ● Upstream board: – GE port: GICK – 10GE port: X2CS
ONU_B	MA5612 (configured with the E81A board) or MA5628

Data Plan

Table 18-11, **Table 18-12** and **Table 18-13** provide the key data plan.

Table 18-11 Key data plan for OLT_A

Configuration Item	Data	Remarks
OPGD	Port: 0/2/1	Assume that OLT_A is cascaded with OLT_B using the OPGD board. Then you need to set the network role of the OPGD board to **cascade**.

Configuration Item	Data	Remarks
EDTB	Port: 0/5/0 Board IP address: 10.10.50.30 Board MAC address: obtained dynamically Local UDP port number: 50050	MAC address configuration modes (the MAC address is statically configured or dynamically obtained) at two ends must be consistent to establish a connection. You are advised to set MAC address configuration mode to dynamic, which facilitates configuration and maintenance. The UDP port cannot be the port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.
VLAN ID and IP address	In-band management VLAN ID: 8 In-band management IP address: 192.168.50.30/24 Service VLAN ID: 100	To telnet to another OLT or ONU from the OLT and then configure the OLT or ONU, you must configure the in-band management VLANs and IP addresses of the OLT on the OLT. If the management IP address and the IP address of OLT_B or ONU_B are not in the same network segment, you also need to configure routes.
System clock	E1/T1 line clock: 0/5/0	The system clock is obtained from the SDH line and transmitted to cascaded OLT_B through GE/ 10GE ports.

Table 18-12 Key data plan for OLT_B

Configuration Item	Data	Remarks
GPON line attributes	DBA profile: type1. The fixed bandwidth is 64 Mbit/s. The default DBA bandwidth allocation mode at the GPON port is minimum bandwidth delay. ONU line profile ID: 10 ONU management mode: SNMP ONU ID: 1 ONU authentication mode: SN authentication GPON port: 0/3/1	The recommended bandwidth for each E1/T1 port is 8192 kbit/s, and 65536 kbit/s in total for eight ports.
VLAN ID and IP address	Service VLAN ID: 100 In-band management VLAN ID: 8 In-band management IP address: 192.168.50.10/24	Use an optical fiber to connect the OPGD board on OLT_A and the upstream port on the GICK board on OLT_B to achieve physical cascading. To telnet to the ONU from the OLT and then configure the ONU, you must configure the in-band management VLANs and IP addresses of the OLT and the ONU on the OLT.
System clock	E1/T1 line clock: 0/5/0	The GPON network transmits clock information to the ONU.

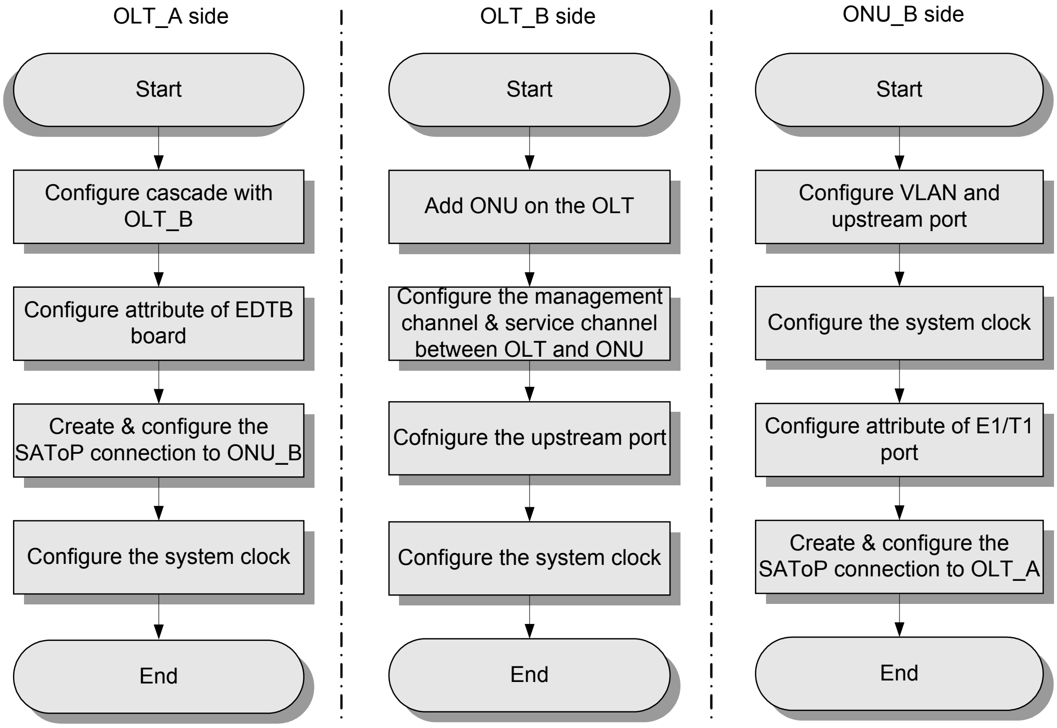
Table 18-13 Key data plan for the ONU

Configuration Item	Data	Remarks
VLAN ID and IP address	In-band management VLAN ID: 8 In-band management IP address: 192.168.50.20/24 Service VLAN ID: 100	-

Configuration Item	Data	Remarks
E1/T1 port	E1 port number: 0/1/0 Port working mode: ● E1: UDT ● T1: SDT Transmit clock of the port: system clock TDM virtual channel link (VCL) ID: 10 Board IP address: 10.10.50.20 Board MAC address: obtained dynamically Local UDP port number: 50050	The UDP port cannot be the port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Configuration Flowchart

The OLT/ONU configuration process is as follows.


OLT_A side
Start
Configure cascade with OLT_B
Configure attribute of EDTB board
Create & configure the SAToP connection to ONU_B
Configure the system clock
End
OLT_B side
Start
Add ONU on the OLT
Configure the management channel & service channel between OLT and ONU
Cofnigure the upstream port
Configure the system clock
End
ONU_B side
Start
Configure VLAN and upstream port
Configure the system clock
Configure attribute of E1/T1 port
Create & configure the SAToP connection to OLT_A
End

Procedure

- Configure OLT_A.

  OLT_A has the following functions on the network:

1. In the downstream direction, creates SAToP connections with ONU_B; in the upstream direction, restores E1/T1 signals and transmits the signals to the SDH network.
2. Cascaded with OLT_B and transmits clock synchronization information downstream.

1. Configure the management VLAN and IP address.

   Create management VLAN 8, and set the management IP address to 192.168.50.30 and subnet mask to 255.255.255.0.

   ```
   huawei(config)#vlan 8 smart
   huawei(config)#interface vlanif 8
   huawei(config-if-vlanif8)#ip address 192.168.50.30 24
   ```

2. Configure cascading with OLT_B.

   Cascade OLT_A and OLT_B through GE port 0/2/1 on the OPGD board. Set the port attribute to **cascade**, and add the cascading port to VLAN 100.

   ```
   huawei(config)#interface opg 0/2
   huawei(config-if-opg-0/2)#network-role cascade
   huawei(config-if-opg-0/2)#quit
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/2 1
   ```

3. Configure EDTB board attributes.

   Set the board working mode to SAToP.

   ```
   huawei(config)#interface edt 0/5
   huawei(config-if-edt-0/5)#board workmode satop
   ```

   Configure the access mode and frame format.

   - For E1 access, run the following command:
     ```
     huawei(config-if-edt-0/5)#tdm access-mode E1
     ```
   - For T1 access, run the following commands:
     ```
     huawei(config-if-edt-0/5)#tdm access-mode T1
     huawei(config-if-edt-0/5)#frame-mode 0 esf
     ```

     NOTE

     The T1 frame format must be the same as that on the SDH side.

   Configure the IP address of the E1/T1 port on the EDTB board. The following uses port 0/5/0 as an example. Set the IP address to 10.10.50.10.

   ```
   huawei(config)#interface edt 0/5
   huawei(config-if-edt-0/5)#set ip-address 10.10.50.10
   huawei(config-if-edt-0/5)#quit
   ```

4. Create a SAToP connection.

   Create TDM VCL 10.

   - For E1 access, set the TDM VCL type to SAToP.
     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/5/0
     ```
   - For T1 access, set the TDM VCL type to CESoP. Set the timeslot to 0xfffffff.
     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 cesop 0/5/0 timeslot 0xffffff
     ```

   Create a SAToP connection at E1/T1 port 0/5/0. Set SVLAN to 100, local UDP port number to 50050, the remote IP address (the IP address of the E1/T1 access board on the ONU) to 10.10.50.20, and remote UDP port number to 50050. The remote MAC address is obtained dynamically.

   NOTE

   During an SAToP connection setup, the EDTB board requires that the local UDP port ID must be the same as the remote UDP port ID of the ONU. Actually, they have the following relationship: Local UDP + 50048 on the OLT side = Remote UDP on the ONU side.

```
huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 2 remote-ip
10.10.50.20 remote-udp 50050
```

You can also create a SAToP connection by configuring the MAC address statically. Assume that the remote MAC address (the MAC address of the E1 access board on the ONU, which can be queried by running the **display cesop-mac-address** command on the ONU) is 00e0-fc01-0450. You can create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 2 remote-mac
 00e0-fc01-0450 remote-ip 10.10.50.20 remote-udp 50050
```

5. (Optional) Configure attributes of the SAToP connection.

   NOTE

   The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. In normal cases, use the system default values.

   - Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
   - Run the **cesop encap** command to set SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
   - Run the **cesop jitter-buffer** command to set the buffer depth of the SAToP packet. The default buffer depth is 2000 us.
   - Run the **cesop loadtime** command to set the load time of the SAToP packet. The default load time is 125 us.
   - Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

6. Configure the system clock.

   Use the E1/T1 line clock input from EDTB port 0/5/0 as the system clock 0. Set the priority to **0** (highest priority).

   ```
   huawei(config)#clock source 0 0/5/0
   huawei(config)#clock priority system 0
   ```

7. Save the data.

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

- Configure OLT_B.

  OLT_B has the following functions on the network:

  1. Transmits SAToP-encapsulated packets in GEM frames over the GPON line.
  2. Transmits SAToP packets to OLT_A in Ethernet mode for decapsulation.
  3. Transmits clock synchronization information to ONU_B.

  1. Add an ONU.

     a. Configure a DBA profile.

     The profile name is tdm_64mbps and the type is Type1. The fixed bandwidth is 64 Mbit/s. Enable the bandwidth compensation function, and set the DBA bandwidth allocation mode to minimum bandwidth delay mode for GPON port 0/3/1.

     ```
     huawei(config)#dba-profile add profile-name tdm_64mbps type1 fix
     65536 bandwidth_compensate yes
     huawei(config)#interface gpon 0/3
     huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-
     loop-delay
     ```

     b. Configure an ONU line profile.

     Create GPON ONU line profile 10. Bind T-CONT 10 to the default DBA profile named dba-profile_1, and bind T-CONT 1 to the DBA profile named TDM.

```
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_64mbps
```

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

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 10 priority-
queue 0
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 1 priority-
queue 0
```

Configure the mapping between the GEM port and the ONU-side service to the VLAN mapping mode (default), map the service port of management VLAN 8 to GEM port 0, and map the SAToP traffic streams of VLAN 100 to GEM port 1.

```
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)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. Add an ONU.

```
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
```

d. Confirm that the ONU goes online normally.

```
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, 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.

2. Configure the management channel from the OLT to the ONU.

Create management VLAN 8, and set the in-band management IP address to 192.168.50.10/24 for the OLT.

```
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
```

Set 192.168.50.20/24 as the static IP address of the ONU and VLAN 8 (the same as that of the OLT) as the management VLAN of the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address
192.168.50.20 mask 255.255.255.0 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Configure an in-band 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 in-band 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
```

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.

3. Configure the service channel between the OLT and the ONU.

Set the service port ID to 1, SVLAN ID to 100, GEM port ID to 1, and CVLAN ID to 100. Rate limit 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)#vlan 100 smart
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
```

4. Configure the upstream port.

   Add upstream port 0/19/0 (on the GICK board) to VLAN 100.

   ```
   huawei(config)#port vlan 100 0/19 0
   ```

5. Configure the system clock.

   Obtain the system clock through the GICK board in synchronous Ethernet mode. The clock is transmitted to the ONU over the GPON line.

   ```
   huawei(config)#clock source 0 0/19/0
   huawei(config)#clock priority system 0
   ```

6. 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 upstream VLAN and upstream port of the ONU.

   Create upstream VLAN 100, and add upstream port 0/0/0 to VLAN 100.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/0 0
   ```

2. Configure the system clock.

   The system clock of the OLT is applied to the ONU through the PON port on the OLT, achieving clock synchronization between the OLT and the ONU.

   ```
   huawei(config)#clock source 0 0/0/0
   huawei(config)#clock priority system 0
   ```

3. Configure E1/T1 port attributes.

   Configure the IP address of TDM service board 0/1 as 10.10.50.20.

   ```
   huawei(config)#interface tdm 0/1
   huawei(config-if-tdm-0/1)#set ip-address 10.10.50.20
   ```

   Configure the port working mode and transmit clock.

   - For E1 access, set the working mode to UDT and the system clock as the transmit clock.

     ```
     huawei(config-if-tdm-0/1)#port 0 udt system
     ```

   - For T1 access, set the working mode to SDT, set the system clock as the transmit clock, and enable ESF check.

     ```
     huawei(config-if-tdm-0/1)#port 0 sdt system esf enable
     ```

4. Create a SAToP connection.

   Create TDM VCL 10.

   - For E1 access, set the TDM VCL type to SAToP.

     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/1/0
     ```

   - For T1 access, set the TDM VCL type to CESoP. Set the timeslot to 0xfffffff.

     ```
     huawei(config)#tdm-vcl tdm-vcl-id 10 cesop 0/1/0 timeslot 0xffffff
     ```

   Create a SAToP connection at TDM port 0/1/0. Set SVLAN to 100, local UDP port number to 50050, the remote IP address (the IP address of the EDTB board on the OLT) to 10.10.50.10, and remote UDP port number to 50050. The remote MAC address is obtained dynamically.

```
huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 50050 remote-ip
10.10.50.10 remote-udp 50050
```

NOTE

You can also create a SAToP connection by configuring the MAC address statically. Assume that the remote MAC address (the MAC address of the EDTB board on the OLT) is 0800-3E32-5310. You can create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 100 local-udp 50050 remote-mac
 0800-3E32-5310 remote-ip 10.10.50.10 remote-udp 50050
```

5. (Optional) Configure attributes of the SAToP connection.

   NOTE

   The attributes of the SAToP connection on the ONU must be consistent with those on the OLT. In normal cases, use the system default values.

   - Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
   - Run the **cesop encap** command to set SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
   - Run the **cesop jitter-buffer** command to set the buffer depth of the SAToP packet. The default buffer depth is 2000 us.
   - Run the **cesop loadtime** command to set the load time of the SAToP packet. The default load time is 125 us.
   - Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

6. Save the data.

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

----End

Result

1. Use the networking shown in **Figure 18-9**. Connect a test instrument to the upstream port of OLT_A, and perform a local loopback at E1/T1 port 0/1/0 of ONU_B using the **loopback 0 local** command. Use the test instrument to transmit packets continuously. The 12-hour BER should be less than 1E-9.
2. Services of an enterprise can be provisioned normally.

18.4 Example: Configuring TDM SHDSL for Transparently Transmitting the Narrowband Data Private Line Service

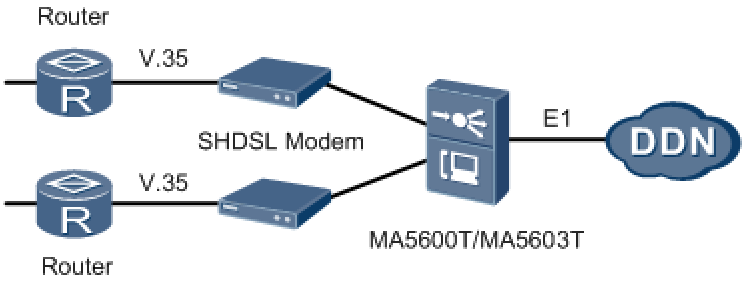
The TDM SHDSL extends the access distance. With the TDM SHDSL, the MA5600T/MA5603T transparently transmits user data to the digital data network (DDN). In this way, the twisted pair can be fully used and the E1 line deployment expense decreases.

Service Requirements

- Use the existing rich twisted pair resources for long-distance transmission, extending the DDN node.
- The user data is transparently transmitted on the MA5600T/MA5603T.

The following figure shows an example network of TDM SHDSL for transparently transmitting the narrowband data private line service.

Figure 18-10 Example network of TDM SHDSL for transparently transmitting the narrowband data private line service



Data Plan

The following table lists the data plan for configuring TDM SHDSL for transparently transmitting the narrowband data private line service.

Table 18-14 Data plan for configuring TDM SHDSL for transparently transmitting the narrowband data private line service

Item	Data
EDTB board	Working mode: voice Working sub-mode: transparent mode Slot ID: 0/3

Prerequisite

- The H802EDTB board must be in position and must work in the normal state.
- An SHDSL modem must be correctly connected and the SHDSL port(s) must be activated. For details, see **4.5 Configuring an xDSL Port**.

Procedure

Step 1 (Optional) Configure the working mode of the board.

Configure the working mode of the board to voice.

NOTE
The working sub-mode of the board can be configured only when the working mode of the board is configured to voice. By default, the working mode of the board is voice.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
```

Step 2 Configure the working sub-mode of the board.

According to the service requirement, configure the working sub-mode of the board to transparent mode.

NOTE

- Before changing the service mode to transparent mode, make sure that no service is configured for the board.
- In the transparent mode, the E1 ports and SHDSL ports are in one-to-one mapping, that is, ports 0-15 map ports 16-31 one by one.

```
huawei(config-edt-0/3)#runmode transparent
huawei(config-edt-0/3)#quit
```

Step 3 Save the data.

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

----End

Result

The user can normally access the DDN network by using the MA5600T/MA5603T.

Configuration File

```
interface edt 0/3
board workmode voice
runmode transparent
quit
save
```

18.5 Example: Configuring the Private Line Service Leasing E1 Timeslots

Leasing an entire E1 line is expensive and also a waste of the bandwidth resources. The private line service leasing E1 timeslots can meet the requirement leasing a part of an E1 line. With this service, users are assigned specific timeslots of an E1 line, and therefore can share the bandwidth of the E1 line, hence saving the E1 line lease expense.

Prerequisites

- The H802EDTB board must be in position and must work in the normal state.
- An SHDSL modem must be correctly connected and the SHDSL port(s) must be activated.

Service Requirements

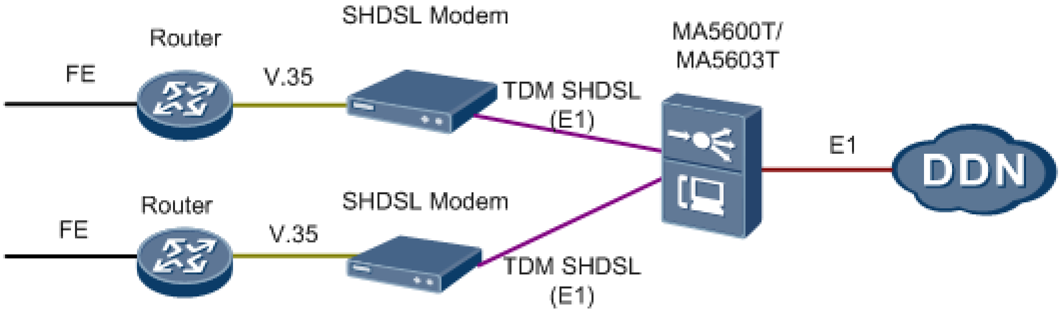
- Use the existing rich twisted pair resources for long-distance transmission, extending the DDN node.
- The carrier does not need to deploy the new E1 line, which saves the deployment cost. The user leases only one or more timeslots of the E1 line to save the lease expense.

Networking

Figure 18-11 shows an example network of the private line service leasing E1 timeslots.

The user end is connected to an SHDSL modem through a router that supports the V.35 port, and then connected to the EDTB board of the MA5600T/MA5603T through the TDM SHDSL (E1) port provided by the modem. By establishing internal SPCs between different timeslots of the E1 and SHDSL ports, the EDTB board multiplexes timeslot channels of different lines to the same E1 upstream port, implementing convergence of multiple Nx64 kbit/s channels to the E1 port and saving E1 resources.

Figure 18-11 Example network of the private line service leasing E1 timeslots



Data Plan

Table 18-15 data plan for configuring the private line service leasing E1 timeslots.

Table 18-15 Data plan for configuring the private line service leasing E1 timeslots

Item	Data
EDTB board	Working mode: voice Working sub-mode: service mode Clock source: system clock
E1 port	Upstream port ID: 0/3/0 Line coding mode: HDB3 (default) Port impedance: 75 ohms (default) Port signaling mode: UNFRAME
SHDSL port	Port IDs: 0/3/16 and 0/3/17 Port signaling mode: UNFRAME Line profile ID of the port: 106 (default)
Internal SPC	Establish internal SPCs between B channels 0-15 of SHDSL port 0/3/16 and timeslots 16-31 of E1 port 0/3/0. Establish internal SPCs between B channels 0-15 of SHDSL port 0/3/17 and timeslots 0-15 of E1 port 0/3/0.

Procedure

Step 1 Configure the working mode and clock source of the EDTB board.

Configure the working mode of the board to voice, working sub-mode to service, and clock source to system clock.

NOTE

To configure the private line service leasing timeslots, the working mode of the board must be configured to voice and the sub-mode must be configured to service.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
huawei(config-edt-0/3)#runmode service
huawei(config-edt-0/3)#set clockmode system
```

Step 2 Configure the attributes of the SHDSL port.

Configure the signaling mode of SHDSL ports 0/3/16 and 0/3/17 to UNFRAME, that is, all 32 timeslots can be used to transmit valid data and the entire 2M is used as a link.

NOTE

To configure the private line service leasing timeslots, the signaling mode of the SHDSL port must be configured to UNFRAME.

```
huawei(config-edt-0/3)#shdslport signal 16 unframe
huawei(config-edt-0/3)#shdslport signal 17 unframe
```

Step 3 Configure the attributes of the upstream E1 port.

Configure the signaling mode of E1 port 0/3/0 to UNFRAME, that is, all 32 timeslots can be used to transmit valid data and the entire 2M is used as a link.

NOTE

To configure the private line service leasing timeslots, the signaling mode of the E1 port must be configured to UNFRAME.

```
huawei(config-edt-0/3)#e1port signal 0 unframe
huawei(config-edt-0/3)#quit
```

Step 4 Configure internal SPCs.

Create one-to-one mapping from B channels 0-15 of SHDSL port 0/3/16 to timeslots 16-31 of E1 port 0/3/0; create one-to-one mapping from B channels 0-15 of SHDSL port 0/3/17 to timeslots 0-15 of E1 port 0/3/0. This implements the convergence of two 16x64 kbit/s channels.

```
huawei(config)#spc
huawei(config-spc)#anspc add start 0/3/16/0 end 0/3/0/16 apptype normal channelnum
16
huawei(config-spc)#anspc add start 0/3/17/0 end 0/3/0/0 apptype normal channelnum
16
```

Step 5 Query the status of the internal SPCs.

```
huawei(config-spc)#display anspc from-connectid 0
{ <cr>|to-connectid<K> }:

  Command:
          display anspc from-connectid 0
-------------------------------------------------------------------------------
  ConnectId                :0
  Start F/S/P/Chn          :0  /3/16/0
  End F/S/P/Chn            :0  /3/0 /16
  BChannelNum              :16
  State                    :normal
  Apptype                  :normal
  Description              :timeslot0-15_to_e1timeslot16-31
-------------------------------------------------------------------------------
  ConnectId                :1
  Start F/S/P/Chn          :0  /3/17/0
  End F/S/P/Chn            :0  /3/0 /0
  BChannelNum              :16
  State                    :normal
  Apptype                  :normal
  Description              :timeslot0-15_to_e1timeslot0-15
-------------------------------------------------------------------------------
```

----End

Result

The user can normally access the DDN network by using the leased E1 timeslots.

Configuration File

```
interface edt 0/3
board workmode voice
runmode service
set clockmode system
shdslport signal 16 unframe
shdslport signal 17 unframe
e1port signal 0 unframe
quit
spc
anspc add start 0/3/16/0 end 0/3/0/16 apptype normal channelnum 16
anspc add start 0/3/17/0 end 0/3/0/0 apptype normal channelnum 16
display anspc from-connectid 0
```

19 Example: MSTP Subtending Network

About This Chapter

This topic describes how to configure the integrated services on the MA5600T/MA5603Ts in the MSTP ring network.

19.1 MSTP Networking

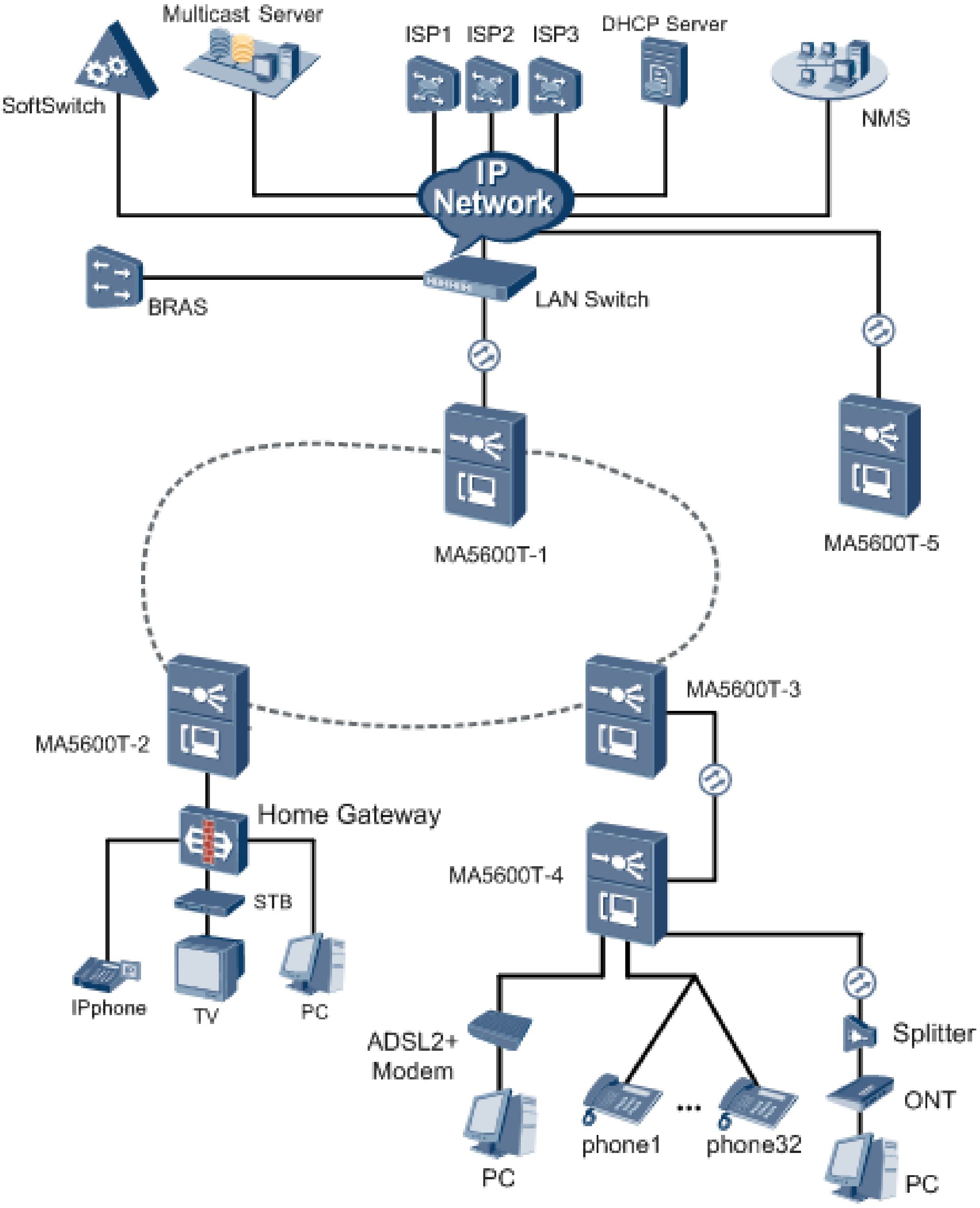
This topic describes the typical networking in the MSTP mode.

Three MA5600T/MA5603Ts (MA5600T/MA5603T-1, MA5600T/MA5603T-2, and MA5600T/MA5603T-3) form an MSTP ring network.

- MA5600T/MA5603T-1 is connected to the IP network.
- MA5600T/MA5603T-2 is connected to the home gateway at the user end through the xDSL service board, providing the Internet, voice, and IPTV services concurrently.
- MA5600T/MA5603T-3, through whose GE port, is subtended with MA5600T/MA5603T-4.
- MA5600T/MA5603T-1 works with MA5600T/MA5603T-5 to provide the QinQ service through the IP network.

Figure 19-1 shows an example MSTP network of the MA5600T/MA5603T.

Figure 19-1 Example MSTP network of the MA5600T/MA5603T



19.2 MSTP Dataplan

This topic provides the data plan for the example RSTPMSTP network.

Table 19-1 provides the service and the data plan for the example network of the MA5600T/MA5603T.

Table 19-1 Data plan for the example RSTPMSTP network

Item	MA5600T/ MA5603T-1	MA5600T/ MA5603T-2	MA5600T/ MA5603T -3	MA5600T/ MA5603T-4	MA5600T/ MA5603T-5
Service	● ADSL2+ service ● SHDSL service ● GPON service ● POTS service ● QinQ private line service (interoperate with MA5600T / MA5603T -5) ● Multicast service	● ADSL2+ service ● SHDSL service ● POTS service ● Stacking wholesale service ● Triple play service (multiple PVCs for multiple services) ● Multicast service	● ADSL2+ service ● SHDSL service ● GPON service	● ADSL2+ service ● SHDSL service ● POTS service ● GPON service ● Multicast service	● VDSL2 service ● QinQ private line service (interoperate with MA5600 T/ MA5603 T-1)
Inband NMS address	10.10.1.2 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.3 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.4 255.255.255 .0 Gateway: 10.10.1.1/24	10.10.1.5 255.255.255. 0 Gateway: 10.10.1.1/24	10.10.1.6 255.255.255. 0 Gateway: 10.10.1.1/24
GE port of the GIU board	Upstream: 0/20/0 RSTP: 0/19/0-0/19/1	Upstream: 0/19/0-0/19/1	Upstream: 0/19/0-0/19/1 RSTP: 0/20/0	Upstream: 0/19/0	Upstream: 0/19/0

Item	MA5600T/ MA5603T-1	MA5600T/ MA5603T-2	MA5600T/ MA5603T -3	MA5600T/ MA5603T-4	MA5600T/ MA5603T-5
VLAN	NMS: 10 QinQ: 50 Multicast: 100 ADSL2+: 1000-1031 (uses the VLAN authentication) SHDSL: 1300-1315 (uses the VLAN authentication) GPON: 1510 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H. 248 protocol)	NMS: 10 Multicast: 100 Stacking: 60-62 (inner stacking: 111-113) Triple play: 100-102 ADSL2+: 2020 (uses the PPPoE authentication) SHDSL: 3020 (uses the PPPoE authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 ADSL2+: 2030 (uses the PPPoE authentication) SHDSL: 3030 (uses the PPPoE authentication) GPON: 1530 (the ONT uses the SN + password authentication)	NMS: 10 Multicast: 100 ADSL2+: 2040 (uses the PPPoE authentication) SHDSL: 3040 (uses the PPPoE authentication) GPON: 1540 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H. 248 protocol)	NMS: 10 QinQ: 50 VDSL2: 1800 (uses the PPPoE authentication)
Slot	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3 QinQ: 0/5/31 Multicast: 0/2/2, 0/2/3	ADSL2+: 0/2 SHDSL: 0/5 POTS: 0/3 Stacking: 0/2/0-10 (maps VLAN 60, ISP1) 0/2/11-20 (maps VLAN 61, ISP2) 0/2/21-30 (maps VLAN 62, ISP3) Triple Play: 0/2/31	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3 Multicast: 0/2/2, 0/2/3	SHDSL: 0/5 VDSL: 0/2 QinQ: 0/5/15

Item	MA5600T/ MA5603T-1	MA5600T/ MA5603T-2	MA5600T/ MA5603T -3	MA5600T/ MA5603T-4	MA5600T/ MA5603T-5
User PVC	PVC VPI/VCI of all users: 0/35	VPI/VCI of the triple play: ● Video service: 0/35 ● Internet service: 0/36 ● Voice service: 0/37	PVC VPI/ VCI of all users: 0/35	PVC VPI/ VCI of all users: 0/35	PVC VPI/ VCI of all users: 0/35
POTS service	MGC IP address: 10.30.80.65/24 Media/Signaling IP address of the MG interface: 10.176.6.33/24 Default media gateway of the MG interface: 10.176.6.62/24 IP address of the VLAN: 10.176.6.33/24 MG interface attributes: index is 0, supported protocol is H.248, coding type is text, signaling port number is 2944, port number of the active MGC is 2944, and transmission mode is UDP.				
NMS host	2.2.2.2 and 2.2.2.3				
Log host	3.3.3.3 and 3.3.4.3				
Time server	4.4.4.4 and 4.4.4.5				
Multicast server	10.10.10.10				
EMU	AC PS4845 power monitoring, fan monitoring				
DHCP server	DHCP server1: 10.1.1.2 (active) 10.1.1.3 (standby) Gateway: 10.1.1.1/24 DHCP server2: 10.4.4.2 (active) 10.4.4.3 (standby) Gateway: 10.4.4.1/24				
Upper-layer device	The upper-layer device supports the DHCP option82 function. The BRAS supports the PITP, stacking VLAN and QinQ VLAN function. The BRAS supports inner and outer VLAN tags. The VLAN ID of the traffic flow sent from the IP network to the DSLAM is 100. The upper layer device classifies the downstream traffic. Different service carries different 802.1p labels. The VLAN mapping to the DSLAM is configured in the upper-layer IP network.				

NOTE

- In this networking, MA5600T/MA5603T-1 can be replaced with a GE switch or a BRAS.
- The upstream port of MA5600T/MA5603T supports the port aggregation function. In the actual network planning, you can aggregate multiple ports for use.
- In this networking, the five MA5600T/MA5603Ts support the ADSL2+, SHDSL, VDSL2, GPON, and POTS services. You can plan the services according to your actual network conditions.

19.3 Configuring MA5600T/MA5603T-1

This topic describes how to configure MA5600T/MA5603T-1.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-2
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.2 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   ```

```
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
huawei(config)#packet-filter inbound ip-group 3050 port 0/20/0
```

4. Configure the SNMP parameters.

   - Configure the community name and the access authority.

     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```

   - Configure the contact information.

     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```

   - Configure the device location information.

     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```

   - Configure the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the NMS version is set as SNMP v2c.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```

5. Enable the trap sending.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

6. Set the trap destination address.

   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```

7. Set the trap source address.

   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and PS4875L power supply as an example to describe how to configure the environment monitoring unit (EMU).

By default, the default slave node number of the fan EMU is 0. In this example, suppose the slave node number is 1. In this case, you need to set the DIP switch of the slave node number on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Configure GIU subtending

MA5600T/MA5603T-1 is subtended with MA5600T/MA5603T-2, MA5600T/MA5603T-3 and MA5600T/MA5603T-4. Therefore, subtending should be configured.

```
huawei(config)#vlan 60 to 62 standard
huawei(config)#port vlan 60 to 62 0/19 0-2
```

```
huawei(config)#vlan 101 to 102 standard
huawei(config)#port vlan 101 to 102 0/19 0-2
```

Step 7 Configure MSTP.

1. Enable the MSTP function.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take 
several 
minutes,are you sure to change global stp state? [Y/N][N] 
Y
```

2. Set the MST region name.

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg
```

3. Configure MSTP instance 1.

```
huawei(stp-region-configuration)#instance 1 vlan 1 to 4094
```

4. Activate the configuration of the MST region.

```
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration, it may take several minutes,are you sure 
to 
active region configuration? [Y/N][N]y
```

5. Set the priority of MA5600T/MA5603T_1 in the instance.

```
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 0 priority 0
huawei(config)#stp instance 1 priority 0
```

Step 8 Configure ADSL2+ service.

The MA5600T/MA5603T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding 
profile
  Press 'Q' to quit the current configuration and new configuration will 
be 
neglected
>  Do you want to name the profile (y/n) 
[n]:
>    Transmission 
mode:
>       0: 
Custom
>       1: All (G.
992.1~5,T1.413,ETSI)
>       2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>       3: G.DMT (G.
992.1/3/5)
>       4: G.HS (G.
992.1~5)
>       5: ADSL (G.
992.1~2,ETSI,T1.413)
>       6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6) 
[1]:
>  Trellis mode 1-disable 2-enable (1~2) 
[2]:
```

```
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
```

```
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#adsl line-template add
10
  Start adding
template
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the template (y/n)
[n]:
>  Please set the line-profile index (1~128) [1]:
10
>  Will you set channel configuration parameters? (y/n)
[n]:y
>    Please set the channel number (1~2) [1]:
1
>    Channel1 configuration
parameters:
>    Please set the channel-profile index (1~128) [1]:
10
  Add template 10
successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For detailed configuration, see "**4.1.1 Configuring an ADSL2+ Template**." This example adopts the default alarm profile 1 in the system.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 1
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.
   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as that of the peer device.

     Run the **auto-neg** command to set the port to work in the auto-negotiation mode. If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.
   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1000 to 1031 mux
huawei(config)#port vlan 1000 to 1031 0/19 0-2
huawei(config)#port vlan 60 to 62 0/19 0-2
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1000 port 0/2 0-31 vpi 0 vci 35 rx-
cttr 6 tx-cttr 6
```

Step 9 Configure the SHDSL service.

The MA5600T/MA5603T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic takes the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.
3. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

4. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T-1 adopt the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1300 to 1315 mux
huawei(config)#port vlan 1300 to 1315 0/19 0-2
```

5. Add the service port.

   Ports 0-14 in slot 0/5 provide the SHDSL service. To activate the ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1300 port 0/5 0-15 vpi 0 vci 35 rx-
cttr 6 tx-cttr 6
```

Step 10 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1510 smart
huawei(config)#port vlan 1510 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#dba-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

   NOTE

   - You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
   - You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 sn-auth hwhw-10101010 profile-id 2
```

   NOTE

   In this example, the ONT uses the default capability set profile 2. You can run the **ont-profile add** command to configure the capability set profile of the ONT based on your requirements.

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 1 vlan 1510
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

    NOTE

    In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1510
```

12. Add the service port.

```
huawei(config-if-gpon-0/18)#quit
huawei(config)#service-port vlan 1510 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 11 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#port vlan 1600 0/19 0
huawei(config)#interface vlanif 1600
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
huawei(config-if-vlanif1600)#quit
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
huawei(config-voip)#quit
```

4. Configure the MG interface.

Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
10.176.6.33
```

Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

NOTE

After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

6. Configure the PSTN user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660000
huawei(config-esl-user)#quit
```

Step 12 Configure the QinQ private line service.

MA5600T/MA5603T-1 and MA5600T/MA5603T-5 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN 50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0-2
```

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values set during the execution of the **service-port** command must be the same as those on the modem.

   The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#traffic table ip index 7 cir off priority 0 priority-policy
local-Setting
huawei(config)#service-port vlan 50 shdsl mode atm 0/5/15 vpi 0 vci 36 rx-cttr
7 tx-cttr 7
```

Step 13 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 must be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2/3 do not need authenticating.

1. Configure the xDSL.

   In this example, it is unnecessary to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

   - Create a VLAN.

```
huawei(config)#vlan 100 smart
```

   - Add the upstream port to the VLAN.

```
huawei(config)#port vlan 100 0/19 0-2
```

   - Configure the native VLAN.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#native-vlan 1 vlan 100
huawei(config-if-giu-0/19)#native-vlan 2 vlan 100huawei(config-if-giu-0/19)
#quit
```

   - Create the traffic profile.

```
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
local-Setting
```

   - Add ADSL2+ port 2 and 3 to VLAN 100.

```
huawei(config)#service-port 100 vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8
tx-cttr 8
huawei(config)#service-port 101 vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8
tx-cttr 8
```

3. Configure the multicast service.

   - Enable the multicast proxy.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   - Add the upstream port.

```
huawei(config-mvlan100)#igmp default uplink-port 0/20/0
huawei(config-mvlan100)#igmp uplink-port 0/20/0
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode mstp
Are you sure to change the uplink port mode?(y/n)[n]:y
```

- Configure the preview parameters.

  In this example, set the preview authority profile 1 with the preview duration for the program to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
```

- Configure the program library.

```
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10 preview-profile 1
```

- Configure the authority profile.

```
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add port 0/2/3 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/2 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/2 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
```

Step 14 Configure the subtending multicast service.

In the MSTP ring network, MA5600T/MA5603T-1 is subtended with MA5600T/MA5603T-3, and MA5600T/MA5603T-3 is subtended with MA5600T/MA5603T-4. According to the data plan, MA5600T/MA5603T-4 provides the multicast service. In this way, it is necessary to configure the multicast subtending on MA5600T/MA5603T-1 first.

1. Add the upstream port.

   The upstream port is already added in **Step 13.3**. It is unnecessary to configure it again.

2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 13.3**. It is unnecessary to configure it again.

3. Configure the program library.

   The program library is already configured in **Step 13.3**. It is unnecessary to configure it again.

4. Configure the multicast for the subtending port.

   - Specify a subtending port.

```
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp cascade-port 0/19/0
huawei(config-btv)#igmp cascade-port 0/19/1
```

- Modify the subtending port.

```
huawei(config-btv)#igmp cascade-port modify 0/19/0 static enable
huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
```

Step 15 Save the data.

```
huawei(config-btv)#quit
huawei(config)#save
```

----End

19.4 Configuring MA5600T/MA5603T-2

This topic describes how to configure MA5600T/MA5603T-2.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.

     ```
     huawei(config)#vlan 10 standard
     ```

   - Add the upstream port.

     ```
     huawei(config)#port vlan 10 0/19 0-1
     ```

   - Enter NMS VLAN interface mode.

     ```
     huawei(config)#interface vlanif 10
     ```

   - Configure the IP address of the NMS VLAN interface.

     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.3 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```

2. Add the route.
   - Configure the route destined to the NMS (Trap destination host).

     ```
     huawei(config)#ip route-static 2.2.2.0 255.255.255.0 10.10.1.1
     preference 1
     ```

   - Configure the route destined to the time server.

     ```
     huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```

   - Configure the route destined to the log host.

     ```
     huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```

3. Add the ACL rule.

   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   ```

```
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.

- Configure the community name and access authority.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

- Configure the contact information.

```
huawei(config)#snmp-agent sys-info contact HW-075512345678
```

- Configure the device local information.

```
huawei(config)#snmp-agent sys-info location Shenzhen China
```

- Configure the SNMP version.

NOTE

The SNMP version must be the same as that of NMS. In this example, the NMS version is set as SNMP V2C.

```
huawei(config)#snmp-agent sys-info version v2c
```

5. Enable trap sending.

```
huawei(config)#snmp-agent trap enable standard
```

6. Set the trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
trap-paramsname 123
```

7. Set the trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as an example to describe how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit to 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Configure GIU subtending.

MA5600T/MA5603T-1 is subtended with MA5600T/MA5603T-2, MA5600T/MA5603T-3 and MA5600T/MA5603T-4. Therefore, the subtending should be configured.

Step 7 Configure MSTP.

1. Enable the MSTP function.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take
several
minutes,are you sure to change global stp state? [Y/N][N]
Y
```

2. Set the MST region name.

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg
```

3. Configure MSTP instance 1.

```
huawei(stp-region-configuration)#instance 1 vlan 1 to 4094
```

4. Activate the configuration of the MST region.

```
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration, it may take several minutes,are you sure
to
active region configuration? [Y/N][N]y
huawei(stp-region-configuration)#quit
```

Step 8 Enable PITP.

```
huawei(config)#pitp enable pmode
```

Step 9 Configure ADSL2+ service.

The MA5600T/MA5603T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
992.1/3/5)
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
```

```
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
```

```
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For detailed configuration, see "**4.1.1 Configuring an ADSL2+ Template**." This example uses the default alarm profile 1 in the system.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 10
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

The configuration of the upstream port of the GIU board should be the same as the configuration of the peer device.

Run the **auto-neg** command to set the port to work in the auto-negotiation mode.

If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

- Configure the VLAN.

  The ADSL2+ users of MA5600T/MA5603T-2 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2020 smart
huawei(config)#port vlan 2020 0/19 0-1
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ services. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 2020 port 0/2 0-31 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
```

Step 10 Configure the SHDSL service.

The MA5600T/MA5603T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 1) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T-2 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3020 smart
huawei(config)#port vlan 3020 0/19 0-1
```

6. Add the service port.

- Ports 0-15 of the SHDSL board in 0/5 provide the SHDSL services.
- To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3020 port 0/5 0-15 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 11 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#port vlan 1600 0/19 0
huawei(config)#interface vlanif 1600
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
huawei(config-if-vlanif1600)#quit
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
huawei(config-voip)#quit
```

4. Configure the MG interface.

Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
10.176.6.33
```

Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

NOTE

After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

6. Configure the PSTN user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660032
huawei(config-esl-user)#quit
```

Step 12 Configure the stacking multi-ISPs wholesale service.

ISP1 provides users of ports 0/2/0 to 0/2/10 on board with the multi-ISP wholesale service. ISP2 provides users of ports 11-20 to with the multi-ISP wholesale service. ISP3 provides users of port 21-30 with the multi-ISP wholesale service.

1. Create a VLAN and set the attribute as stacking.

```
huawei(config)#vlan 60 to 62 smart
huawei(config)#vlan attrib 60 to 62 stacking
```

2. Add the upstream port.

```
huawei(config)#port vlan 60 to 62 0/19 0-1
```

3. Add the service port.

```
huawei(config)#multi-service-port vlan 60 port 0/2 0-10 vpi 0 vci 35 rx-cttr 6
tx-cttr 6
huawei(config)#multi-service-port vlan 61 port 0/2 11-20 vpi 0 vci 35 rx-cttr
6 tx-cttr 6
huawei(config)#multi-service-port vlan 62 port 0/2 21-30 vpi 0 vci 35 rx-cttr
6 tx-cttr 6
```

4. Configure the inner label.

```
huawei(config)#stacking label vlan 60 baselabel 111
huawei(config)#stacking label vlan 61 baselabel 112
huawei(config)#stacking label vlan 62 baselabel 113
```

Step 13 Configure the triple play service.

After the configuration, the following results should be achieved: Users of ports 0/2/16 can watch the programs stored on servers 224.1.1.1 and 224.1.1.2, and can preview the programs stored on server 224.1.1.3.

1. Configure the upstream port and the VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/19 0-1
huawei(config)#vlan 101 mux
huawei(config)#port vlan 101 0/19 0-1
huawei(config)#vlan 102 smart
huawei(config)#port vlan 102 0/19 0-1
```

2. Configure the traffic table.

The voice service has the highest priority, and the Internet access service has the lowest priority.

Assume that the Internet access service uses traffic table 6, with the priority of 0. The following shows how to create the traffic tables for the voice service and the video service respectively.

```
huawei(config)#traffic table ip index 7 cir 1024 priority 7
priority-policy local-Setting
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
local-Setting
```

3. Configure the service port.

```
huawei(config)#service-port vlan 100 adsl 0/2/31 vpi 0 vci 35 rx-cttr 8 tx-cttr
8
huawei(config)#service-port vlan 101 adsl 0/2/31 vpi 0 vci 36 rx-cttr 6 tx-cttr
6
huawei(config)#service-port vlan 102 adsl 0/2/31 vpi 0 vci 37 rx-cttr 7 tx-cttr
7
```

4. Configure the DHCP relay mode for the video service.

- Enable the DHCP mode.

```
huawei(config)#dhcp mode layer-3 option60
```

- Configure the DHCP server.

```
huawei(config)#dhcp-server 1 ip 10.1.1.2 10.1.1.3
huawei(config)#dhcp domain video
huawei(config-dhcp-domain-video)#dhcp-server 1
huawei(config-dhcp-domain-video)#quit
```

- Configure the gateway mapped to the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.1.1.1 24
   huawei(config-if-vlanif100)#dhcp domain video gateway 10.1.1.1
   huawei(config-if-vlanif100)#quit
```

- Enable the DHCP option82 function.

```
huawei(config)#dhcp option82 enable
huawei(config)#raio-mode xdsl-port-rate
```

5. Configure the DHCP relay mode for the voice service.

- Configure the DHCP server.

```
huawei(config)#dhcp-server 2 ip 10.4.4.2 10.4.4.3
huawei(config)#dhcp domain voice
huawei(config-dhcp-domain-voice)#dhcp-server 2
huawei(config-dhcp-domain-voice)#quit
```

- Configure the gateway mapped to the DHCP domain.

```
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 10.4.4.1 24
huawei(config-if-vlanif102)#dhcp domain voice gateway 10.4.4.1
huawei(config-if-vlanif102)#quit
```

6. Configure the multicast service.

- Enable the multicast proxy.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

- Configure the preview parameters.

  In this example, configure preview authority profile 1 with the preview duration for the program to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config)#btv
huawei(config-btv)#igmp preview-profile index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
huawei(config-btv)#quit
```

- Configure the program library.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10
preview-profile 1
huawei(config-mvlan100)#quit
```

- Configure the authority profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp user add port 0/2/15 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/16 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/16 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/15
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/16
```

Step 14 Configure the subtending multicast service.

In the MSTP ring network, MA5600T/MA5603T-1 is subtended with MA5600T/MA5603T-3, and MA5600T/MA5603T-3 is subtended with MA5600T/MA5603T-4. According to the data plan, MA5600T/MA5603T-4 provides the multicast service. In this way, it is necessary to configure the multicast subtending on MA5600T/MA5603T-2 first.

1. Configure the upstream port.

   The upstream port is already added in **Step 13.6**. It is unnecessary to configure it again.
2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 13.6**. It is unnecessary to configure it again.
3. Configure the program library.

   The program library is already configured in **Step 13.6**. It is unnecessary to configure it again.
4. Configure the multicast for the subtending port.
   - Specify the subtending port.
     ```
     huawei(config-btv)#igmp cascade-port 0/19/0
     huawei(config-btv)#igmp cascade-port 0/19/1
     ```
   - Modify the subtending port.
     ```
     huawei(config-btv)#igmp cascade-port modify 0/19/0 static enable
     huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
     huawei(config-btv)#quit
     ```

Step 15 Save the data.

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

----End

19.5 Configuring MA5600T/MA5603T-3

This topic describes how to configure MA5600T/MA5603T-3.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-2
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.4 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.0 255.255.255.0 10.10.1.1
     preference 1
     ```

- Configure the route destined to the time server.
  ```
  huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
  preference 1
  ```
- Configure the route destined to the log host.
  ```
  huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
  preference 1
  huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
  preference 1
  ```

3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#quit
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
   ```
4. Configure SNMP.
   - Configure the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Configure the contact information.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Configure the device local information.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Configure the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the NMS version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set the trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface
vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface
vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as examples to describe how to configure the environment monitoring unit (EMU).

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Configure GIU subtending.

MA5600T/MA5603T-1 is subtended with MA5600T/MA5603T-2, MA5600T/MA5603T-3 and MA5600T/MA5603T-4. Therefore, the subtending should be configured.

```
huawei(config)#vlan 60 to 62 standard
huawei(config)#port vlan 60 to 62 0/19 0-1
huawei(config)#vlan 101 to 102 standard
huawei(config)#port vlan 101 to 102 0/19 0-1
huawei(config)#vlan 100 standard
huawei(config)#port vlan 100 0/19 0-3
```

Step 7 Enable MSTP.

1. Enable the MSTP function.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take
several
minutes,are you sure to change global stp state? [Y/N][N]
Y
```

2. Set the MST region name.

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg
```

3. Configure MSTP instance 1.

```
huawei(stp-region-configuration)#instance 1 vlan 1 to 4094
```

4. Activate the configuration of the MST region.

```
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration, it may take several minutes,are you sure
to
active region configuration? [Y/N][N]y
huawei(stp-region-configuration)#quit
```

Step 8 Configure the ADSL2+ service.

The MA5600T/MA5603T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
```

```
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
992.1/3/5)
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
```

```
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   The configured ADSL2+ line profile and the ADSL2+ channel profile are bound together in the ADSL2+ line template and the index of the ADSL2+ line template is 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

You can configure the ADSL2+ alarm profile based on your requirements. For details on the configuration, see "**4.1.1 Configuring an ADSL2+ Template**." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/3
huawei(config-if-adsl-0/3)#deactivate all
huawei(config-if-adsl-0/3)#alarm-config all 1
huawei(config-if-adsl-0/3)#activate all template-index 10
huawei(config-if-adsl-0/3)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as that of the peer device.
     Run the **auto-neg** command to set the port to work in the auto-negotiation mode. If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T-3 use the VLAN authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2030 smart
huawei(config)#port vlan 2030 0/19 0
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1000 port 0/3 0-31 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 9 Configure the SHDSL service.

The MA5600T/MA5603T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 1) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T-3 use the VLAN authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3030 smart
huawei(config)#port vlan 3030 0/19 0-1
```

6. Add the service port.

   Ports 0-15 in slots 0/5 provide the SHDSL service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3030 port 0/5 0-15 vpi 0 vci 35 user-encap
pppoe rx-cttr 6 tx-cttr 6
```

Step 10 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1530 smart
huawei(config)#port vlan 1530 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#dba-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

   NOTE

   - You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
   - You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 sn-auth hwhw-10101010 profile-id 2
```

   NOTE

   In this example, the ONT uses the default capability set profile 2. You can run the **ont-profile add** command to configure the capability set profile of the ONT based on your requirements.

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1530
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1530
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1530 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 11 Configure the subtending multicast service.

1. Configure the multicast service.

- Configure the native VLAN.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#native-vlan 1 vlan 100
huawei(config-if-giu-0/19)#quit
```

- Enable the multicast proxy.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

- Configure the program library.

```
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10
huawei(config-mvlan100)#quit
```

2. Configure the subtending multicast.

- Specify the subtending ports.

```
huawei(config)#btv
huawei(config-btv)#igmp cascade-port 0/19/0
huawei(config-btv)#igmp cascade-port 0/19/1
huawei(config-btv)#igmp cascade-port 0/20/0
huawei(config-btv)#igmp cascade-port 0/20/0
```

- Modify the subtending ports.

```
huawei(config-btv)#igmp cascade-port modify 0/19/0 static enable
huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
huawei(config-btv)#igmp cascade-port modify 0/20/0 static enable
huawei(config-btv)#quit
```

Step 12 Save the data.

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

----End

19.6 Configuring MA5600T/MA5603T-4

This topic describes how to configure MA5600T/MA5603T-4.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0
     ```
   - Enter NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.5 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#quit
   ```

```
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure the SNMP.
   - Configure the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Configure the contact information.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Configure the device local information.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Configure the SNMP version.

     The SNMP version must be the same as that of NMS. In this example, the NMS version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set the trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as examples to describe how to configure the environment monitoring unit (EMU).

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Enable PITP.

```
huawei(config)#pitp enable pmode
```

Step 7 Configure the ADSL2+ service.

The MA5600T/MA5603T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
992.1/3/5)
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
```

```
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   The configured ADSL2+ line profile and the ADSL2+ channel profile are bound together in the ADSL2+ line template and the index of the ADSL2+ line template is 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
> Will you set channel configuration parameters? (y/n) [n]:y
>   Please set the channel number (1~2) [1]:1
>   Channel1 configuration parameters:
>   Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For details on the configuration, see "**4.1.1 Configuring an ADSL2+ Template**." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 10
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as the configuration of the peer device.
     Run the **auto-neg** command to set the port to work in the auto-negotiation mode. If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T-4 adopt the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2040 smart
huawei(config)#port vlan 2040 0/19 0
```

8. Add the service port.

   All ports in slot 0/2 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 2040 port 0/2 0-31 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 8 Configure the SHDSL service.

The MA5600T/MA5603T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
```

```
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 1) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T-4 adopt the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3040 smart
huawei(config)#port vlan 3040 0/19 0
```

6. Add the service port.

   Ports 0-15 in slot 0/5 provide the SHDSL service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3040 port 0/5 0-15 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 9 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1530 smart
huawei(config)#port vlan 1530 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#dba-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

   NOTE

   - You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
   - You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 sn-auth hwhw-10101010 profile-id 2
```

NOTE

In this example, the ONT uses the default capability set profile 2. You can run the **ont-profile add** command to configure the capability set profile of the ONT based on your requirements.

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1530
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1530
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1530 gpon 0/18/0 gemport 150 multi-service
 user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 10 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#port vlan 1600 0/19 0
huawei(config)#interface vlanif 1600
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
huawei(config-if-vlanif1600)#quit
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
huawei(config-voip)#quit
```

4. Configure the MG interface.

Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
 transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
10.176.6.33
```

Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

NOTE

After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

6. Configure the PSTN user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660000
huawei(config-esl-user)#quit
```

Step 11 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 must be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2/3 do not need authenticating.

1. Configure the xDSL.

   In this example, it is unnecessary to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

   - Create a smart VLAN.

```
huawei(config)#vlan 100 smart
```

   - Set the VLAN upstream port.

```
huawei(config)#port vlan 100 0/19 0
```

   - Configure the native VLAN.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#quit
```

   - Create a traffic profile.

```
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
local-Setting
```

   - Add ADSL2+ ports 2 and port 3 to VLAN 100.

```
huawei(config)#service-port vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8
tx-cttr 8
huawei(config)#service-port vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8
tx-cttr 8
```

3. Configure the multicast service.

   - Enable the multicast proxy function.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   - Add the upstream port.

```
huawei(config-mvlan100)#igmp uplink-port 0/19/0
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode mstp
Are you sure to change the uplink port mode?(y/n)[n]:y
```

   - Configure the preview parameters.

In this example, configure the preview authority profile with the preview duration for the program to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
huawei(config-btv)#quit
```

- Configure the program library.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10 preview-profile 1
huawei(config-mvlan100)#quit
```

- Configure the authority profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the user data.

```
huawei(config-btv)#igmp user add port 0/2/3 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/2 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/2 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
huawei(config-mvlan100)#quit
```

Step 12 Save the data.

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

----End

19.7 Configuring MA5600T/MA5603T-5

This topic describes how to configure MA5600T/MA5603T-5.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.

   - Create the NMS VLAN.

   ```
   huawei(config)#vlan 10 standard
   ```

   - Add the upstream port.

   ```
   huawei(config)#port vlan 10 0/19 0
   ```

   - Enter the NMS VLAN interface mode.

```
huawei(config)#interface vlanif 10
```

- Configure the IP address of the NMS VLAN interface.

```
huawei(config-if-vlanif10)#ip address 10.10.1.6 255.255.255.0
huawei(config-if-vlanif10)#quit
```

2. Add the route.

- Configure the route destined to the NMS (trap destination host).

```
huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
preference 1
```

- Configure the route destined to the time server.

```
huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
preference 1
```

- Configure the route destined to the log host.

```
huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
preference 1
huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
preference 1
```

3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.

- Configure the community name and access authority.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

- Configure the contact information.

```
huawei(config)#snmp-agent sys-info contact HW-075512345678
```

- Configure the device local information.

```
huawei(config)#snmp-agent sys-info location Shenzhen China
```

- Configure the SNMP version.

  The SNMP version must be the same as the SNMP version of the NMS. In this example, the NMS version is set as SNMP V2C.

```
huawei(config)#snmp-agent sys-info version v2c
```

5. Enable the trap sending.

```
huawei(config)#snmp-agent trap enable standard
```

6. Set the trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
trap-paramsname 123
```

7. Set the trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as an example to describe how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Configure the VDSL2 service.

The MA5600T/MA5603T supports the VDSL2 Internet service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the VDSL2 service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the VDSL2 line profile.

   You can configure the VDSL2 line profile based on your requirements.

```
huawei(config)#vdsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>       0:
Custom
>       1: All (G.992.1~5,T1.413,G.
993.2)
>       2: Full rate(G.992.1/3/5,T1.413,G.
993.2)
>       3: G.DMT (G.992.1/3/5,G.
993.2)
>       4: G.HS (G.992.1~5,G.
993.2)
>       5: ADSL (G.
992.1~5,T1.413)
>       6: VDSL (G.
993.2)
>    Please select (0~6)
[1]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream   1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
```

```
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set UPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set ADSL tone blackout configuration parameter? (y/n)
[n]:
>  Will you set VDSL tone blackout configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n)
[n]:
>  Will you set INM parameter? (y/n)
[n]:
>  Will you set SOS downstream parameter? (y/n)
[n]:
>  Will you set SOS upstream parameter? (y/n)
[n]:
  Add profile 10 successfully
```

2. Configure the VDSL2 channel profile.

   You can configure the VDSL2 channel profile based on your requirements.

```
huawei(config)#vdsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [1]:
3
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
```

```
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [1]:
3
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~200 ms)
[20]:
>    Maximum interleaving delay upstream (0~200 ms)
[20]:
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (64~100000 Kbps)
[64]:
>    Minimum reserved transmit rate downstream (64~100000 Kbps)
[64]:
>    Maximum transmit rate downstream (64~100000 Kbps)
[100000]:
>    Minimum transmit rate upstream (64~100000 Kbps)
[64]:
>    Minimum reserved transmit rate upstream (64~100000 Kbps)
[64]:
>    Maximum transmit rate upstream (64~100000 Kbps)
[100000]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n)
[n]:
>  Will you set SOS bit rate (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the VDSL2 line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

   ```
   huawei(config)#vdsl line-template add 10
     Start adding template
     Press 'Q' to quit the current configuration and new configuration will be
   neglected
   >  Do you want to name the template (y/n) [n]:
   >  Please set the line-profile index (1~128) [1]:10
   >  Will you set channel configuration parameters? (y/n) [n]:y
   >    Please set the channel number (1~2) [1]:
   >    Channel1 configuration parameters:
   >    Please set the channel-profile index (1~128) [1]:10
     Add template 10 successfully
   ```

4. Configure the VDSL2 alarm profile.

   You can configure the VDSL2 alarm profile based on your requirements. For the configuration, see "4.1.3 Configuring VDSL2 Profiles." In this example, the default alarm profile 1 is used.

5. Configure the VDSL2 traffic profile.

   You can configure the VDSL2 traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the VDSL2 port.

   ```
   huawei(config)#interface vdsl 0/2
   huawei(config-if-vdsl-0/2)#alarm-config all
   huawei(config-if-vdsl-0/2)#activate all template-index 10
   huawei(config-if-vdsl-0/2)#quit
   ```

7. Configure the upstream port.
   - Configure the GIU board.

     In general, the GE optical port uses the default gigabit full-duplex mode.

     To change the mode, switch to the GIU config mode. Then run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

     The settings of the upstream port must be the same as the settings on the peer device.
   - Configure the VLAN.

     The VDSL2 users of MA5600T/MA5603T-1 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 1800 smart
huawei(config)#port vlan 1800 0/19 0
```

8. Add the service port.

   All ports in slot 0/2 provide the VDSL2 Internet access service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 1800 port 0/2 0-23 vpi 0 vci 35
 user-encap pppoe rx-cttr 6 tx-cttr 6
```

Step 7 Configure the QinQ private line service.

MA5600T/MA5603T-1 and MA5600T/MA5603T-5 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0
```

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values set during the execution of the **service-port** command must be the same as those on the modem.

   The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#traffic table ip index 7 cir off priority 0 priority-policy
local-Setting
huawei(config)#service-port vlan 50 shdsl mode atm 0/5/15 vpi 0 vci 35 rx-cttr
7 tx-cttr 7
```

Step 8 Save the data.

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

----End

19.8 Verification

All services configured on all DSLAMs run in the normal state.

20 Example: Configuring VPLS

About This Chapter

Virtual private LAN service (VPLS) enables geographically isolated users (individuals or branch offices of an enterprise) to establish point-to-multipoint connections between each other using Ethernet links, achieving fast and flexible service deployment.

Prerequisites

Only the SPUB board supports the VPLS.

Context

As a combination of Ethernet and Multiprotocol Label Switching (MPLS) technologies, VPLS emulates all functions of the traditional local area network (LAN), with a purpose to connect multiple geographically isolated LANs that consist of Ethernet using the IP or MPLS network provided by carriers and make the LANs work as a LAN.

Currently, the MA5600T/MA5603T only supports Label Distribution Protocol (LDP)-based VPLS.

Table 20-1 provides basic concepts of VPLS.

Table 20-1 Basic concepts of VPLS

Concept	Description
VSI	Virtual switch instance. This concept corresponds to virtual local area network (VLAN) of Ethernet switch. Each VSI provides independent VPLS service. VSI supports the Ethernet bridge function and can terminate PW.

Concept	Description
PW	Pseudo wire. PW is a virtual connection between two PEs and transmits frames between the PEs. PEs use signaling to establish PWs and maintain PW status. On a VPLS network, PE routers transmit signaling to each other to establish PWs of full interconnection. Signaling exchange modes are as follows: ● Martini mode: In this mode, signaling is exchanged using the LDP protocol. This mode does not support the PE automatic discovery function. PEs need to be configured manually. With this mode, the networking is simple, and low requirements are imposed on PEs which do not need to cross domains. ● Kompella mode: Signaling is exchanged using the Border Gateway Protocol (BGP). The MA5600T/MA5603T does not support this mode.
AC	Attachment circuit. AC attaches a CE to a PE. An AC can be a physical or logical link. It transmits frames between the CE and PE.
Split horizon	Split horizon is a technology that prevents route loops and speeds up route convergence. In a VPLS network, full mesh and split horizon are used to prevent loops. Split horizon in VPLS means that the data packets received from the PW at the PSN side are not forwarded to other PWs. Instead, they are forwarded to the private network.

20.1 Example: Configuring the VPLS Internet Access Service
This topic describes how to configure the Internet access service for individual users when the VPLS networking is used at the access and aggregation layers.

20.2 Example: Configuring the VPLS Multicast Service
In the networking for multicast services, VPLS deployed on the MA5600T/MA5603T enables the MA5600T/MA5603T to be dual homed to AGS devices (aggregation switches), which ensures network reliability.

20.3 Example: Configuring the VPLS Enterprise Private Line Service
This topic describes how to configure the enterprise private line service when the VPLS networking is used at the access and aggregation layers.

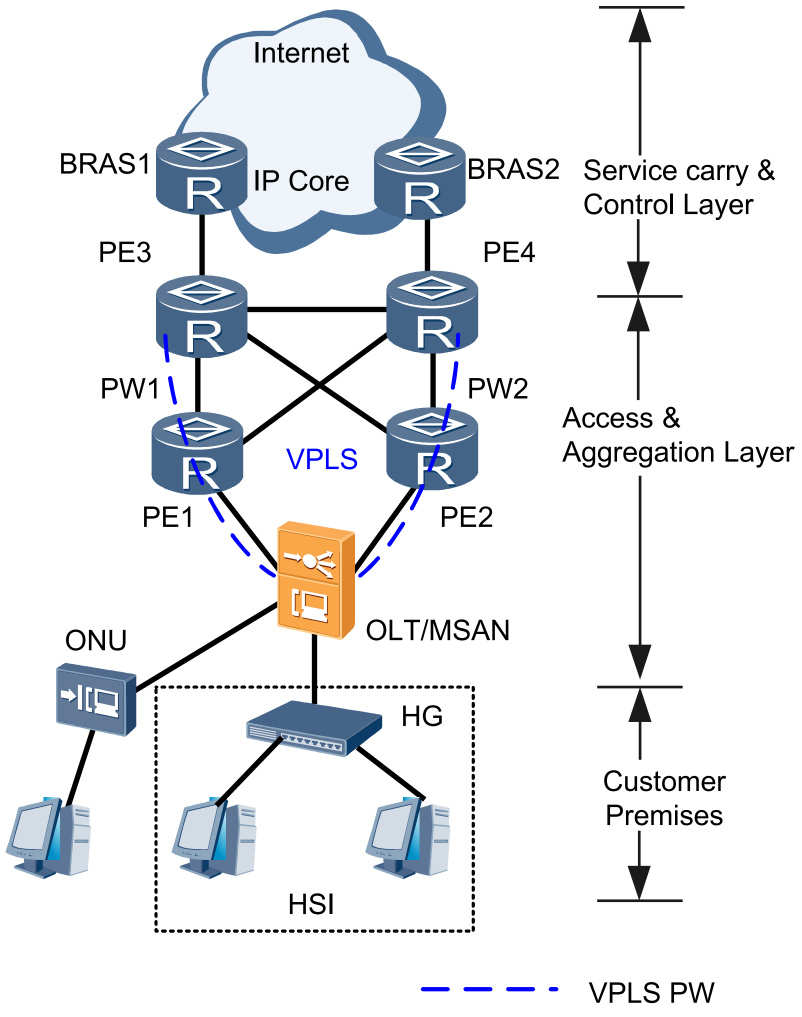
20.1 Example: Configuring the VPLS Internet Access Service

This topic describes how to configure the Internet access service for individual users when the VPLS networking is used at the access and aggregation layers.

Application Context

As shown in **Figure 20-1**, the MA5600T/MA5603T is dual homed to two AGS devices (aggregation switches) PE3 and PE4 through VPLS, and the Internet access service is received in PPPoE dialup mode. In the upstream direction, the traffic stream is mapped into the VPLS domain through VLAN. The PPPOE active discovery initiation (PADI) packets initiated by the user are broadcast in the VPLS domain it belongs to, and then the broadcast packets are received by the two AGS devices. The AGS devices terminate packets of some users respectively in delay response mode to achieve load sharing. When a BRAS device is faulty, the user dials up again. Then the VPLS MAC learning and forwarding mechanism automatically selects a new BRAS to provide services.

Figure 20-1 Networking for the VPLS Internet access service for individual users



Prerequisite

Traffic streams have been configured on the MA5600T/MA5603T for the Internet access service.

NOTE

To configure the Internet access service, you must configure SVLAN 100-based traffic streams on the MA5600T/MA5603T and perform corresponding configurations on the HG. The configurations are the same as those for common Internet access service, which are not described here.

Data Plan

Table 20-2 provides the key data plan for the MA5600T/MA5603T.

Table 20-2 Key data plan

Configuration Item	Data	Remarks	Requirement on PE3 and PE4
MPLS	● LSR ID: 10.10.10.10 ● VLAN: 4001	MPLS must be enabled at three layers. ● MPLS must be enabled globally. ● MPLS must be enabled for VLAN. ● MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	● MPLS LDP is enabled. ● Split horizon is enabled.	MPLS LDP must be enabled at three layers. ● MPLS LDP must be enabled globally. ● MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5600T/MA5603T is configured on PE3 and PE4.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5600T/MA5603T and those on PE3 and PE4 can ping each other.	Layer 3 interfaces and routes are configured on PE3 and PE4. Ensure that the Layer 3 interfaces and LSR IDs on PE3 and PE4 and those on the MA5600T/MA5603T can ping each other.

Configuration Item	Data	Remarks	Requirement on PE3 and PE4
VPLS PW	● PW ID: 1 and 2 ● Service type: vpls ● Encapsulation type: ethernet tagged ● The control word is enabled.	On the MA5600T/ MA5603T, PW1 and PW2 are created for PE3 and PE4 respectively. In this way, packets can be transmitted to BRAS devices over two trails.	The LDP VPLS is supported. VPLS PWs to the MA5600T/ MA5603T are configured on PE3 and PE4, and attributes of PWs are consistent with those on the MA5600T/ MA5603T.
VSI	● PW1 and PW2 are bound to VSI. ● VLAN 100 of the Internet access service is bound to VSI.	VSI binds VLAN and PW to map VLAN to the VPLS domain, so that PADI packets for the Internet access service can be broadcast in the VPLS domain at first, until one of the BRAS response.	VSI is configured on PE3 and PE4 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

   Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 10.10.10.10 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

   ```
   huawei(config)#mpls lsr-id 10.10.10.10
   ```

3. Enable MPLS globally.

   Trigger LDP by the IP address of the host to set up an LSP.

   ```
   huawei(config)#mpls
   huawei(config-mpls)#lsp-trigger host
   huawei(config-mpls)#quit
   ```

4. Enable the L2VPN function.

   ```
   huawei(config)#mpls l2vpn
   ```

5. Enable the LDP function globally and enable the split horizon policy.

   ```
   huawei(config)#mpls ldp
   huawei(config-mpls-ldp)#outbound peer all split-horizon
   huawei(config-mpls-ldp)#quit
   ```

Step 2 Configure VLAN and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add upstream port 0/19/0 and 0/19/1 to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19/0
huawei(config)#port vlan 4001 0/19/1
```

2. Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

3. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5600T/MA5603T to PE3 (LSR ID: 3.3.3.3) and PE4 (LSR ID: 4.4.4.4) respectively. Name the sessions **to_pe3** and **to_pe4** respectively.

```
huawei(config)#mpls ldp remote-peer to_pe3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip 3.3.3.3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe3)#quit
huawei(config)#mpls ldp remote-peer to_pe4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip 4.4.4.4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe4)#quit
```

Step 5 Configure a VSI.

1. Add a VSI.

   Create a VSI named **hsi**. Set the signaling protocol to **LDP**. and VSI ID to **1**.

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#pwsignal ldp
huawei(config-vsi-hsi)#vsi-id 1
```

2. (Optional) Configure the attributes of VSI.

   Configure basic attributes of VSI as required, including the encapsulation type, control word, MTU value, and traffic suppression policy. In the following example, the control word is enabled and default values are used for other parameters.

```
huawei(config-vsi-hsi)#control-word
```

Step 6 Configure PWs.

Create two PWs with IDs 1 and 2. Set the service type to **vpls**, remote IP addresses to **3.3.3.3** and **4.4.4.4** respectively, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240** and **10250** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 3.3.3.3
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 4.4.4.4
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW1 and PW2 to the VSI named **hsi** to establish the VPLS PW service.

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#vsi-pw-binding pwindex 1
huawei(config-vsi-hsi)#vsi-pw-binding pwindex 2
```

Step 8 Bind AC and VSI.

Bind VLAN 100 to the VSI named hsi, so that the Internet access service packets of VLAN 100 can be forwarded in the VSI.

```
huawei(config-vsi-hsi)#vsi-ac-binding vlan 100
```

----End

Result

1. A user performs PPPoE dialup. A PADI packet is transmitted upstream.
2. The OLT maps the PADI packet to VSI based on SVLAN carried in the packet and broadcasts the packet on two PWs. At the same time, the OLT learns user's MAC address.
3. After receiving the PADI packet, two BRAS devices respond with PPPOE active discovery offer (PADO) packets in random delay mode.
4. After receiving the PADO packets from PWs, the OLT learns the MAC address carried in the packets from PWs and forwards the packets to the user.
5. The user receives two PADO packets at different time and only responds to the first received PADO packet to establish a PPPoE session.
6. The OLT forwards subsequent PPPOE active discovery request (PADR) and PPPOE active discovery session-confirmation (PADS) packets based on learnt MAC addresses.

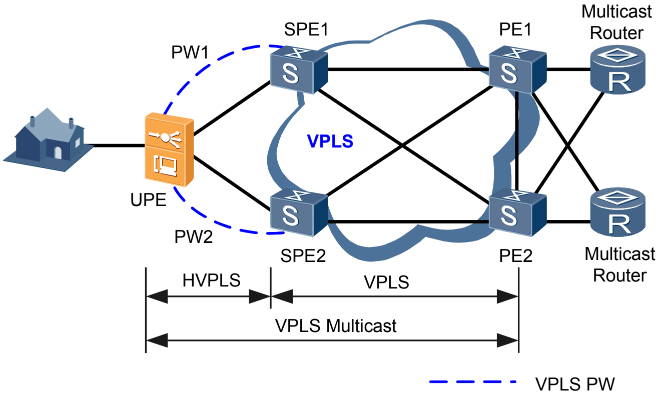
20.2 Example: Configuring the VPLS Multicast Service

In the networking for multicast services, VPLS deployed on the MA5600T/MA5603T enables the MA5600T/MA5603T to be dual homed to AGS devices (aggregation switches), which ensures network reliability.

Application Context

In the VPLS network, multicast services are still deployed based on multicast VLAN other than based on VSI (VPLS instance). The multicast VLAN is bound to VSI for carrying multicast services over the VPLS network, including upstream IGMP packets and downstream multicast traffic streams.

Figure 20-2 Networking for the VPLS multicast service



As shown in **Figure 20-2**:

- The MA5600T/MA5603T, functioning as a UPE (underlayer PE), is located on the edge network of HVPLS. In the downstream direction, the MA5600T/MA5603T accesses multicast users through multicast VLAN whose IGMP mode is proxy or snooping. In the upstream direction, the MA5600T/MA5603T is dual homed to two AGS devices that serve as SPEs (superstratum PEs) through two PWs. The same VSI is set up on the MA5600T/MA5603T and AGS and the two upstream PWs belong to the VSI.
- Multiple AGS devices form a VPLS core bearer network. The AGS devices learn the VPLS multicast forwarding table and duplicate multicast traffic based on VPLS PW connections. Two edge AGS devices functioning as SPEs in the downstream direction access the UPE on the edge network, and two edge AGS devices functioning as PEs in the upstream direction terminate VPLS and are connected to multicast routers.
- Two multicast routers back up each other and import multicast traffic streams from the multicast source to the VPLS bearer network.

NOTE

Currently, a maximum of two PWs are supported for VPLS multicast services and both two PWs are used for transmitting multicast packets upstream.

Prerequisite

The MA5600T/MA5603T has been configured with multicast VLAN 100-based multicast traffic streams, and corresponding configurations have been performed on the HG. The configurations are similar to those for common multicast services. The difference is that multicast upstream ports do not need to be configured for VPLS multicast services and the default mode is used for the multicast upstream ports.

Data Plan

Table 20-3 provides the key data plan for the MA5600T/MA5603T.

Table 20-3 Key data plan

Configuration Item	Data	Remarks	Requirement on SPE1 and SPE2
MPLS	- LSR ID: 10.10.10.10 - VLAN: 4001	MPLS must be enabled at three layers. - MPLS must be enabled globally. - MPLS must be enabled for VLAN. - MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	- MPLS LDP is enabled. - Split horizon is enabled.	MPLS LDP must be enabled at two layers. - MPLS LDP must be enabled globally. - MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5600T/MA5603T is configured on SPE1 and SPE2.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5600T/MA5603T and those on SPE1 and SPE2 can ping each other.	Layer 3 interfaces and routes are configured on SPE1 and SPE2. Ensure that the Layer 3 interfaces and loopback interfaces on SPE1 and SPE2 and those on the MA5600T/MA5603T can ping each other.
VPLS PW	- PW ID: 1 and 2 - Service type: vpls - Encapsulation type: ethernet tagged - The control word is enabled.	L2VPN must be enabled. On the MA5600T/MA5603T, PW1 and PW2 are created for SPE1 and SPE2 respectively.	The LDP VPLS is supported. VPLS PWs to the MA5600T/MA5603T are configured on SPE1 and SPE2, and attributes of PWs are consistent with those on the MA5600T/MA5603T.
VSI	- PW1 and PW2 are bound to VSI. - Multicast service VLAN 100 is bound to VSI.	Multicast VLAN is bound through VSI to map VLAN to the VPLS domain, so that multicast service packets can be broadcast in the VPLS domain.	VSI is configured on SPE1 and SPE2 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

   Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.10.10.10 32
huawei(config-if-loopback0)#quit
```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

   huawei(config)#**mpls lsr-id 10.10.10.10**

3. Enable MPLS globally.

   Trigger LDP by the IP address of the host to set up an LSP.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host
huawei(config-mpls)#quit
```

4. Enable the L2VPN function.

```
huawei(config)#mpls l2vpn
```

5. Enable the LDP function globally and enable the split horizon policy.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#outbound peer all split-horizon
huawei(config-mpls-ldp)#quit
```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add two upstream ports to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19/0
huawei(config)#port vlan 4001 0/19/1
```

2. Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

3. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP sessions from the MA5600T/MA5603T to SPE1 (LSR ID: 1.1.1.1) and SPE2 (LSR ID: 2.2.2.2) respectively. Name the sessions **to_spe1** and **to_spe2** respectively.

```
huawei(config)#mpls ldp remote-peer to_spe1
huawei(config-mpls-ldp-remote-to_spe1)#remote-ip 1.1.1.1
huawei(config-mpls-ldp-remote-to_spe1)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_spe1)#quit
huawei(config)#mpls ldp remote-peer to_spe2
huawei(config-mpls-ldp-remote-to_spe2)#remote-ip 2.2.2.2
huawei(config-mpls-ldp-remote-to_spe2)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_spe2)#quit
```

Step 5 Configure a VSI.

1. Add a VSI.

   Create a VSI named **multicast**. Set the signaling protocol to **LDP** and VSI ID to **1**.
   ```
   huawei(config)#vsi multicast
   huawei(config-vsi-multicast)#pwsignal ldp
   huawei(config-vsi-multicast)#vsi-id 1
   ```

2. (Optional) Disable the suppression of the unknown multicast of the VSI.

   If the VSI unknown multicast suppression is enabled, you need to configure this step. Otherwise, packet loss will occur in the multicast services.
   ```
   huawei(config-vsi-multicast)#undo traffic-suppress multicast
   ```

3. (Optional) Configure attributes of VSI.

   Configure basic attributes of VSI as required, including the encapsulation type, control word, and MTU value. In the following example, the control word is enabled and default values are used for other parameters.
   ```
   huawei(config-vsi-multicast)#control-word
   ```

Step 6 Configure PWs.

Create two PWs with IDs 1 and 2. Set the service type to **vpls**, the remote IP addresses to **1.1.1.1** and **2.2.2.2** respectively, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240** and **10250** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 1.1.1.1
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 2.2.2.2
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW1 and PW2 to the VSI named multicast to establish the VPLS PW service.

```
huawei(config)#vsi multicast
huawei(config-vsi-multicast)#vsi-pw-binding pwindex 1
huawei(config-vsi-multicast)#vsi-pw-binding pwindex 2
```

Step 8 Bind AC and VSI.

Bind multicast VLAN 100 to the VSI named multicast, so that the multicast service packets of VLAN 100 can be forwarded in VSI.

- The same multicast VLAN cannot be bound to the VPLS instance and PW at the same time.
- The same restrictions are set for binding multicast VLANs and VSI as those for binding unicast VLANs and VSI. That is, when the VPLS encapsulation type is raw, one VIS can only be bound to a multicast VLAN; when the VPLS encapsulation type is tag, one VSI can be bound to multiple multicast VLANs.

```
huawei(config-vsi-multicast)#vsi-ac-binding vlan 100
```

----End

Result

1. A user orders a multicast program. An IGMP packet is transmitted upstream.
2. The MA5600T/MA5603T broadcasts the IGMP packet over two upstream PWs which serve as the multicast upstream ports of the multicast VLAN.
3. On the AGS devices, VPLS exchange is performed on the IGMP packet. The AGS devices learn the VPLS multicast forwarding table and duplicate multicast traffic based on VPLS PW connections.
4. Finally, multicast traffic streams are transmitted over one PW. The MA5600T/MA5603T forwards the multicast traffic streams to the corresponding user port based on the local multicast forwarding table. Then the user can watch the multicast program normally.

20.3 Example: Configuring the VPLS Enterprise Private Line Service

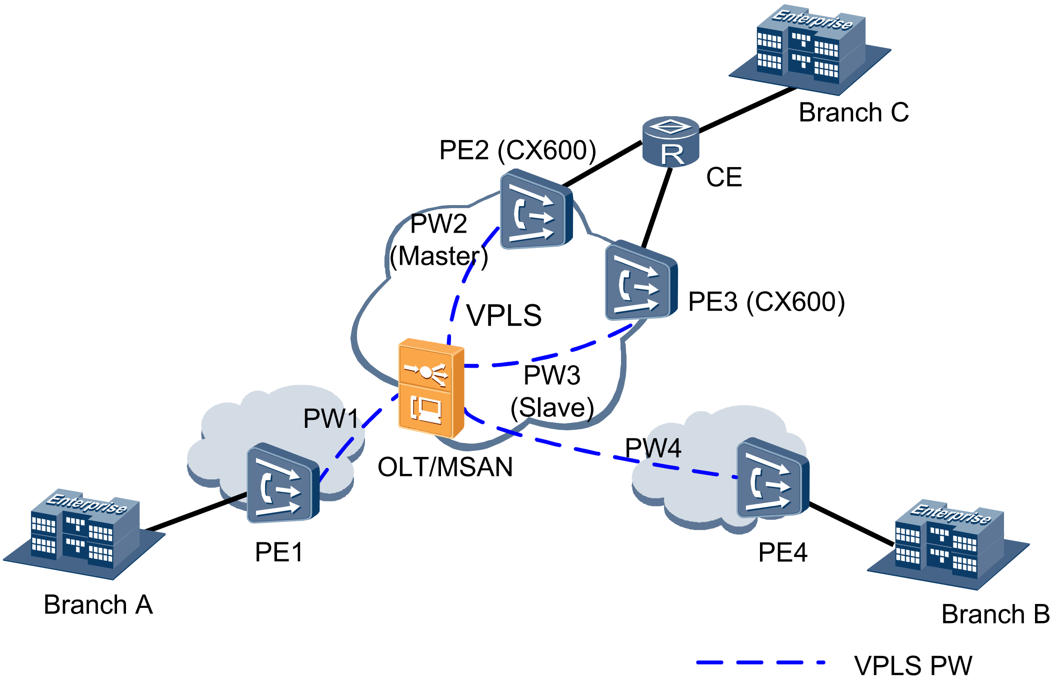
This topic describes how to configure the enterprise private line service when the VPLS networking is used at the access and aggregation layers.

Application Context

As shown in **Figure 20-3**, branch offices of an enterprise access the VPLS network through a CE or PE. By deploying VPLS PWs between PEs, the service provider can provide Ethernet-based multipoint services to enterprise users over the MPLS backbone network and achieve emulation of the local area network (LAN). For important branch offices (for example, branch C in the following figure), PW redundancy is configured to provide protection.

In the following figure, as a key node, the OLT/MSAN (MA5600T/MA5603T) exchanges data with PEs (PE1-PE4) through VPLS PWs. For important branch offices, a PW protection group is configured to provide protection. PEs are connected to the OLT/MSAN using Spoke PW.

Figure 20-3 Networking for the VPLS enterprise private line service



Prerequisite

QinQ traffic streams have been configured on PE1-PE4 for the private line service of different branch offices.

NOTE

To configure the Ethernet-based enterprise private line service, you must configure QinQ VLAN-based Ethernet traffic streams on PE1-PE4, and perform corresponding configurations on routers for branch offices of the enterprise. The configurations are the same as those for common QinQ VLAN private line service, which are not described here.

Data Plan

Table 20-4 provides the key data plan for the OLT/MSAN (MA5600T/MA5603T).

Table 20-4 Key data plan

Configuration Item	Data	Remarks	Requirement on PE1-PE4
MPLS	● LSR ID: 10.10.10.10 ● VLAN: 4001	MPLS must be enabled at three layers. ● MPLS must be enabled globally. ● MPLS must be enabled for VLAN. ● MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	MPLS LDP is enabled.	MPLS LDP must be enabled at three layers. ● MPLS LDP must be enabled globally. ● MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5600T/MA5603T is configured on PE1-PE4.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5600T/MA5603T and those on PE1-PE4 can ping each other.	Layer 3 interfaces and routes are configured on PE1-PE4. Ensure that the Layer 3 interfaces and LSR IDs on PE1-PE4 and those on the MA5600T/MA5603T can ping each other.

Configuration Item	Data	Remarks	Requirement on PE1-PE4
VPLS PW	● PW ID: 1, 2, 3, 4 ● Service type: vpls ● Encapsulation type: ethernet tagged ● The control word is enabled. PW protection group: ● PW ID: 2, 3 ● Working mode: master-slave ● The dual receiving function is enabled for PWs.	On the OLT/MSAN, PW1 and PW4 are created for PE1 and PE4 respectively, and PW2 and PW3 are created for PE2 and PE3 respectively. PW2 and PW3 back up each other.	The LDP VPLS is supported, and VPLS PWs to the MA5600T/MA5603T are configured on PE1-PE4, and attributes of PWs are consistent with those on the MA5600T/MA5603T.
VSI	● PW1-PW4 are bound to VSI. ● Binding mode of PW 1 and PW 4: spoke ● VLAN 100 of the private line service is bound to VSI.	VSI binds VLAN and PW to map VLAN to the VPLS domain, so that packets for the enterprise private line service can be broadcast in the VPLS domain.	VSI is configured on PE1-PE4 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

   Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.10.10.10 32
huawei(config-if-loopback0)#quit
```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 10.10.10.10
```

3. Enable MPLS globally.

   Trigger LDP by the IP address of the host to set up an LSP.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host
huawei(config-mpls)#quit
```

4. Enable the L2VPN function.

```
huawei(config)#mpls l2vpn
```

5. Enable LDP globally.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add four upstream ports to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19 0
huawei(config)#port vlan 4001 0/19 1
huawei(config)#port vlan 4001 0/20 0
huawei(config)#port vlan 4001 0/20 1
```

2. Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

3. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5600T/MA5603T to PE1 (LSR ID: 5.5.5.5), PE2 (LSR ID: 2.2.2.2), PE3 (LSR ID: 3.3.3.3), and PE4 (LSR ID: 4.4.4.4) respectively. Name the sessions **to_pe1**, **to_pe2**, **to_pe3**, and **to_pe4** respectively.

```
huawei(config)#mpls ldp remote-peer to_pe1
huawei(config-mpls-ldp-remote-to_pe1)#remote-ip 5.5.5.5
huawei(config-mpls-ldp-remote-to_pe1)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe1)#quit
huawei(config)#mpls ldp remote-peer to_pe2
huawei(config-mpls-ldp-remote-to_pe2)#remote-ip 2.2.2.2
huawei(config-mpls-ldp-remote-to_pe2)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe2)#quit
huawei(config)#mpls ldp remote-peer to_pe3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip 3.3.3.3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe3)#quit
huawei(config)#mpls ldp remote-peer to_pe4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip 4.4.4.4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe4)#quit
```

Step 5 Configure VSI.

1. Add a VSI.

   Create a VSI named **enterprise_vpn**. Set the signaling protocol to **LDP** and VSI ID to **1**.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#pwsignal ldp
huawei(config-vsi-enterprise_vpn)#vsi-id 1
```

2. (Optional) Configure the attributes of VSI.

   Configure basic attributes of VSI as required, including the encapsulation type, control word, MTU value, and traffic suppression policy. In the following example, the control word is enabled and default values are used for other parameters.

```
huawei(config-vsi-enterprise_vpn)#control-word
```

Step 6 Configure PWs.

Create four PWs with IDs 1-4. Set the service type to **vpls**, the remote IP addresses to the IP addresses of PE1-PE4, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240**, **10250**, **10260**, and **10270** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 5.5.5.5
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 1
huawei(config-pw-para-index-2)#peer-address 2.2.2.2
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
huawei(config)#pw-para pwindex 3
huawei(config-pw-para-index-3)#service-type vpls
huawei(config-pw-para-index-3)#pwid 3
huawei(config-pw-para-index-3)#peer-address 3.3.3.3
huawei(config-pw-para-index-3)#pw-type ethernet tagged
huawei(config-pw-para-index-3)#control-word enable
huawei(config-pw-para-index-3)#dyn-receive-label 10260
huawei(config-pw-para-index-3)#quit
huawei(config)#pw-para pwindex 4
huawei(config-pw-para-index-4)#service-type vpls
huawei(config-pw-para-index-4)#pwid 4
huawei(config-pw-para-index-4)#peer-address 4.4.4.4
huawei(config-pw-para-index-4)#pw-type ethernet tagged
huawei(config-pw-para-index-4)#control-word enable
huawei(config-pw-para-index-4)#dyn-receive-label 10270
huawei(config-pw-para-index-4)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW 1 and PW 4 in spoke mode, and dynamically bind PW 2 and PW 3 to the VSI named **enterprise_vpn** to establish the VPLS PW service. The spoke mode is used to identify the peer is a user-side PE, and split horizon is not performed between PWs.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 1 spoke
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 2
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 3
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 4 spoke
```

Step 8 Configure VPLS PW protection.

Configure PW2 and PW3 as a PW protection group named **pg_pw**. Set the working mode to master-slave and enable the dual receiving function for PWs. In the protection group enabled with dual receiving, two PWs are always allowed to receive traffic. In this way, when the remote device performs traffic switching, the traffic will not be dropped.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#protect-group pg_pw
huawei(config-vsi-enterprise_vpn-group-pg_pw)#pw-protect primary-pw pwindex 2
secondary-pw pwindex 3
huawei(config-vsi-enterprise_vpn-group-pg_pw)#protect-mode master
huawei(config-vsi-enterprise_vpn-group-pg_pw)#stream-dual-receiving
```

Step 9 Bind AC and VSI.

Bind QinQ VLAN 100 to the VSI named enterprise_vpn, so that the enterprise private line service packets can be forwarded in the VSI.

```
huawei(config-vsi-enterprise_vpn)#vsi-ac-binding vlan 100
```

----End

Result

As shown in **Figure 20-3**, the private networks distributed in different branches can establish point-to-multipoint communication with each other and various services can be provisioned between these private networks. When a PE which branch C is connected to is faulty, services can be automatically switched to another PE and therefore services are not affected.

21 Example: Subtending Networking

About This Chapter

This topic describes how to configure the integrated services on the MA5600Ts in the multi-tier subtending network.

21.1 Subtended Network

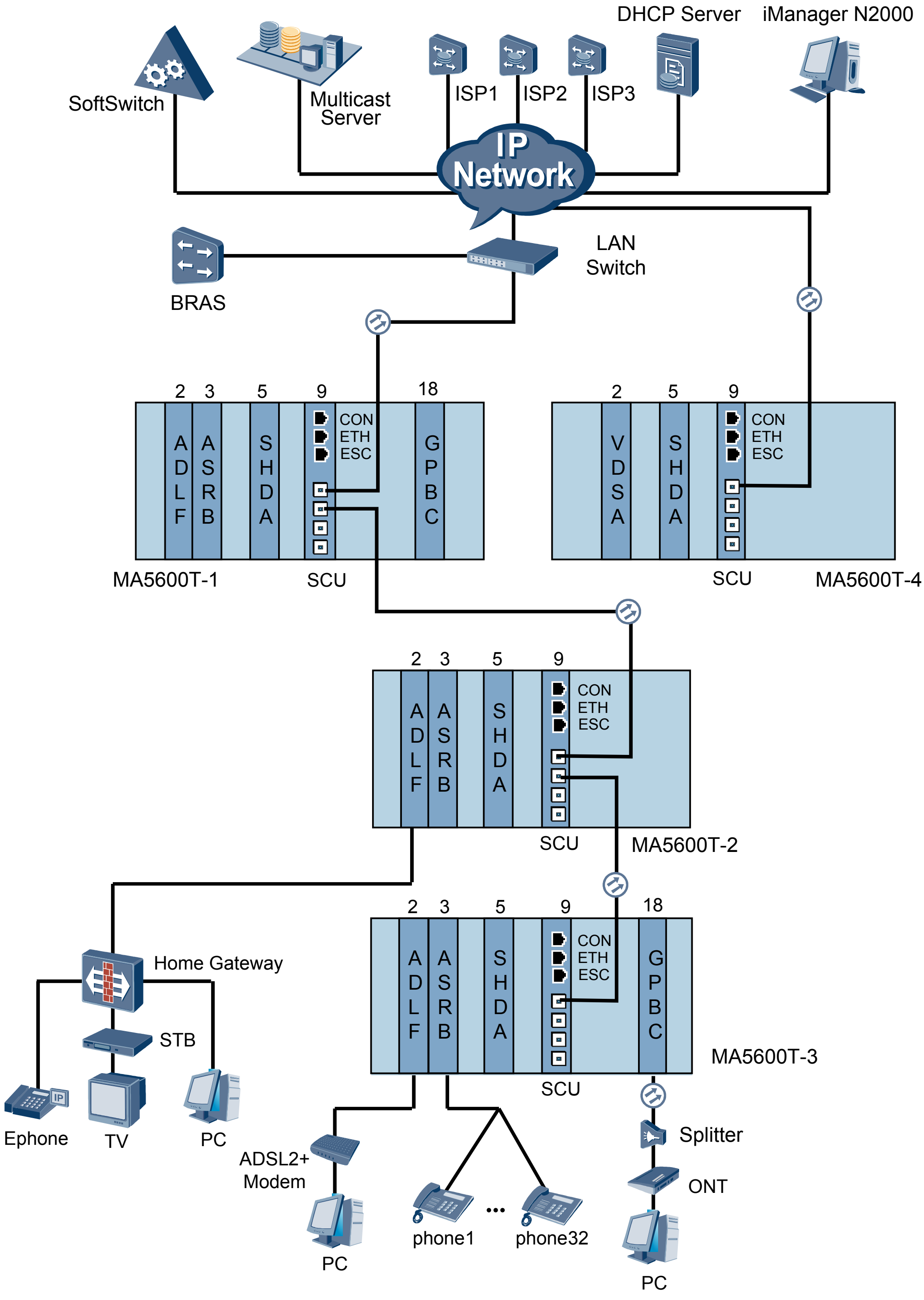
This topic describes an example of subtended network.

As shown in **Figure 21-1**:

- MA5600T-1 is subtended with MA5600T-2 through the GE port on the GIU board.
- MA5600T-2 is subtended with MA5600T-3 through the GE port on the GIU board.

Figure 21-1 shows an example subtended network of the MA5600T.

Figure 21-1 Example subtended network of the MA5600T



21.2 Data Plan for Subtended Network

This topic describes the data plan for the example subtended network.

Table 21-1 provides the service and the data plan for the example subtended network of the MA5600T in Figure 21-1.

Table 21-1 Data plan for the example subtended network

	MA5600T-1	MA5600T-2	MA5600T-3	MA5600T-4
Service	● ADSL2+ service ● SHDSL service ● GPON service ● POTS service ● QinQ private line service (for the private line interconnection withMA5600T-4) ● Multicast service	● ADSL2+ service ● SHDSL service ● POTS service ● Stacking wholesale service ● Triple play service	● ADSL2+ service ● SHDSL service ● GPON service ● POTS service ● Multicast service	● VDSL2 service ● QinQ private line service (for the private line interconnection withMA5600T-1)
Inband NMS address	10.10.1.2 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.3 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.4 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.5 255.255.255.0 Gateway: 10.10.1.1/24
GE port of the GIU board	Upstream: 0/19/0 Subtending: 0/19/1	Upstream: 0/19/0 Subtending: 0/19/1	Upstream: 0/19/0	Upstream: 0/19/0

	MA5600T-1	MA5600T-2	MA5600T-3	MA5600T-4
VLAN	NMS: 10 QinQ: 50 Multicast: 100 ADSL2+: 1000-1031 (uses the VLAN authentication) SHDSL: 1300-1315 (uses the VLAN authentication) GPON: 1510 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 Stacking: 60-62 (inner label: 111-113) Triple play: 100-102 ADSL2+: 1000 (uses the PPPoE authentication) SHDSL: 1300 (uses the PPPoE authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 Multicast: 100 ADSL2+: 1000 (uses the PPPoE authentication) SHDSL: 1300 (uses the PPPoE authentication) GPON: 1530 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 QinQ: 50 VDSL2: 1800 (uses the PPPoE authentication)
Slot and port	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3 QinQ: 0/5/15 Multicast: 0/2/2, 0/2/3	ADSL2+: 0/2 SHDSL: 0/5 POTS: 0/3 Stacking: 0/2/0-10 (map VLAN 60, ISP1) 0/2/11-20 (map VLAN 61, ISP2) 0/2/21-30 (map VLAN 62, ISP3) Triple play: 0/2/31	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3	SHDSL: 0/5 VDSL: 0/2 QinQ: 0/5/15
POTS service	MGC IP address: 10.30.80.65/24 Media/Signaling IP address of the MG interface: 10.176.6.33/24 Default media gateway of the MG interface: 10.176.6.62/24 IP address of the VLAN: 10.176.6.33/24 MG interface attributes: index is 0, supported protocol is H.248, coding type is text, signaling port number is 2944, port number of the active MGC is 2944, and transmission mode is UDP.			
NMS host	2.2.2.2 and 2.2.2.3			
Log host	3.3.3.3 and 3.3.4.3			
Time server	4.4.4.4 and 4.4.4.5			

	MA5600T-1	MA5600T-2	MA5600T-3	MA5600T-4
Multicast server	10.10.10.10			
EMU	Fan monitoring			
DHCP server	DHCP server1: 10.1.1.2 (active), 10.1.1.3 (standby) Gateway: 10.1.1.1/24 DHCP server2: 10.4.4.2 (active), 10.4.4.3 (standby) Gateway: 10.4.4.1/24			
Upper-layer device	The upper-layer device supports the DHCP option82 function. The BRAS supports the PITP, Stacking, and QinQ function. The BRAS supports inner and outer VLAN tags. The VLAN ID of the traffic flow sent from the IP network to the DSLAM is 100. The upper-layer device classifies the downstream traffic. Different services carry different 802.1p labels. The VLAN mapping to the DSLAM is configured at the upper-layer device.			

NOTE

- In this networking, MA5600T-1 can be replaced with a GE switch or a BRAS.
- The upstream port of the MA5600T supports the port aggregation function. In the actual network planning, you can aggregate multiple upstream ports for use.
- In this networking, the four MA5600Ts support the ADSL2+, SHDSL, VDSL2, GPON, and POTS services. You can plan the services according to your actual network conditions.

21.3 Configuring MA5600T-1

This topic describes how to configure MA5600T-1.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-1
       It will take several minutes, and console may be timeout, please use
     command
     idle-timeout to set time
     limit
       Are you sure to add standard port(s)? (y/n)[n]:y
     ```

- Enter the NMS VLAN interface mode.

```
huawei(config)#interface vlanif 10
```

- Configure the IP address of the NMS interface.

```
huawei(config-if-vlanif10)#ip address 10.10.1.2 255.255.255.0
```

2. Add the route.

- Configure the route destined to the NMS (Trap destination address).

```
huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
 preference 1
huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
preference 1
```

- Configure the route destined to the time server.

```
huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
preference 1
huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
preference 1
```

- Configure the route destined to the log host.

```
huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
preference 1
huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
preference 1
```

3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
 destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
 destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
 destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
 destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
 destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
 destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.

- Set the community name and access authority.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

- Set the SysContact.

```
huawei(config)#snmp-agent sys-info contact HW-075512345678
```

- Set the SysLocation.

```
huawei(config)#snmp-agent sys-info location Shenzhen China
```

- Set the SNMP version.

  The SNMP version must be the same as that of the NMS. In this example, the SNMP version is set as SNMP V2C.

```
huawei(config)#snmp-agent sys-info version v2c
```

5. Enable the trap sending.

```
huawei(config)#snmp-agent trap enable standard
```

6. Set trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
```

```
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
trap-paramsname 123
```

7. Set trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801ESC 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure GIU subtending.

MA5600T-1 is subtended with MA5600T-2 andMA5600T-3. Therefore, the subtending should be configured.

```
huawei(config)#vlan 60 to 62 standard
huawei(config)#port vlan 60 to 62 0/19 0-1
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#vlan 101 to 102 standard
huawei(config)#port vlan 101 to 102 0/19 0-1
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

Step 7 Configure the ADSL2+ service.

The MA5600T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure it based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,ETSI)
>      2: Full rate(G992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G992.1/3/5)
>      4: G.HS (G992.1~5)
>      5: ADSL (G992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G992.3~5)
>    Please select (0~6) [1]:
>  Trellis mode 1-disable 2-enable (1~2) [2]:
>  Bit swap downstream 1-disable 2-enable (1~2) [2]:
>  Bit swap upstream 1-disable 2-enable (1~2) [2]:
```

```
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set power management parameters? (y/n) [n]:
>  Will you set tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   The ADSL2+ channel profile should be configured based on the actual channel condition.

```
huawei(config)#adsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:24
>    Maximum interleaving delay upstream (0~63 ms) [6]:12
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (32~32000 Kbps) [32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps) [32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:8000
>    Minimum transmit rate upstream (32~6000 Kbps) [32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps) [32]:
>    Maximum transmit rate upstream (32~6000 Kbps) [1024]:
>  Will you set rate thresholds? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the configured line profile to the configured channel profile. The index of the line template is 10.

```
huawei(config)#adsl line-template add
10
  Start adding
template
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the template (y/n)
[n]:
>  Please set the line-profile index (1~128) [1]:
10
>  Will you set channel configuration parameters? (y/n)
[n]:y
>    Please set the channel number (1~2) [1]:
1
>    Channel1 configuration
parameters:
>    Please set the channel-profile index (1~128) [1]:
10
```

```
  Add template 10
successfully
```

4. Configure the ADSL2+ alarm profile.

   The ADSL2+ alarm profile should be configured based on the actual line condition. see "**4.1.1 Configuring an ADSL2+ Template**" for the configuration. The following uses the alarm profile 1 as an example.

5. Configure the ADSL2+ traffic profile.

   To configure the ADSL2+ traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 1
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     By default, the GE optical port of the GIU board works in the full duplex mode with the rate of 1000 Mbit/s.

     To change the port working mode and the port rate, run the **speed** and **duplex** command in the GIU mode.

     The settings must be the same as the settings of the peer device.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1000 to 1031 mux
huawei(config)#port vlan 1000 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#port vlan 1001 to 1031 0/19 0
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1000 port 0/2 0-31 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 8 Configure the SHDSL service.

The MA5600T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
```

```
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shdsl-0/5)#deactivate all
huawei(config-if-shdsl-0/5)#alarm-config all 1
huawei(config-if-shdsl-0/5)#activate all 10
huawei(config-if-shdsl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1300 to 1314 mux
huawei(config)#port vlan 1300 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#port vlan 1300 to 1314 0/19 0
```

6. Add the service port.

   - Ports 0-15 in slot 0/5 provide the SHDSL service.
   - To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1300 port 0/5 0-14 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 9 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1510 smart
huawei(config)#port vlan 1510 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#tcont-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

NOTE

- You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
- You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 0 hwhw-10101010 password-auth huawei
profile-id 2
```

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1510
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1510
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1510 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 10 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#interface vlanif 1600
huawei(config)#port vlan 1600 0/19 0
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
```

4. Configure the MG interface.

Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
```

```
transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
10.176.6.33
```

Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

NOTE

After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

6. Configure the PSTN user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660032
```

Step 11 Configuring the QinQ private line service.

MA5600T-1 and MA5600T-4 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN 50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0
```

4. Add the service port.

To add the service port, run the **service-port** command. Note that the VPI and VCI values of the virtual port must be the same as those on the modem.

The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#traffic table ip index 7 cir off priority 0 priority-policy
local-Setting
huawei(config)#service-port vlan 50 shdsl 0/5/15 vpi 0 vci 35 rx-cttr 7
tx-cttr 7
```

Step 12 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 need to be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2/3 do not need to be authenticated.

1. Configure the xDSL.

In this example, there is no need to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

- Create a VLAN.

```
huawei(config)#vlan 100 smart
```

- Configure the VLAN upstream port.

```
huawei(config)#port vlan 100 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
```

```
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

- Configure the native VLAN.

NOTE

When the VLAN ID of the tag packet is the same as the VLAN ID of the native VLAN of the egress, the egress removes the tag of the packet. That is, the tagged packet becomes to the untagged packet (without VLAN ID) after the tagged packet passes through the egress.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#native-vlan 1 vlan 100
```

- Create the traffic profile.

```
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
local-Setting
```

- Add ADSL2+ ports 0/0/2 and 0/0/3 to VLAN 100.

```
huawei(config)#service-port vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8 tx-
cttr 8
huawei(config)#service-port vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8 tx-
cttr 8
```

3. Configure the multicast service.

- Enable the multicast proxy function.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

- Set the upstream port.

```
huawei(config-mvlan100)#igmp uplink-port 0/19/0
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

- Set the preview parameters.

  In this example, configure the preview authority profile with the preview duration for the program to 150s, the number of preview attempts to 6 each day and the preview interval to 60s.

```
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
huawei(config-btv)#quit
```

- Configured the program library.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10 preview-profile 1
huawei(config-mvlan100)#quit
```

- Configure the authority profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp user add port 0/2/3 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/2 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/2 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
```

Step 13 Configure the subtending multicast service.

1. Set the upstream port.

   The upstream port is already configured in **Step 12.3**.

2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 12.3**.

3. Configure the program library.

   The program library is already configured in **Step 12.3**.

4. Configure the multicast for the subtending port.

   - Specify a subtending port.
     ```
     huawei(config-btv)#igmp cascade-port 0/19/1
     ```
   - Modify a subtending port.
     ```
     huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
     ```
   - Add programs for the static subtending port.
     ```
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.1 vlan
     100
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.2 vlan
     100
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.3 vlan
     100
     huawei(config-btv)#quit
     ```

Step 14 Save the data.

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

----End

21.4 Configuring MA5600T-2

This topic describes how to configure MA5600T-2.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.

   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-1
       It will take several minutes, and console may be timeout, please use
     command
     idle-timeout to set time
     ```

```
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

- Enter the NMS VLAN interface mode.
  ```
  huawei(config)#interface vlanif 10
  ```
- Configure the IP address of the NMS interface.
  ```
  huawei(config-if-vlanif10)#ip address 10.10.1.3 255.255.255.0
  ```

2. Add the route.
   - Configure the route destined to the NMS (Trap destination address).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#quit
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
   ```
4. Configure SNMP.
   - Set the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Set the SysContact.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Set the SysLocation.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Set the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the SNMP version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable the trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```

6. Set trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
trap-paramsname 123
```

7. Set the trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801esc 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure GIU subtending

MA5600T-2 is subtended with MA5600T-3. Therefore subtending should be configured transparently transmit the VLAN data of MA5600T-3. There are four VLANs configured on MA5600T-3, with the VLAN ID of 10, 100, 1000 and 1300.

These VLAN are already configured with subtending, and it is unnecessary to configure them again.

Step 7 Configure the ADSL2+ service.

The MA5600T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure it based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,ETSI)
>      2: Full rate(G992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G992.1/3/5)
>      4: G.HS (G992.1~5)
>      5: ADSL (G992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G992.3~5)
>    Please select (0~6) [1]:
>  Trellis mode 1-disable 2-enable (1~2) [2]:
>  Bit swap downstream 1-disable 2-enable (1~2) [2]:
>  Bit swap upstream 1-disable 2-enable (1~2) [2]:
>  Please select the form of transmit rate adaptation downstream:
```

```
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set power management parameters? (y/n) [n]:
>  Will you set tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   The configuration data in the ADSL2+ channel profile is set according to the actual channel conditions.

```
huawei(config)#adsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:24
>    Maximum interleaving delay upstream (0~63 ms) [6]:12
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (32~32000 Kbps) [32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps) [32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:8000
>    Minimum transmit rate upstream (32~6000 Kbps) [32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps) [32]:
>    Maximum transmit rate upstream (32~6000 Kbps) [1024]:
>  Will you set rate thresholds? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the configured line profile and channel profile together to form line template 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your own needs. For details, see "**4.1.1 Configuring an ADSL2+ Template**." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   To configure the ADSL2+ traffic profile, run the **traffic table ip** command.

In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all 10
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

- Configure the GIU board.

  By default, the GE optical port of the GIU board works in the full duplex mode with the rate of 1000 Mbit/s.

  To change the port working mode and the port rate, run the **speed** and **duplex** commands in GIU mode.

  The settings must be the same as the settings of the peer device.

- Configure the VLAN.

  The ADSL2+ users of MA5600T-1 use the VLAN authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2020 smart
huawei(config)#port vlan 2020 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

8. Add the service port.

All ports in slot 0/2 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 2020 port 0/2 0-31 vpi 0 vci 35 user-
encap pppo
 rx-cttr 6 tx-cttr 6
```

Step 8 Configure the SHDSL service.

The MA5600T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

To configure the SHDSL traffic profile, run the **traffic table ip** command.

In this example, the default profile (profile 6) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shdsl-0/5)#deactivate all
huawei(config-if-shdsl-0/5)#alarm-config all 1
huawei(config-if-shdsl-0/5)#activate all 10
huawei(config-if-shdsl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T-2 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3020 smart
huawei(config)#port vlan 3020 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

6. Add the service port.

   - Ports 0-15 of in slot 0/5 provide the SHDSL service.
   - To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3020 port 0/5 0-15 vpi 0 vci 35 user-
encap
pppoe rx-cttr 6 tx-cttr 6
```

Step 9 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#interface vlanif 1600
huawei(config)#port vlan 1600 0/19 0
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
```

2. Configure the static route destined to the MGC.

   NOTE

   When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
```

4. Configure the MG interface.

   Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

   Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
 transfer udp mgcip_1 10.30.80.65 mgcport_1 2944 mg-media-ip 10.176.6.33
```

   Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

6. Configure the PSTN user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660032
```

Step 10 Configure the stacking multi-ISP wholesale service.

- ISP1 provides users of ports 0/2/0 to 0/2/10 with the multi-ISP wholesale service.
- ISP2 provides users of ports 0/2/11 to 0/2/20 with the multi-ISP wholesale service.
- ISP3 provides users of ports 0/2/21 to 0/2/30 with the multi-ISP wholesale service.

1. Create a stacking VLAN.

```
huawei(config)#vlan 60 to 62 smart
huawei(config)#vlan attrib 60 to 62 stacking
huawei(config)#stacking outer-ethertype 0x8000
```

2. Add the upstream port.

```
huawei(config)#port vlan 60 to 62 0/19 0
```

3. Add the service port.

```
huawei(config)#multi-service-port vlan 60 adsl 0/2 0-10 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
huawei(config)#multi-service-port vlan 61 adsl 0/2 11-20 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
huawei(config)#multi-service-port vlan 62 adsl 0/2 21-30 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
```

4. Configure the inner label.

```
huawei(config)#stacking label vlan 60 baselabel 111
huawei(config)#stacking label vlan 61 baselabel 112
huawei(config)#stacking label vlan 62 baselabel 113
```

Step 11 Configure the triple play service.

After the configuration, the following results should be achieved: Uses of port 0/2/31 can watch the programs stored on servers 224.1.1.1 and 224.1.1.2, and can preview the programs stored on server 224.1.1.3.

1. Configure the upstream port and the VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#vlan 101 mux
huawei(config)#port vlan 101 0/19 0
huawei(config)#vlan 102 smart
huawei(config)#port vlan 102 0/19 0
```

2. Configure the traffic table.

   The voice service has the highest priority, and the network access service has the lowest priority.

   Assume that the network access service uses traffic table 6, with the priority of 0. The following shows how to create the new traffic tables for the voice service and video service respectively.

```
huawei(config)#traffic table ip index 7 cir 1024 priority 7 priority-policy
Tag-In-Package
  Create traffic descriptor record
successfully
```

```
------------------------------------------------
  TD Index            :
7
  TD Name             : ip-traffic-
table_7
  Priority            :
7
  Copy Priority       :
-
  Mapping Index       :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index  :
-
  CTAG Default Priority:
0
  Priority Policy     : tag-
pri
  CIR                 : 1024
kbps
  CBS                 : 34768
bytes
  PIR                 : 2048
kbps
  PBS                 : 67536
bytes
  Referenced Status   : not
used

------------------------------------------------
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy tag-
In-Package
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index            :
8
  TD Name             : ip-traffic-
table_8
  Priority            :
5
  Copy Priority       :
-
  Mapping Index       :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index  :
-
  CTAG Default Priority:
0
  Priority Policy     : tag-
pri
  CIR                 :
off
  CBS                 :
off
  PIR                 :
off
  PBS                 :
off
  Referenced Status   : not
used

------------------------------------------------
```

3. Configure the service port.

```
huawei(config)#service-port vlan 100 adsl 0/2/31 vpi 0 vci 35
rx-cttr 8 tx-cttr 8
huawei(config)#service-port vlan 101 adsl 0/2/31 vpi 0 vci 36
rx-cttr 6 tx-cttr 6
huawei(config)#service-port vlan 102 adsl 0/2/31 vpi 0 vci 37
rx-cttr 7 tx-cttr 7
```

4. Configure DHCP relay mode for video service.

- Enable DHCP mode.
  ```
  huawei(config)#dhcp mode layer-3 option-60
  ```
- Configure the DHCP server.
  ```
  huawei(config)#dhcp-server 1 ip 10.1.1.2 10.1.1.3
  huawei(config)#dhcp domain video
  huawei(config-dhcp-domain-video)#dhcp-server 1
  ```
- Configure the gateway mapped to the DHCP domain.
  ```
  huawei(config)#interface vlanif 100
  huawei(config-if-vlanif100)#ip address 10.1.1.1 24
  huawei(config-if-vlanif100)#dhcp domain video gateway 10.1.1.1
  ```
- Enable DHCP Option82.
  ```
  huawei(config)#dhcp option82 enable
  ```

5. Configure DHCP relay mode for voice service.

- Configure the DHCP server.
  ```
  huawei(config)#dhcp-server 2 ip 10.4.4.2 10.4.4.3
  huawei(config)#dhcp domain voice
  huawei(config-dhcp-domain-voice)#dhcp-server 2
  ```
- Configure the gateway mapped to the DHCP domain.
  ```
  huawei(config)#interface vlanif 102
  huawei(config-if-vlanif102)#ip address 10.4.4.1 24
  huawei(config-if-vlanif102)#dhcp domain voice gateway 10.4.4.1
  ```
- Enable the DHCP option82.
  ```
  huawei(config)#dhcp option82 enable
  ```

6. Configure the multicast service.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#igmp uplink-port 0/19/0
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode mstp
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3 sourceip
10.10.10.10
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
huawei(config-btv)#igmp user add port 0/2/31 auth
huawei(config-btv)#igmp user bind-profile port 0/2/31 profile-name profile0
huawei(config-btv)#quit
```

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/31
```

Step 12 Configure the subtending multicast service.

1. Configure the upstream port.

   The upstream port is already configured in **Step 11.6**.

2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 11.6**.

3. Configure the program library.

   The program library is already configured in **Step 11.6**

4. Configure the multicast for the subtending port.

   - Specify a subtending port.

     ```
     huawei(config-btv)#igmp cascade-port 0/19/1
     ```

   - Modify a subtending port.

     ```
     huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
     ```

   - Add programs for the static subtending port.

     ```
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.1 vlan
     100
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.2 vlan
     100
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.3 vlan
     100
     huawei(config-btv)#quit
     ```

Step 13 Save the data.

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

----End

21.5 Configuring MA5600T-3

This topic describes how to configure MA5600T-3.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.

   - Create the NMS VLAN.

     ```
     huawei(config)#vlan 10 standard
     ```

   - Add the upstream port.

     ```
     huawei(config)#port vlan 10 0/19 0
     ```

   - Enter the NMS VLAN interface mode.

     ```
     huawei(config)#interface vlanif 10
     ```

   - Configure the IP address of the NMS interface.

     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.4 255.255.255.0
     ```

2. Add the route.

   - Configure the route destined to the NMS (Trap destination address).

```
huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
preference 1
huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
preference 1
```

- Configure the route destined to the time server.

```
huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
preference 1
huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
preference 1
```

- Configure the route destined to the log host.

```
huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
preference 1
huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
preference 1
```

3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.

- Set the community name and access authority.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

- Set the SysContact.

```
huawei(config)#snmp-agent sys-info contact HW-075512345678
```

- Set the SysLocation.

```
huawei(config)#snmp-agent sys-info location Shenzhen China
```

- Set the SNMP version.

  The SNMP version must be the same as the SNMP version of the NMS. In this example, the SNMP version is set as SNMP V2C.

```
huawei(config)#snmp-agent sys-info version v2c
```

5. Enable the trap sending.

```
huawei(config)#snmp-agent trap enable standard
```

6. Set trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
 trap-paramsname 123
```

7. Set the trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801ESC 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure the ADSL2+ service.

The MA5600T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure it based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,ETSI)
>      2: Full rate(G992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G992.1/3/5)
>      4: G.HS (G992.1~5)
>      5: ADSL (G992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G992.3~5)
>    Please select (0~6) [1]:
>  Trellis mode 1-disable 2-enable (1~2) [2]:
>  Bit swap downstream 1-disable 2-enable (1~2) [2]:
>  Bit swap upstream 1-disable 2-enable (1~2) [2]:
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set power management parameters? (y/n) [n]:
>  Will you set tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   The configuration data in the ADSL2+ channel profile is set according to the actual channel conditions.

```
huawei(config)#adsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:24
>    Maximum interleaving delay upstream (0~63 ms) [6]:12
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (32~32000 Kbps) [32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps) [32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:8000
>    Minimum transmit rate upstream (32~6000 Kbps) [32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps) [32]:
>    Maximum transmit rate upstream (32~6000 Kbps) [1024]:
>  Will you set rate thresholds? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the configured line profile and channel profile together to form line template 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your own needs. For details, see "**4.1.1 Configuring an ADSL2+ Template**." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   To configure the ADSL2+ traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all 1
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     By default, the GE optical port of the GIU board works in the full duplex mode with the rate of 1000 Mbit/s.

     To change the port working mode and the port rate, run the **speed** and **duplex** commands in GIU mode.

The settings must be the same as the settings of the peer device.

- Configure the VLAN.

  The ADSL2+ users of MA5600T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 3030 smart
huawei(config)#port vlan 3030 0/19 0
```

8. Add the service port.

   All ports of in slot 0/2 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3030 port 0/3 0-31 vpi 0 vci 35 user-
encap
 pppoe rx-cttr 6 tx-cttr 6
```

Step 7 Configure the SHDSL service.

The MA5600T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048 psd
 symmetric transmission Annex-A remote disable probe disable snr-margin ds-
curr 10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shdsl-0/5)#deactivate all
huawei(config-if-shdsl-0/5)#alarm-config all 1
huawei(config-if-shdsl-0/5)#activate all 10
huawei(config-if-shdsl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T-3 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3030 smart
huawei(config)#port vlan 3030 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

6. Add the service port.

   - Ports 0-15 of SHDSL board 0/5 provide the SHDSL service.

- To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3030 port 0/5 0-15 vpi 0 vci 35 user-
encap
 pppoe rx-cttr 6 tx-cttr 6
```

Step 8 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1530 smart
huawei(config)#port vlan 1530 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#tcont-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

NOTE

- You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
- You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 0 hwhw-10101010 password-auth huawei
profile-id 2
```

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1530
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1530
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1530 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 9 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#interface vlanif 1600
huawei(config)#port vlan 1600 0/19 0
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
```

4. Configure the MG interface.

Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
 transfer udp mgcip_1 10.30.80.65 mgcport_1 2944 mg-media-ip 10.176.6.33
```

Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

NOTE

After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

6. Configure the PSTN user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660000
```

Step 10 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 need to be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2 do not need to be authenticated.

1. Configure the xDSL.

In this example, it is unnecessary to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

- Create a smart VLAN.

```
huawei(config)#vlan 100 smart
```

- Set the VLAN upstream port.

```
huawei(config)#port vlan 100 0/19 0
```

- Configure the native VLAN.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
```

- Create the traffic profile.

```
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
tag-I
n-Packag
```

- Add ADSL2+ port 2 and 3 to VLAN 100.

```
huawei(config)#service-port vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8 tx-
cttr 8
huawei(config)#service-port vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8 tx-
cttr 8
```

3. Configure the multicast service

- Enable the multicast proxy function.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

- Configure the upstream port.

```
huawei(config-mvlan100)#igmp uplink-port 0/19/0 100
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

- Configure the preview parameters.

  In this example, set the preview duration for program 1 to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
huawei(config-btv)#quit
```

- Configure the program library.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10 preview-profile 1
huawei(config-mvlan100)#quit
```

- Configure the authority profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp user add port 0/2/3 no-auth
huawei(config-btv)#igmp user add port 0/2/2 auth
huawei(config-btv)#igmp user bind-profile port 0/2/16 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
huawei(config-btv)#quit
```

Step 11 Save the data.

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

----End

21.6 Configuring MA5600T-4

This topic describes how to configure MA5600T-4.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.5 255.255.255.0
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination address).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   ```

```
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.

   - Set the community name and access authority.

     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```

   - Set the SysContact.

     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```

   - Set the SysLocation.

     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```

   - Set the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the SNMP version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```

5. Enable the trap sending.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

6. Set trap destination address.

   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```

7. Set the trap source address.

   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801ESC 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure the VDSL2 service.

The MA5600T supports the VDSL2 Internet service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the VDSL2 service. For other encapsulation modes, see "**17.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the VDSL2 line profile.

   You can configure the VDSL2 line profile based on your requirements.

```
huawei(config)#vdsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,G993.2)
>      2: Full rate(G992.1/3/5,T1.413,G993.2)
>      3: G.DMT (G992.1/3/5,G993.2)
>      4: G.HS (G992.1~5,G993.2)
>      5: ADSL (G.992.1~5,T1.413)
>      6: VDSL (G993.2)
>    Please select (0~6) [1]:
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed 2-adaptAtStartup (1~2) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed 2-adaptAtStartup (1~2) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set UPBO parameters? (y/n)[n]:
>  Will you set RFI notch configuration parameter? (y/n) [n]:
>  Will you set ADSL tone blackout configuration parameter? (y/n) [n]:
>  Will you set VDSL tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the VDSL2 channel profile.

   You can configure the VDSL2 channel profile based on your requirements.

```
huawei(config)#vdsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:1
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [1]:3
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [1]:3
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~200 ms) [20]:
>    Maximum interleaving delay upstream (0~200 ms) [20]:
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (128~100000 Kbps) [128]:512
>    Maximum transmit rate downstream (512~100000 Kbps) [100000]:
>    Minimum transmit rate upstream (128~100000 Kbps) [128]:
>    Maximum transmit rate upstream (128~100000 Kbps) [100000]:
  Add profile 10 successfully
```

3. Configure the VDSL2 line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#vdsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
  Add template 10 successfully
```

4. Configure the VDSL2 alarm profile.

   You can configure the VDSL2 alarm profile based on your requirements. For the configuration, see "**4.1.3 Configuring VDSL2 Profiles**." In this example, the default alarm profile 1 is used.

5. Configure the VDSL2 traffic profile.

   You can configure the VDSL2 traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the VDSL2 port.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#alarm-config all
huawei(config-if-vdsl-0/2)#activate all template-index 10
huawei(config-if-vdsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     In general, the GE optical port uses the default gigabit full-duplex mode.

     To change the mode, switch to the GIU config mode. Then run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

     The settings of the upstream port must be the same as the settings on the peer device.

   - Configure the VLAN.

     The VDSL2 users of MA5600T-1 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 1800 smart
huawei(config)#port vlan 1800 0/19 0
```

8. Add the service port.

   All ports in slot 0/2 provide the VDSL2 Internet access service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 1800 port 0/2 0-23 vpi 0 vci 35 user-encap
 pppoe rx-cttr 6 tx-cttr 6
```

Step 7 Configure the QinQ private line service.

MA5600T-4 and MA5600T-1 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN 50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0
```

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values of the service port must be the same as those on the modem.

   The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#service-port vlan 50 shdsl 0/5/15 vpi 0 vci 35
 rx-cttr 7 tx-cttr 7
```

Step 8 Save the data.

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

----End

21.7 Verification

All services configured on all DSLAMs run in the normal state.

22 Appendix: Common Configuration Operations

About This Chapter

This chapter describes how to configure the common service. There is no obvious logical relation between configurations. You can perform configurations according to actual requirements.

22.1 Manually Disconnecting Login Operators

This topic describes how to disconnect one or multiple online users who have logged in to the device.

Context

Only the super user and the administrator can forcedly disconnect the users at lower levels.

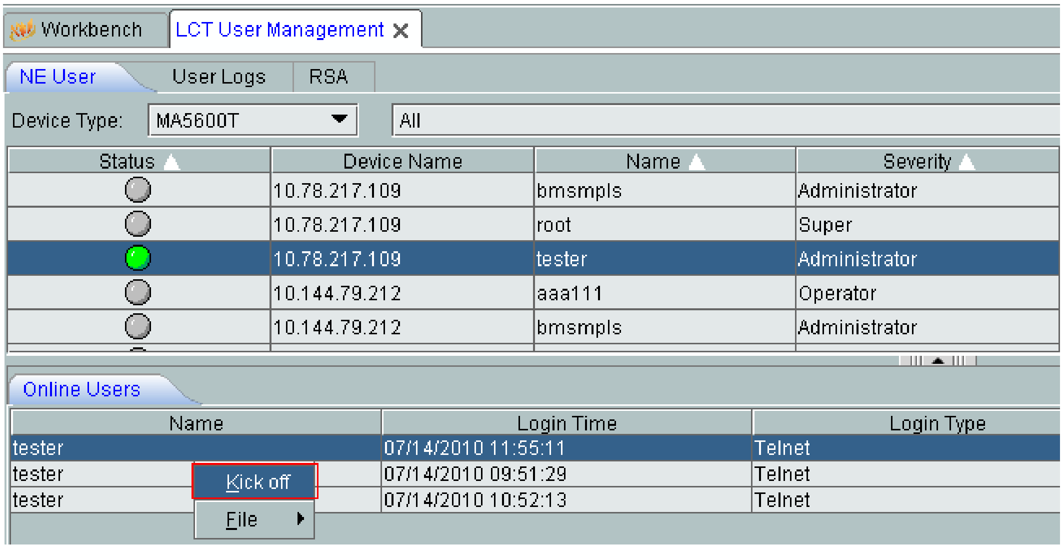
Procedure

Step 1 Choose **Administration** > **NE Security Management** > **LCT User Management**.

Step 2 On the **NE User** tab page that is displayed, select a required device type from the **Device Type** drop-down list.

Step 3 Click **Filter** and enter proper parameters to display the required NE users.

Step 4 Select the record of the NE user to be forcedly deleted from the NE user list on the **Online Users** tab page, right-click and choose **Kick off**.



Device Type: MA5600T All

Status	Device Name	Name	Severity
○	10.78.217.109	bmsmpls	Administrator
○	10.78.217.109	root	Super
●	10.78.217.109	tester	Administrator
○	10.144.79.212	aaa111	Operator
○	10.144.79.212	bmsmpls	Administrator

Name	Login Time	Login Type
tester	07/14/2010 11:55:11	Telnet
tester	07/14/2010 09:51:29	Telnet
tester	07/14/2010 10:52:13	Telnet

----End

Result

After a user is forcedly disconnected, the user cannot perform any operation on the system.

Related Command

To...	Run Command...	Remarks
Query the information about the current login user	**display client**	You can query the information about only the login users whose levels are equal to or lower than yours.

To...	Run Command...	Remarks
Disconnect a login user forcedly	**client kickoff** *clientid*	First run the **display client** command to query *clientid*, and then specify the user to be disconnected by *clientid*.

22.2 Querying the MAC Addresses of the Online Users and the Ports That Provide the Access for the Users

Procedure

Step 1 Run the **display mac-address all** command to query the MAC addresses of all the online users.

Step 2 Run the **display location** command to query the ports of the online users according to the specified MAC addresses.

----End

22.3 Changeing the Management IP Address and VLAN of a device

Procedure

Step 1 Log in to the gateway where the MA5600T/MA5603T is located, and then run the **telnet** command to log in to the MA5600T/MA5603T through the gateway.

Step 2 Run the **display packet-filter** or **display firewall packet-filter statistics** command to query the ACL configuration. Make sure that the new IP address can access the device.

Step 3 Run the **vlan** command to create a management VLAN, run the **port vlan** command to add an upstream port to the VLAN, and then run the **interface vlanif** command to enable the Layer 3 interface of the VLAN. Then, run the **ip address** command to configure the management IP address, and run the **ip route-static** command to add a route.

Step 4 Log out of the MA5600T/MA5603T. Run the **ip address** command to change the IP address of the gateway interface to be in the same subnet as the new management IP address. Then, use the new management IP address to log in to the device. Run the **undo interface vlanif** command to delete the Layer 3 interface of the original management VLAN, run the **undo port vlan** command to delete the upstream port of the original management VLAN, and then run the **undo vlan** command to delete the original management VLAN. Run the **undo ip route-static** command to delete the original route.

Step 5 Run the **save** command to save the data, and then exit.

----End

22.4 Changing the Port Rate of the xDSL User

This topic describes how to change the port rate of the xDSL user on the MA5600T/ MA5603T.

Context

After using the device, the user may change the default user name and password, users may forget their password.

Procedure

- Changing the port rate of the ADSL user.
  1. Run the **interface adsl** command to enter the ADSL mode.
  2. Run the **deactivate** command to deactivate the port.
  3. Run the **activate** command to activate the port and bind a new line profile to the port.
- Changing the port rate of the VDSL user.
  1. Run the **interface vdsl** command to enter the VDSL mode.
  2. Run the **deactivate** (in the common mode) or **deactivate** (in the TI mode) command to deactivate the port.
  3. Run the **activate** (in the common mode) or **activate** (in the TI mode) command to activate the port and bind a new line profile to the port.
- Changing the port rate of the SHDSL user.
  1. Run the **interface shl** command to enter the SHDSL mode.
  2. Run the **deactivate** command to deactivate the port.
  3. Run the **activate** command to activate the port and bind a new line profile to the port.

----End

22.5 Changing the Rate of the User Port in a xPON System

Context

In a PON system, when the rate of the user port fails to meet the requirement, the possible causes are as follows:

- The rate of the ONT port does not meet the requirement.
- The user bandwidth configured in the DBA profile is improper.

Procedure

- When the rate of the ONT port does not meet the requirement, run the **ont port attribute** command to change the rate of the ONT port.
- When the user bandwidth configured in the DBA profile is improper, do as follows:
  1. Run the **undo tcont** command to unbind the T-CONT from the DBA profile.

2. Run the **dba-profile modify** command to change the user bandwidth configured in the DBA profile.
3. Run the **tcont** command to bind the T-CONT to the DBA profile.

----End

22.6 Re-binding the ONT Line Profile

This topic describes how to re-bind the ONT line profile on the MA5600T/MA5603T in the GPON profile mode.

Context

Bind DBA profiles to T-CONTs in ONT line profile mode or GPON mode. Run the **display ont info** ***portid ontid*** command to query the ONT status. Bind T-CONTs with asterisk (*) to DBA profiles in GPON mode.

Procedure

- Bind the DBA profile to the T-CONT by running the **tcont** command in the ONT line profile mode.
  1. Run the **interface gpon** command to enter the GPON mode.
  2. Run the **ont modify** ***portid ontid*** **ont-lineprofile-id** ***profile-id*** command to bind a new line profile to the ONT.

  NOTE

  If the T-CONT in the original line profile is bound to the GEM port and a traffic stream is configured on the GEM port, the T-CONT in the new profile must be bound to the DBA profile. Otherwise, the configuration fails.
- Bind the DBA profile to the T-CONT by running the **tcont bind-profile** command in the GPON mode.
  1. Run the **interface gpon** command to enter the GPON mode.
  2. Run the **ont modify** ***portid ontid*** **ont-lineprofile-id** ***profile-id*** command to bind a new line profile to the ONT.

  NOTE

  If the T-CONT in the original line profile is bound to the GEM port and a traffic stream is configured on the GEM port, the T-CONT in the new profile must be bound to the GEM port. Otherwise, the configuration fails.

----End

22.7 Calculating the Remaining Bandwidth of a PON Port

Context

- The remaining bandwidth of a PON port on the MA5600T/MA5603T cannot be calculated. When the downstream packets exceed 2.5 G, excessive packets will be discarded. To limit the downstream bandwidth of a specified service, refer to **Configuring GPON Rate Limitation**.

- You can run a command to query the remaining upstream bandwidth of a PON port on the MA5600T/MA5603T or manually calculate the remaining upstream bandwidth of a PON port on the MA5600T/MA5603T.
- Each ONT has a default T-CONT 0 that is bound to DBA profile 1 by default for transmitting ONT management messages. This T-CONT can be modified but cannot be deleted.
- 8000 frames are sent per second (namely, one frame per 125 μs) in the PON network. If one byte (8 bits) is assigned to an ONT per each frame, the rate is 64 kbit/s (8 bits/125 μs). Therefore, 1 byte can represent 64 kbit/s in the PON network.

Procedure

- Run a command to query the remaining upstream bandwidth of a PON port:

  Run the **display port info(gpon)** command to query the remaining committed bandwidth of a port. The remaining bandwidth is 1164032 kbps.

  NOTE

  When you run the **display port state(gpon)** command to query the port status, the **Available bandwidth** parameter in the output result indicates the available bandwidth of the port, that is, the actually available bandwidth. This value is a dynamic value. In an actual network, although multiple ONTs may be configured for an xPON port, yet some ONTs may not fully occupy their fixed bandwidth. The bandwidth that is not occupied is the remaining bandwidth.

- Manually calculate the remaining upstream bandwidth of a PON port:
  1. Run the **display ont info(gpon)** command to query the related information about the ONT of a port.
  2. Run the **display DBA-profile** command to query the DBA profile.
  3. The remaining upstream bandwidth of the PON port is the difference between the total upstream bandwidth and the occupied bandwidth.
     - Maximum upstream bandwidth of the PON port: 1244160 kbit/s = 19440 bytes. .
     - Occupied bandwidth:
       - Bandwidth reserved for emergency PLOAM messages of the OLT: (52 x 64) kbit/s = 52 bytes
       - PLOu bandwidth reserved for each ONT: 32 bytes.
       - The fixed bandwidth of the DBA profiles that bound ONT service T-CONTs.

----End

22.8 Changing IP Address of Voice service VLAN Interface

The configured IP address is placed into the IP address pool and functions as the signaling IP address of the MG or the media IP address, which is used to communicate with the MGC. The IP address of the voice VLAN L3 interface cannot be changed but it can be added again after being deleted.

Context

An IP interface can be added only after the L3 interface of the VLAN is configured.

Procedure

Step 1 In the Main Topology, double-click the required **MA5603UMA5680TMA5600V3MA5600T** or **MA5603TMA5606TUA5000(IPMB)UA5000(PVMV1)**ONU in the **Physical Root** navigation tree; or right-click the required **MA5603UMA5680TMA5600V3MA5600T** or **MA5603TMA5606TUA5000(IPMB)UA5000(PVMV1)**ONU and choose **NE Explorer** from the shortcut menu.

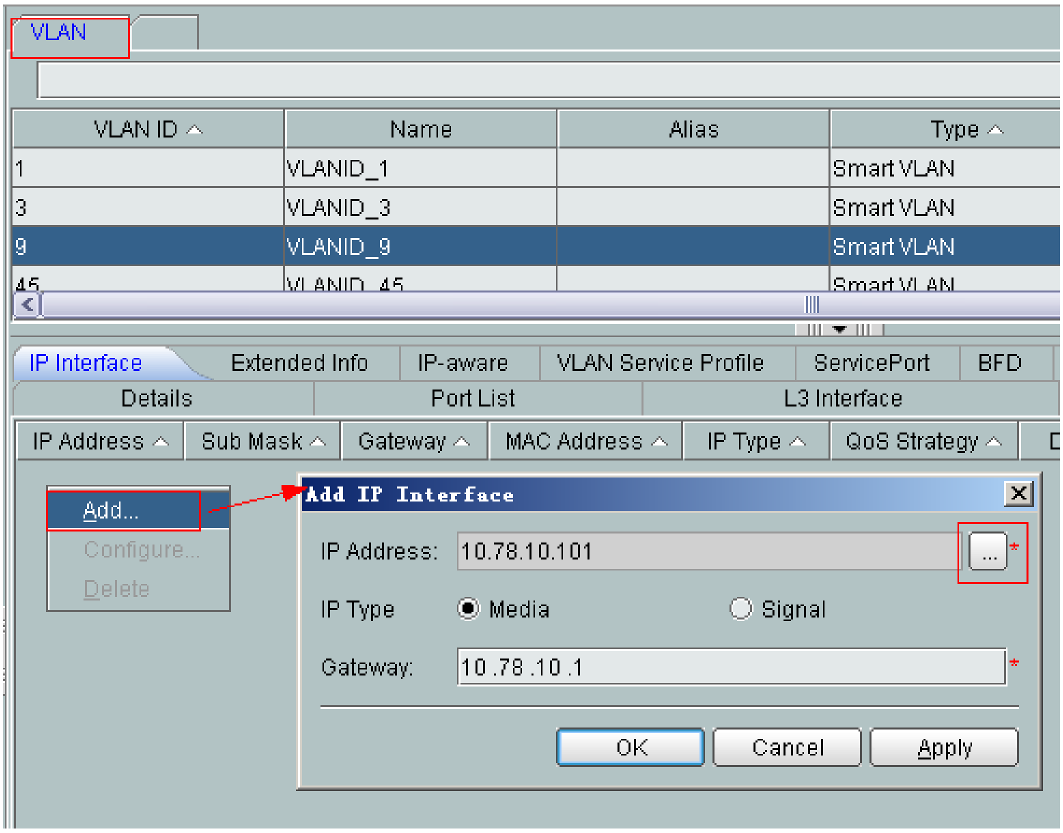
Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.

Step 4 Select a VLAN from the VLAN list, and then click the **IP Interface** tab in the lower pane.

Step 5 On the **IP Interface** tab page, right-click, and then choose **Add** from the shortcut menu.

Step 6 In the dialog box that is displayed, set the parameters of the IP interface.



VLAN ID	Name	Alias	Type
1	VLANID_1		Smart VLAN
3	VLANID_3		Smart VLAN
9	VLANID_9		Smart VLAN
45	VLANID_45		Smart VLAN

Add IP Interface

IP Address: 10.78.10.101 ... *

IP Type ● Media ○ Signal

Gateway: 10 .78 .10 .1 *

Step 7 Click **OK**.

----End

Related Command

To...	Run Command...	Remarks
Change IP address of voice VLAN L3 interface	● If the original IP address of the VLAN L3 interface is not added in the media or signaling IP address pool, in the VLAN interface mode, run the **undo ip address** command to delete the original IP address and then run the **ip address** command to configure a new IP address. ● If the original IP address of the VLAN L3 interface is added in the media or signaling IP address pool, in the VoIP mode, run the **undo ip address** command to delete the IP address from the IP address pool. Then, enter the VLAN interface mode, run the **undo ip address** command to delete the original IP address, and run the **ip address** command to configure a new IP address.	User rights: operator or higher

22.9 Loading the Version of the Standby Control Board

This topic describes how to load the version of the standby control board of the MA5600T if the active control board functions properly.

Context

If one of the control boards of the MA5600T is faulty, the faulty control board needs to be replaced.

Procedure

- For H801SCUN or H801SCUH, there is no need to check the versions of control boards on the live network or the version of the substitute control board. This is because the H801SCUN supports duplicating of all information to the standby control board. No manual operation is required.

- For H801SCUB, H801SCUF, or H801SCUL,
  - When the version of the original control board is earlier than V800R008C01, automatic information duplication to the standby control board is supported if the version of the substitute control board is V800R006C02 or later. No manual operation is required.
  - When the version of the original control board is V800R008C01 or later, automatic information duplication to the standby control board is supported if the version of the substitute control board is V800R008C01 or later. No manual operation is required.
  - When the version of the original control board is V800R008C01 or later, a patch is required for the substitute control board to support automatic information duplication to the standby control board if the version of the substitute control board is earlier than V800R008C01. Related patches are as follows:
    - V800R006C02: SPC124 or a later patch
    - V800R007C00: SPC307 or a later patch
    - V800R007C01: SPC307 or a later patch
  - When the version of the substitute control board is earlier than V800R006C02. automatic information duplication to the standby control board is not supported. Therefore, manually upgrade the substitute control board to the version of the control board on the live network for information synchronization.

----End

22.10 Realizing the Communication Between Users on the Same Board

This topic describes how to realize the communication between users on the same board, including users in the same VLAN and in different VLANs

Context

When users are in different VLANs, user ports are isolated at Layer 2. Therefore, even if users are on the same board, they cannot directly communicate with each other at Layer 2. To realize the communication between users on the same board, users must belong to the same super VLAN, and therefore different sub VLANs can communicate with each other through the ARP proxy. That is, through the Layer 3 interface of the super VLAN, the services of different sub VLANs can be forwarded at L3, and then users in the same super VLAN can communicate with each other.

Procedure

Step 1 Create VLAN 20,VLAN 30.

```
huawei(config)#vlan 20 smart
huawei(config)#vlan 30 smart
```

Step 2 Create super VLAN 40.

```
huawei(config)#vlan 40 super
```

Step 3 Add a sub VLAN 20 to super VLAN 40.

```
huawei(config)#supervlan 40 subvlan 20
```

Step 4 Add a sub VLAN 30 to super VLAN 40.

```
huawei(config)#supervlan 40 subvlan 30
```

Step 5 Enable the ARP proxy globally.

```
huawei(config)#arp proxy enable
```

Step 6 Enable the ARP proxy on VLAN Layer 3 interface 40.

```
huawei(config)#interface vlanif 40
huawei(config-if-Vlanif40)#arp proxy enable
```

Step 7 Configure the IP address of VLAN Layer 3 interface 40.

```
huawei(config-if-Vlanif40)#ip address 10.1.1.254 24
```

When only users in different VLANs need to communicate with each other, steps 8 is not required.

Step 8 Enable the ARP proxy on VLAN20,VLAN30.

```
huawei(config-if-vlanif40)#arp proxy enable subvlan 20
huawei(config-if-vlanif40)#arp proxy enable subvlan 30
```

----End

22.11 Restricting User Login using ACL

This topic describes how to filter user IP addresses using access control list (ACL) to restrict user logins.

Prerequisites

The IP address of the user to be restricted is obtained.

Procedure

Step 1 Run the **acl** *basic-acl-number* command to create an ACL and enter the ACL mode.

If the specified ACL ID does not exist, create a new ACL. Then, the system enters the corresponding ACL configuration mode. If the specified ACL sequence number exists, the system directly enters the corresponding ACL configuration mode.

Step 2 Run the **rule** [*rule-id*] **deny source** { *sour-addr* { *sour-wildcard* | **0** } | **any** } command to create an ACL rule.

This ACL rule forbids the data packets with the specified IP address or IP address segment to pass.

Step 3 Run the **firewall packet-filter** command to apply the ACL rule to the Ethernet port or the VLAN interface so that unauthorized users cannot access the device through the inband or outband channel.

----End

Example

To create basic ACL 2010, create ACL rule 5, forbid the user with IP address 10.71.43.70 to log in, and apply the ACL rule to the Ethernet port, do as follows:

```
huawei(config)#acl 2010
huawei(config-acl-basic-2010)#rule 5 deny source 10.71.43.70 0
huawei(config-acl-basic-2010)#quit
huawei(config)#firewall enable
huawei(config)#interface meth 0
huawei(config-if-meth0)#firewall packet-filter 2010 inbound
 ACL applied successfully
```

22.12 Configuring ACL and Time Segment to Restrict Users'Access to the Internet

This topic describes how to configure ACL rules on a specified port so that users can access the Internet in a specified time segment.

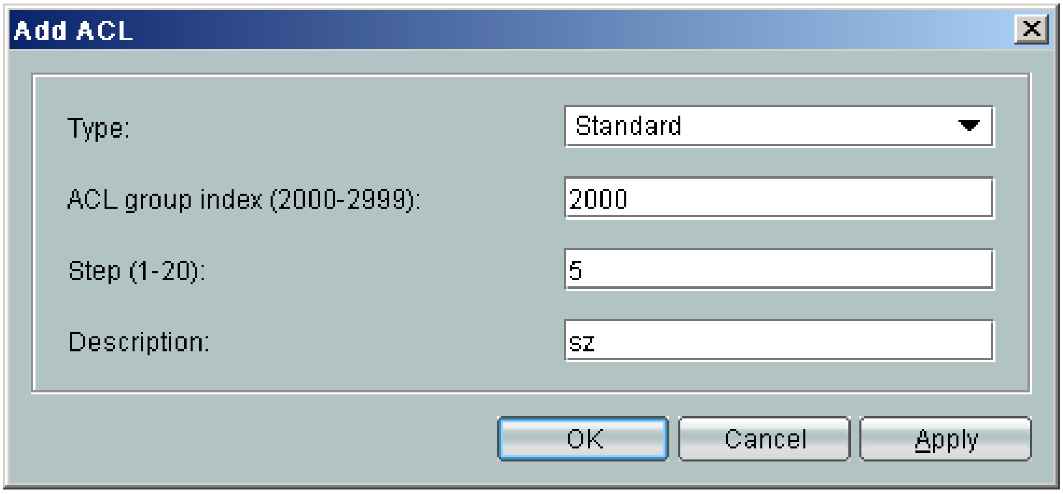
Procedure

Step 1 **Add a time segment.**

1. In the Main Topology, double-click the required NE in the **Physical Root** navigation tree; or right-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **QoS** > **QoS&ACL** from the navigation tree.
3. Click the **Time Segment Management** tab, right-click the list, and then choose **add**.
4. In the dialog box that is displayed, set the name of the time segment.
5. Click **OK**.
6. Select the added time segment, click the **One-off Time** tab or the **Periodic Time** tab in the lower pane, right-click, and then choose **Add**.
7. In the dialog box that is displayed, set the parameters.
   - In the **Add One-off Time** dialog box, set **Start Time** and **End Time** of the time segment.
   - In the **Add Periodic Time** dialog box, set the period, **Start Time** and **End Time** of the time segment.
8. Click **OK**.

Step 2 **Add an ACL group (considering a standard ACL group as an example).**

1. Click the **ACL Management** tab, right-click the list, and then choose **Add**.
2. In the dialog box that is displayed, set **Type**, **Step**, and **ACL group index** of the ACL group.



Type: Standard

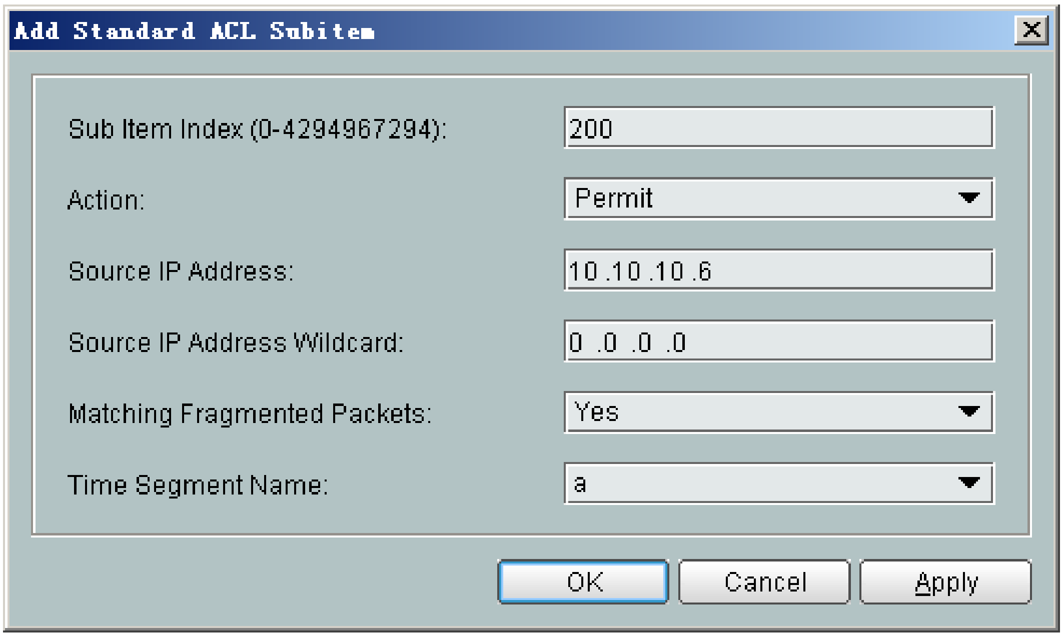
ACL group index (2000-2999): 2000

Step (1-20): 5

Description: sz

3. Click **OK**.

4. Select the added ACL, and then click the **Standard Sub Item** tab in the lower pane. Right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set **Sub Item Index**, **Action**, **Source IP Address**, **Source IP Address Wildcard**, **Matching Fragmented Packets**, and **Time Segment Name**.



Sub Item Index (0-4294967294): 200

Action: Permit

Source IP Address: 10 .10 .10 .6

Source IP Address Wildcard: 0 .0 .0 .0

Matching Fragmented Packets: Yes

Time Segment Name: a

6. Click **OK**.

Step 3 **Add QoS rules (considering adding rules in batches as an example).**

1. Click the **Time Segment Management** tab, right-click the list, and then choose **Batch Add** > **Packet Filter**.
2. In the dialog box that is displayed, set the parameters.

   There are three steps for adding packets filtering, that is, selecting a port, selecting ACL rules, and filling in the packets filtering parameters. The specific operations are as follows:

   - Select a port to be bound, and then click **Next**.
   - Select ACL rules referenced by the port, and then click **Next**.
   - Select the packets filtering parameter, that is, the direction for packets filtering.
3. Click **OK**.

----End

Related Command

To...	Run Command...	Remarks
Add a time segment	**time-range**	The ACL time segment can be relative time or absolute time. ● The relative time refers to the periodic time, for example, from 8:30 to 18:30 on each Monday. ● Absolute time refers to a time range from a specific time to another specific time, for example, from 2006-06-08 12:00 to 2006-08-08 18:00. Guideline for the validity of a time segment: ● When a time segment includes only absolute time or relative time, the union set of all intervals in the time segment takes effect. ● When a time segment includes both absolute time and relative time, the intersection set of the union sets of both relative time and absolute time takes effect.
Add a basic ACL group	**acl** *basic-acl-number*	The range of basic ACL IDs are 2000-3999. Basic ACL rules are used when ACL rules need to be created according to the L3 source IP address.
Add basic ACL rules	**rule** [*rule-id*] [**priority** *priority-value*] { **permit** | **deny** } [[**source** { *sour-addr* { *sour-wildcard* | **0** } | **any** }] | [**time-range** *time-range-name*] | [**fragment**]] *	The parameters are as follows: ● *rule-id*: Indicates the ID of an ACL rule. To create an ACL rule with a specified ID, use this parameter. ● **permit**: Indicates the keyword for allowing the data packets that meet the related conditions to pass. ● **deny**: Indicates the keyword for discarding the data packets that meet the related conditions. ● **time-range**: Indicates the keyword of the time segment during which the ACL rule is effective.

To...	Run Command...	Remarks
Activate an ACL	**packet-filter** { **inbound** | **outbound** } { **user-group** *access-list-number1* [**rule** *rule-id*] | { **ip-group** *access-list-number2* [**rule** *rule-id*] | **link-group** *access-list-number3* [**rule** *rule-id*] } * } **port** *frameid/slotid/portid*	After an ACL rule is configured on a service port by running the **packet-filter** command, the ACL rule takes effect to all other service ports on the same service board. In the case of an upstream port, the ACL rule takes effect to only the upstream port itself.

22.13 Confirming an Upgraded Board

Context

After a board (newly added) is upgraded on a device, the board is not displayed in the software. Or, the board status is displayed as **Auto_find**. In such cases, data cannot be configured on the newly added board.

Procedure

Step 1 Added offline. After you run the **board add** command to add a board to a vacant slot, the system generates a board fault alarm. After that, insert the board into the corresponding slot. If the type of the inserted board is the same as the type of the board added offline, the system generates a board recovery alarm (alarm ID 0x02310000). If the board types do not match, the system generates a non-match alarm (alarm ID 0x02300082).

NOTE

- To add a board successfully, make sure that the shelf ID and slot ID of the board added through the command line interface (CLI) are the same as the actual shelf ID and slot ID of the board inserted manually.
- To add a board successfully, make sure that the type of the board added through the CLI is the same as the actual board type.

Step 2 Auto-found. Insert the board into a vacant slot. When the system prompts that the board is automatically found, you need to run the **board confirm** command to confirm the board.

----End

22.14 Changing Upstream Board for Expanding the Bandwidth of the Upstream Port

Context

When the upstream bandwidth of the device is insufficient, how to expand the bandwidth by changing the port type? Assume that the 2GE GICF upstream board is used in the telecommunications room, and the upstream bandwidth is to be expanded to 4GE or higher.

Procedure

Step 1 Confirm the supported boards: According to the board matching relation description in the *Release Notes*, it can be confirmed that the GICD board supports upstream transmission through the 4GE optical port, and the X1CA/X2CA board supports upstream transmission through the 10GE optical port.

NOTE

Assume that the GICD board is selected.

Step 2 Confirm the installation position of the board: According to the *Hardware Description*, you can confirm the installation position of the GICD board.

Step 3 Confirm the cable required: According to the external ports of each board as described in *board* in the *Hardware Description*, optical fibers are required for connecting the board to the ODF.

Step 4 Install the selected board and optical fibers to expand the upstream bandwidth.

----End