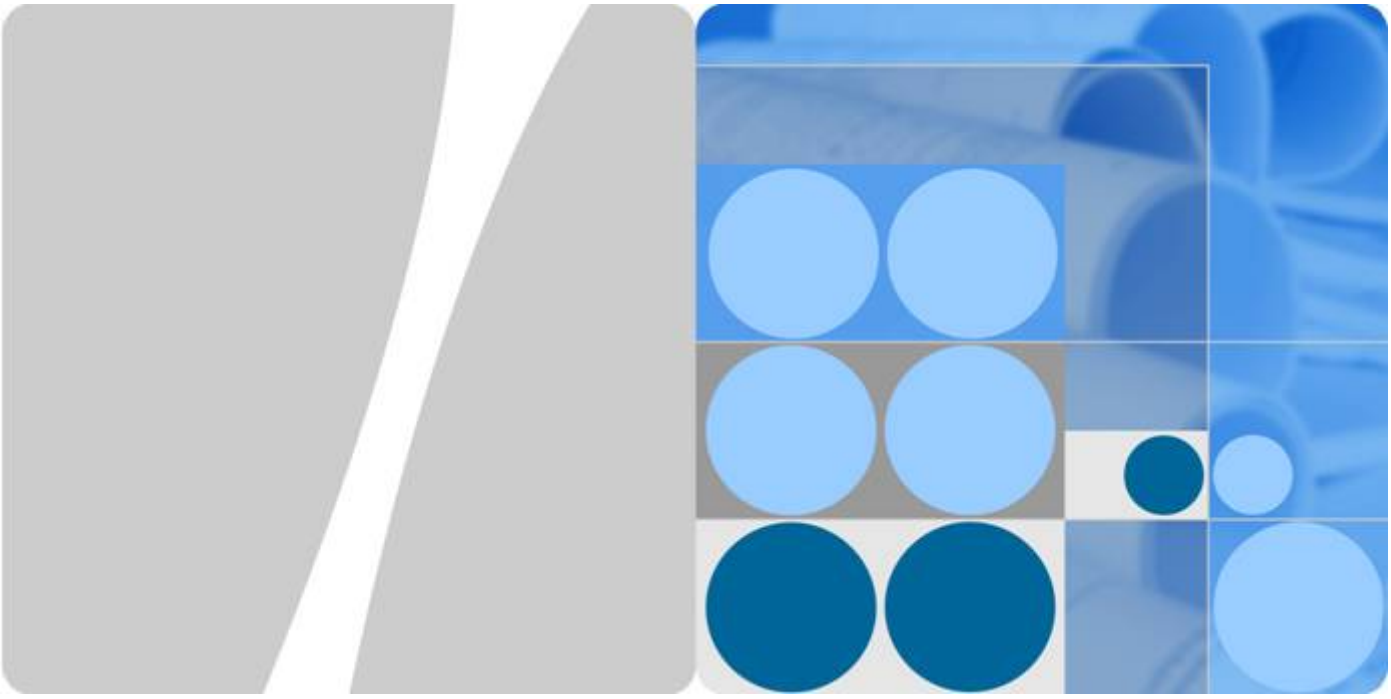


SmartAX MA5616 Multi-service Access Module

V800R308C01

Configuration Guide

Issue 04

Date 2011-10-30

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes the configuration of important services supported by the MA5616. The description covers the following topics:

- Purpose
- Networking
- Data plan
- Prerequisite(s)
- Note
- Configuration flowchart
- Operation procedure
- Result

This document helps users to know the configuration of important services on the MA5616.

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.

Symbol	Description
TIP	Indicates a tip that may help you solve a problem or save your time.
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**.

Updates in Issue 04 (2011-10-30)

Compared with issue 03 (2011-03-31) of V800R308C01, 04 (2011-10-30) has the following changes:

Added: **3.3.3 Configuring the System Energy-Saving Function**

The following information is modified:

- **3.1.4 Configuring Inband Management (GE Upstream)**

- **3.3.1 Configuring an Uplink Ethernet Port**
- **3.15.1.2 Configuring the Monitoring Through the ESCM**
- **3.15.2.1 Configuring the Monitoring Through the EPS30-4815AF**
- **3.15.3 Configuring the Monitoring Through the Fan**

Updates in Issue 03 (2011-03-31)

Compared with issue 02 (2011-03-05) of V800R308C01, 03 (2011-03-31) has the following changes:

The following information is modified: **2 Checking Before the Configuration**

Updates in Issue 02 (2011-03-05)

Compared with issue 01 (2011-01-07) of V800R308C01, 02 (2011-03-05) has the following changes:

The following information is modified:

- **3.6 Configuring a VLAN**
- **3.8.1.1 Configuring the Adaptive Clock Reference Source**
- **3.11.3 Preventing the Attack of Invalid Users**
- **4 Configuring the Ethernet CFM OAM**
- **5.3 Configuring an xDSL Port**
- **6.2.2 Configuring the Multicast Program**
- **8.1.4 Configuration Example of the xDSL IPoA Internet Access Service**

Issue 01 (2011-01-07)

Compared with issue 02 (2010-07-25) of V800R307C01, V800R308C01 has the following changes:

Added:

- **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**
- **3.8 Configuring the System Clock**
- **3.9 Configuring the System Time**
- **3.10 Configuring the User Security**
- **3.12 Configuring AAA**
- **3.13 Configuring the ACL for Packet Filtering**
- **5 Configuring the xDSL Internet Access Service**
- **9 Configuration Example of Services on the MA5616 Through GE Upstream Transmission**

Contents

1 Deploying Network Devices

About This Chapter

Deploy the ONUs at sites according to network planning so that the NMS, OLT, and ONU can communicate with each other.

1.1 Introduction to the Network Device Deployment

This topic describes how to deploy network devices, including optical network unit (ONU) data plan, ONU offline deployment (through the NMS or the CLI of the OLT), ONU installation, and ONU binding. After the deployment, you can remotely configure services for the ONU.

Table 1-1 describes the activities involved in network device deployment in the scenario with the NMS.

Table 1-1 Activities involved in network device deployment in the scenario with the NMS

Activities	Description
ONU data plan **NOTE** The ONU refers to MA5616.	Perform the data plan according to the network planning sheet provided by the NMS. The resource deployment sheet will be generated finally.
ONU offline deployment	Import the resource deployment sheet through the NMS to implement the predeployment for the ONU.
ONU installation	The hardware installation engineer draws the ONU from the storehouse and installs it at the destination site. After installing it and confirming that the hardware is fault-free, the hardware installation engineer returns the ONU type, service port information, and ONU SN to the commissioning engineer.
ONU binding	The IP address and the SN of the ONU are bound through the NMS.

Table 1-2 describes the activities involved in network device deployment in the scenario without the NMS.

NOTE

In the scenario without the NMS, you can add the ONT through the OLT by using one of the following methods:

- Method 1:
  1. Install the ONU and power on the device normally.
  2. Run the **port** *portid* **ont-auto-find** command in the GPON mode to enable the ONU auto-discovery function.
  3. The OLT discovers the ONU automatically.
  4. Run the **ont confirm** command to in the GPON mode confirm the automatically discovered ONU.
- Method 2:
  1. Run the **ont add** command in the GPON mode to add the ONU on the OLT offline.
  2. Install the ONU and power on the device normally.

In this topic, method 1 is used for the deployment.

Table 1-2 Activities involved in network device deployment in the scenario without the NMS

Activities	Description
ONU data plan **NOTE** The ONU refers to MA5616.	Perform the data plan for the OLT and ONU according to the actual FTTx service plan and the corresponding OLT version.
ONU installation	The hardware installation engineer draws the ONU from the storehouse and installs it at the destination site. After installing it and confirming that the hardware is fault-free, the hardware installation engineer returns the ONU type, service port information, and ONU SN to the commissioning engineer.
ONU deployment	Enable the auto-discovery function on the PON port through the CLI command of the OLT, confirm the automatically discovered ONU, and add the ONU by using the preconfigured profile.
Configuration of the services of the ONU	You can telnet to the ONU according to the management IP address of the ONU to configure the services for the ONU.

1.2 Example of Deploying Network Devices

This topic describes how to deploy network devices in the scenario with or without the NMS.

Prerequisites

- Network devices and lines must be in the normal state.
- The control board and the GPON service board of the OLT must be in the normal state.

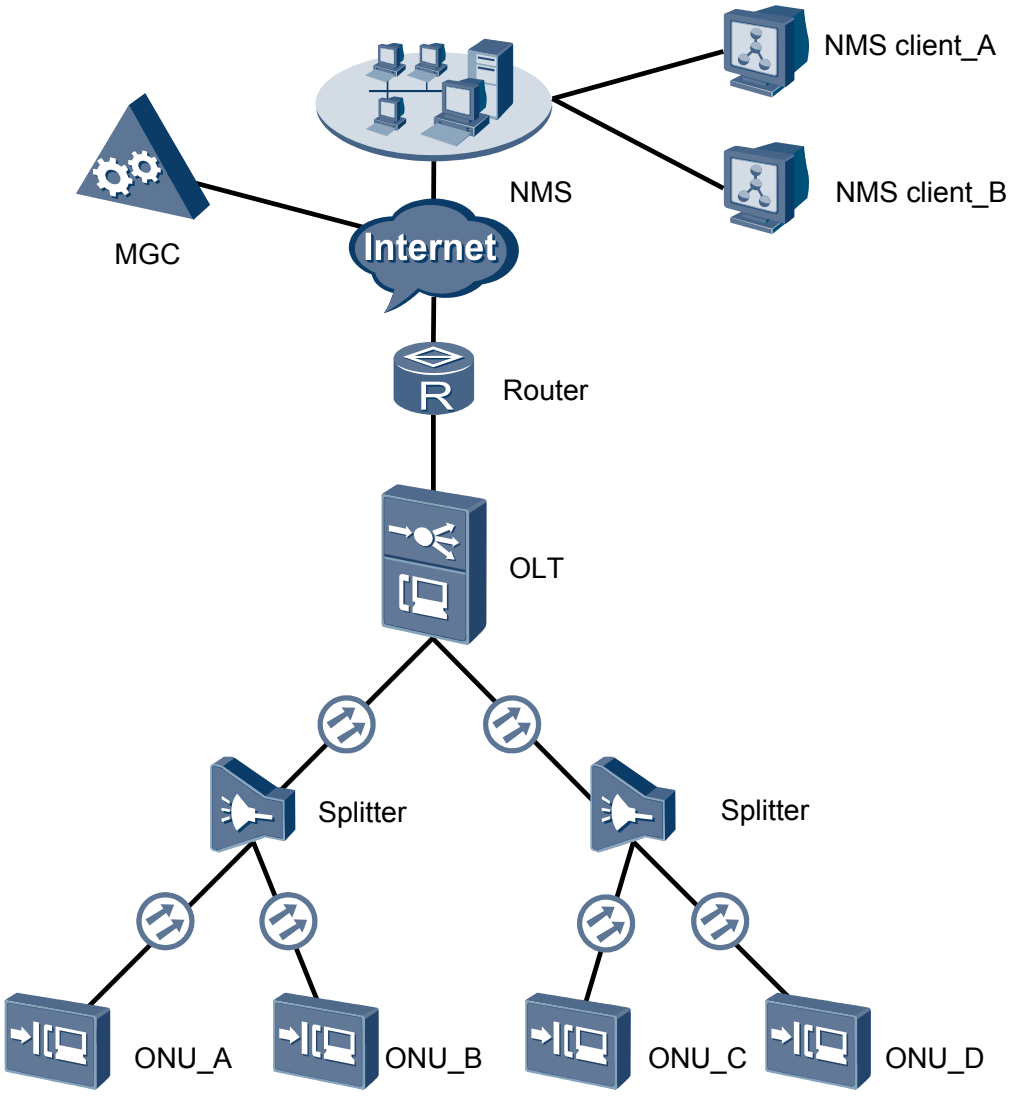
Context

When the ONU adopts the GPON upstream transmission, the SN is used for authentication.

Scenario with the NMS

Figure 1-1 shows an example network of device deployment in the scenario with the NMS.

Figure 1-1 Example network of device deployment in the scenario with the NMS



The procedure for deploying network devices in the scenario with the NMS is as follows:

1. According to the user's FTTx data plan, the commissioning engineer prepares the network planning sheet and obtains the resource deployment sheet.
2. The commissioning engineer imports the resource deployment sheet through the NMS to implement the predeployment for the ONU.
3. The hardware installation engineer draws the ONUs and sends them to the destination sites, and then performs hardware installation, wiring, and power-on operations at the destination sites.
4. The hardware installation engineer checks the running status of the ONU that is installed and powered on.

   There are two LEDs, namely Link and Auth, on the ONU.

   - If the Link LED is on, it indicates that the upstream optical path is through.
   - If the Auth LED is blinking, it indicates that the ONU is registering.

- If the Auth LED is always on, it indicates that the ONU registers successfully.

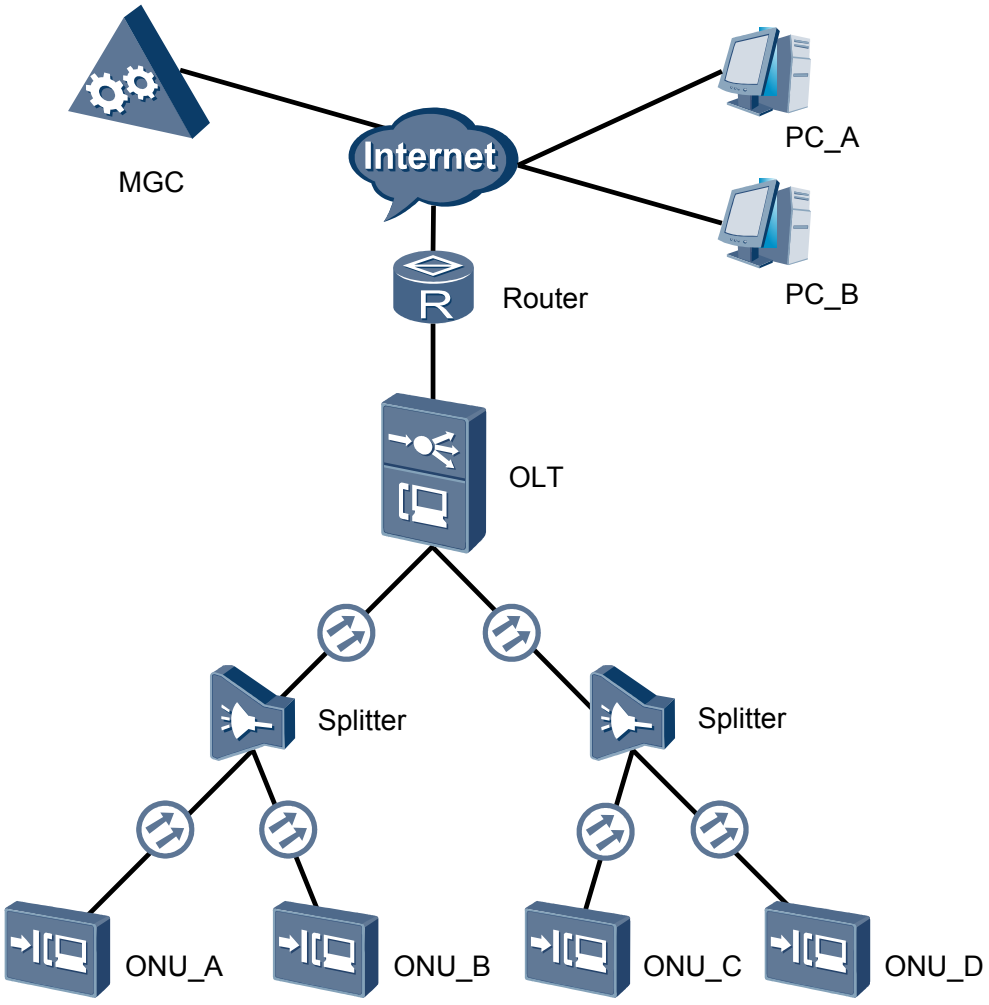
5. After confirming that the ONU works in the normal state (the Link LED is on and the Auth LED blinks), the hardware installation engineer records the ONU SN and reports the SN to the commissioning engineer.
6. The commissioning engineer maps the ONU SN, the management IP address of the ONU, and the physical position of the ONU, and binds the IP address and the SN of the ONU through the NMS.
7. After being powered on, the ONU registers with the OLT automatically. Then, the OLT sends the management channel parameters of the ONU (management VLAN, IP address, and SNMP parameters) to the ONU and also sends the trap message to the NMS for informing the NMS that an ONU goes online.
8. The commissioning engineer receives the trap indicating that the ONU goes online reported by the OLT on the NMS.

   After the trap indicating that the ONU goes online is received on the NMS, the ONU management channel is enabled successfully. Then, you can remotely configure services for the ONU through the NMS.

Scenario Without the NMS

Figure 1-2 shows an example network of device deployment in the scenario without the NMS.

Figure 1-2 Example network of device deployment in the scenario without the NMS



The procedure for deploying network devices in the scenario without the NMS is as follows:

1. According to the user's FTTx service plan and the corresponding OLT version, the commissioning engineer performs the data plan for the OLT and ONU.
2. The hardware installation engineer draws the ONUs and sends them to the destination sites, and then performs hardware installation, wiring, and power-on operations at the destination sites.
3. The hardware installation engineer checks the running status of the ONU that is installed and powered on.

   There are two LEDs, namely Link and Auth, on the ONU.

   - If the Link LED is on, it indicates that the upstream optical path is through.
   - If the Auth LED is blinking, it indicates that the ONU is registering.
   - If the Auth LED is always on, it indicates that the ONU registers successfully.
4. After confirming that the ONU works in the normal state (the Link LED is on and the Auth LED blinks), the hardware installation engineer records the ONU SN and reports the SN to the commissioning engineer.
5. According to the data plan of the OLT and ONU, the commissioning engineer configures data on the OLT.
6. The commissioning engineer enables the auto-discovery function of the OLT for the ONU.
7. The commissioning engineer adds the ONU to the OLT according to the data plan of the OLT and ONU and the SN reported by the hardware installation engineer.
8. The commissioning engineer configures the management IP address of the ONU through the OLT.
9. The commissioning engineer telnets to the ONU according to the management IP address of the ONU to configure the services for the ONU.

2 Checking Before the Configuration

About This Chapter

Before the service configuration, you need to check the software version and board status of the MA5616 to ensure that the service runs normally after the configuration.

2.1 Checking the Software Version

This topic describes how to check whether the current software version meets the deployment requirement.

Prerequisites

You must be logged in to the MA5616. For details about how to log in to the device, see **3.1 Configuring the Maintenance Terminal**.

Procedure

- The procedure of checking the software version through the MA5616 is as follows:
  1. In the user mode, run the **display language** command to check whether the multi-language information supported by the system and the system version meet the deployment requirement.
  2. In the user mode, run the **display version** command to check whether the versions of the host software and patch that is running in the system meet the deployment requirement.
- The procedure of checking the software version through the iManager U2000 is as follows:
  1. In the **Workbench** window, double-click  . The **Main Topology** window is displayed. Click  .
  2. In the **Search** dialog box, select **NE** from the **Search Type** drop-down list and enter the description of the MA5616 to be queried. Then, click **Search**.
  3. In the search result, select the desired MA5616. Click **Locate** and select **Locate to NE Panel** from the list. In the **Device Detailed Info** tab page, verify that the device type and activated patch meet the deployment requirement.

----End

Result

- The versions of the host software and patch meet the deployment requirement.
- If the versions do not meet the deployment requirement, contact Huawei technical support center to upgrade the host software if necessary. For details about the upgrade, see the *MA5616 Upgrade guide*.

2.2 Checking the Board Status

This topic describes how to check whether the inserted board is the same as the board specified in the data plan, and whether the boards are in the normal state.

Procedure

- The procedure of checking the board status through the MA5616 is as follows:
  1. Run the **display board** command to check whether the board information (including the board types and the slots housing the boards) meets the data plan and whether the boards are in the normal state.

- If all the required boards are inserted correctly and all the boards are in the normal state, the operation ends.
- If a required board is not inserted in the device, insert the board and run the **board confirm** command to confirm the board in the auto-find state. Then, run the **display board** command to query the status of all the boards.

- The procedure of checking the board status through the iManager U2000 is as follows:

  1. In the **Workbench** window, double-click  . The **Main Topology** window is displayed. Click  .
  2. In the **Search** dialog box, select **Board** from the **Search Type** drop-down list and enter the description of the board to be queried. Then, click **Search**.
  3. In the search result, select the desired board of the MA5616. Click **Locate to Board**. Then, verity that the board type and slot meet the requirements of the data planning and verify the board status.

----End

Result

- The status of all the boards is "Normal" in the result of the query on the MA5616.
- All the boards on the MA5616 are in the normal state, represented by  , in the result of the query through the iManager U2000.

3 Basic Configuration

About This Chapter

This topic describes how to perform the basic configuration, including common configuration, public configuration, and service preconfiguration. These types of configurations do not have definite logic relations between each other. Therefore, you can perform the configuration based on actual requirements.

Configuring the xDSL profile is a prerequisite for configuring an xDSL access service. This topic describes how to configure an ADSL2+ profile, an SHDSL profile, and a VDSL2 profile.

3.8 Configuring the System Clock
This topic describes how to configure the system clock to restrict the clock frequency and phase of each node on a network within the preset tolerance scope. This prevents the deterioration of the TDM service quality caused by inaccurate signal timing at both the transmit and receive ends in the digital transmission system.

3.9 Configuring the System Time
This topic describes the feature of the NTP protocol and how to configure NTP time on the MA5616.

3.10 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.

3.11 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.

3.12 Configuring AAA
This topic describes how to configure the AAA on the MA5616, including configuring the MA5616 as the local and remote AAA servers.

3.13 Configuring the ACL for Packet Filtering
This topic describes the type, rule, and configuration of the ACL on the MA5616.

3.14 Configuring QoS
This topic describes how to configure quality of service (QoS) on the MA5616 to provide end-to-end quality assurance for user services.

3.15 Configuring Environment Monitoring
This topic provides concepts associated with environment monitoring and describes how to configure environment monitoring on the MA5616.

3.1 Configuring the Maintenance Terminal

This topic describes three modes of managing the MA5616 from the maintenance terminal.

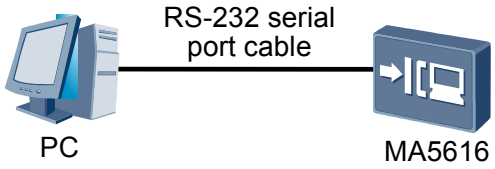
3.1.1 Configuring Management Through a Local Serial Port

This topic describes how to connect the maintenance terminal to the MA5616 through a local serial port, log in to the MA5616, and then manage the MA5616 from the maintenance terminal.

Networking

Figure 3-1 shows an example network for configuring management through a local serial port.

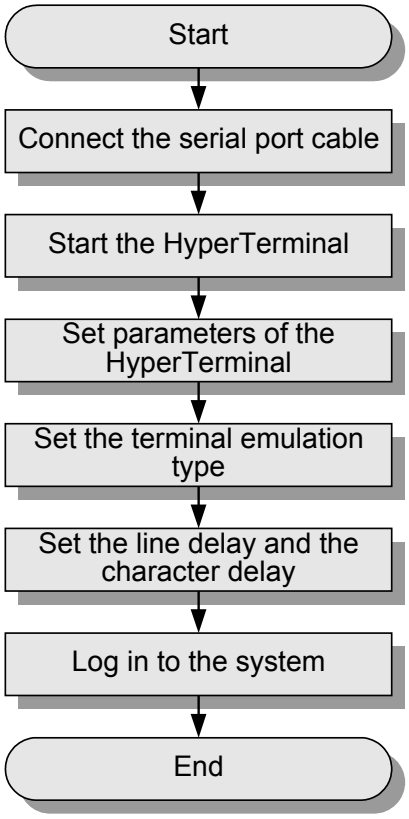
Figure 3-1 Example network for configuring management through a local serial port



Configuration Flowchart

Figure 3-2 shows the flowchart for configuring management through a local serial port.

Figure 3-2 Flowchart for configuring management through a local serial port



Procedure

Step 1 Connect the serial port cable.

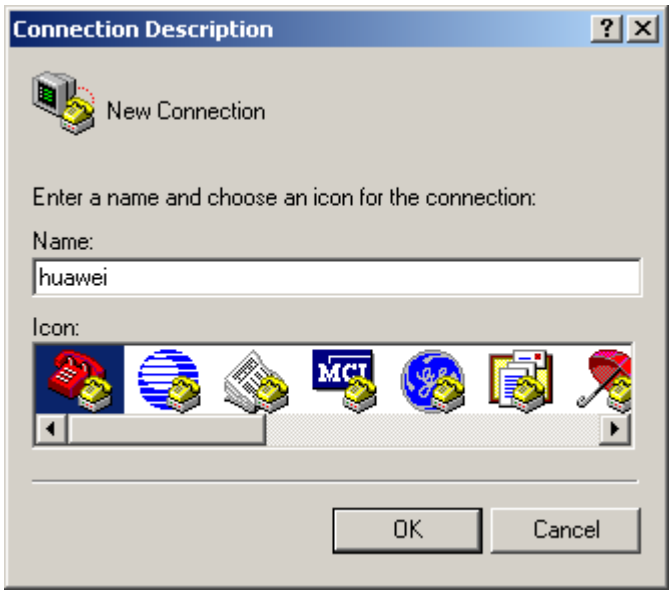
Use a standard RS-232 serial port cable to connect the serial port of the PC to the CONSOLE port (maintenance serial port) on the control board of the MA5616, as shown in **Figure 3-1**.

Step 2 Start the HyperTerminal.

1. Set up a connection.

   Choose **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal** on the PC. The **Connection Description** dialog box is displayed. Enter the connection name, as shown in **Figure 3-3**, and click **OK**.

Figure 3-3 Setting up a connection



2. Set the serial port.

   On the PC that is connected to the MA5616, select the number of the standard character terminal or PC terminal serial port. You can select "COM1" or "COM2". In this example, "COM2" is selected, as shown in **Figure 3-4**. Click **OK**.

Figure 3-4 Selecting the serial port ID

Step 3 Set the communication parameters of the HyperTerminal.

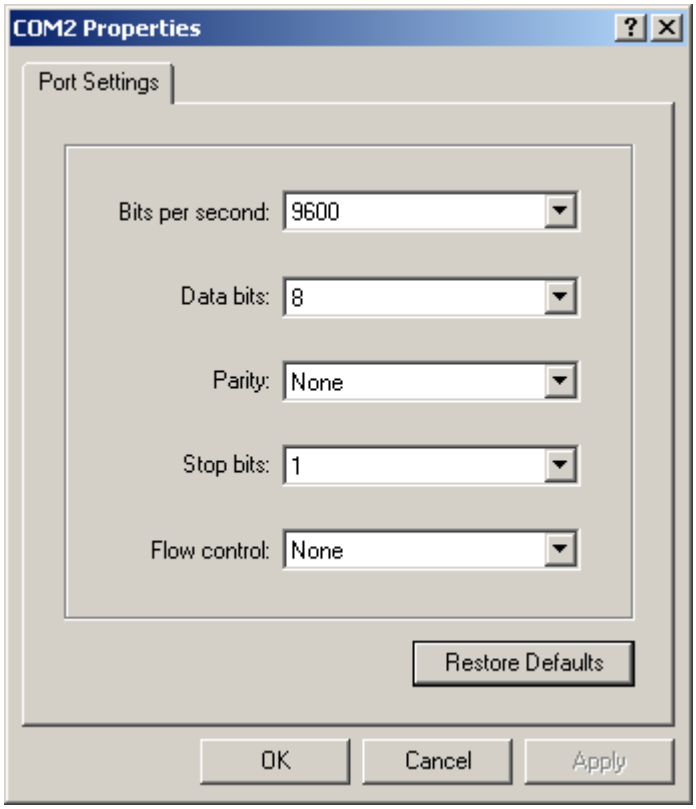
Set the parameters in the **COM2 Properties** dialog box, as shown in **Figure 3-5**. The parameters are as follows:

- Baud rate: 9600 bit/s
- Data bit: 8
- Parity: None
- Stop bit: 1
- Flow control: None

NOTE

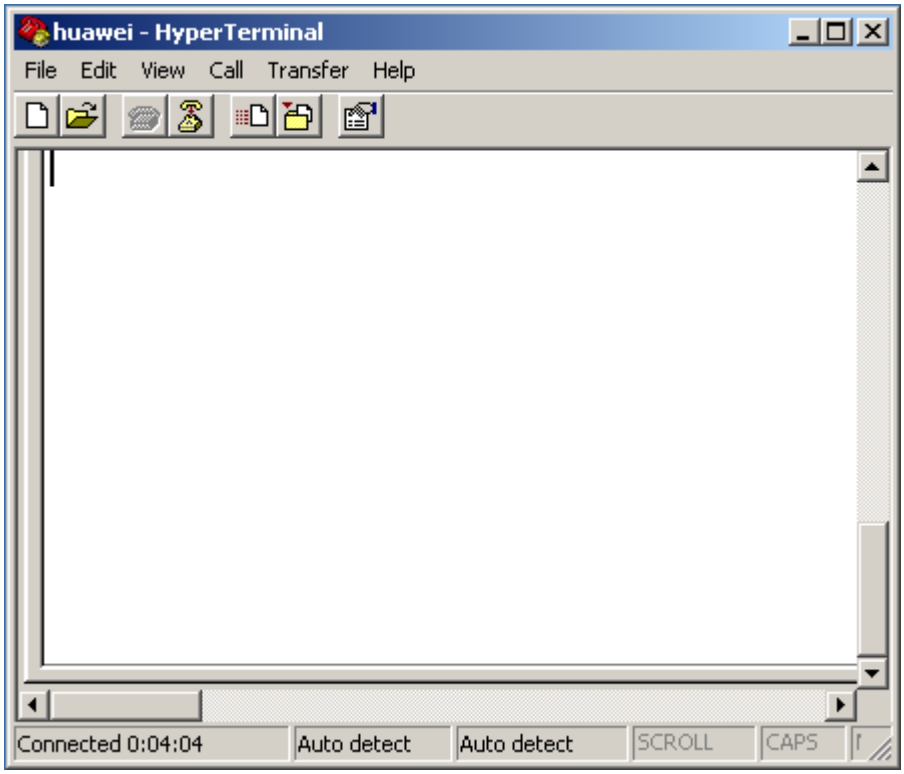
- The baud rate of the HyperTerminal must be the same as that of the serial port on the MA5616. By default, the baud rate of the serial port on the MA5616 is 9600 bit/s.
- There may be illegible characters in the displayed input information after you log in to the system. This is because the baud rates between the HyperTerminal and the MA5616 are not the same. In this case, set a different baud rate 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.

Figure 3-5 Setting the parameters of the HyperTerminal



Click **OK**, and the HyperTerminal interface is displayed, as shown in **Figure 3-6**.

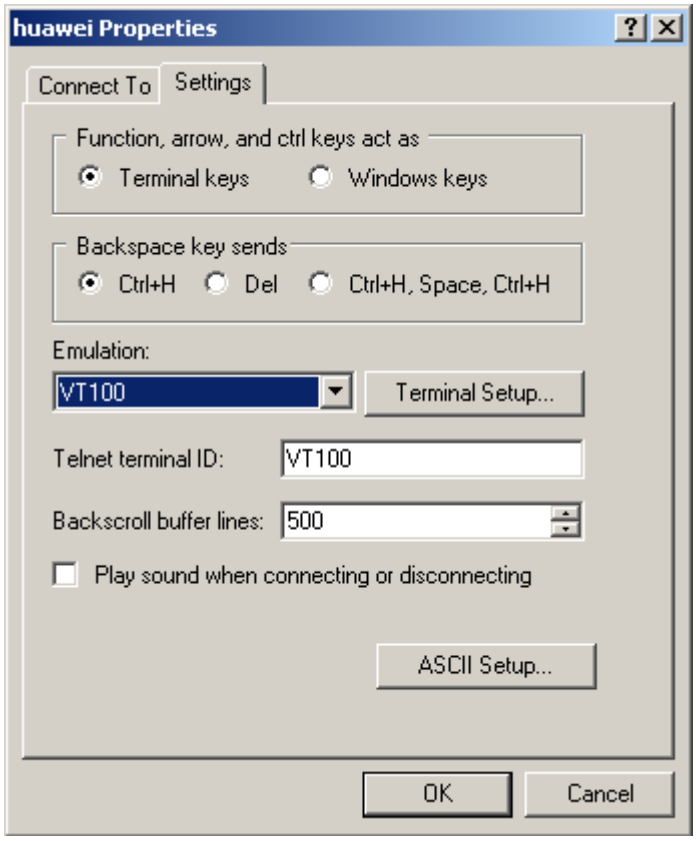
Figure 3-6 HyperTerminal interface



Step 4 Set the terminal emulation type.

Choose **File** > **Properties** on the HyperTerminal interface. In the dialog box that is displayed, click the **Settings** tab, and set the terminal emulation type to **VT100** or **Auto detect**. Use default values for other parameters. Then, click **OK**, as shown in **Figure 3-7**.

Figure 3-7 Setting the terminal emulation type



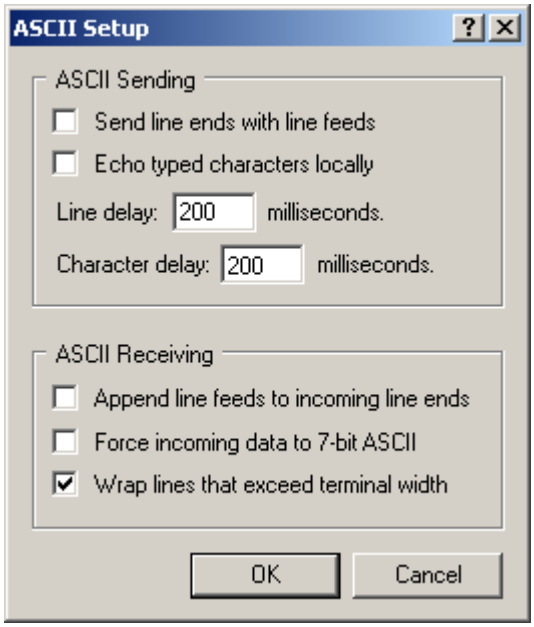
Step 5 Set the line delay and the character delay.

Click **ASCII Setup**. In the dialog box that is displayed, set **Line delay** to 200 ms and **Character delay** to 200 ms, and use default values for other parameters. Click **OK**, as shown in **Figure 3-8**.

NOTE

- By default, **Line delay** is 0, and **Character delay** is 0.
- 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.

Figure 3-8 Setting the line delay and the character delay



----End

Result

On the HyperTerminal interface, press **Enter**, and the system prompts you to enter the user name. Enter the user name and the password for user registration (by default, the super user name is **root** and the password is **mduadmin**), and wait until the CLI prompt character is displayed. For instructions on CLI, see CLI Operation Characteristics.

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

3.1.2 Configuring Outband Management

This topic describes how to connect the MA5616 to the maintenance terminal through an outband management port, log in to the MA5616, and then manage the MA5616.

Prerequisites

- You must log in to the system through a local serial port. For the configuration process, see **3.1.1 Configuring Management Through a Local Serial Port**.
- The IP address of the maintenance terminal must be properly configured.

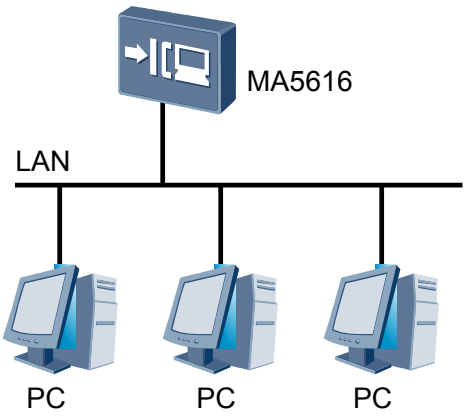
NOTE

In the following operations, the configurations of the MA5616 must be performed through a local serial port.

Networking - LAN

Figure 3-9 shows an example network for configuring outband management over a LAN in the telnet mode.

Figure 3-9 Example network for configuring outband management over a LAN in the telnet mode



In this example network, the IP address of the maintenance Ethernet port of the MA5616 and the IP address of the maintenance terminal are in the same network segment. You can also manage the MA5616 through an outband channel by directly connecting the maintenance Ethernet port of the maintenance terminal to the maintenance Ethernet port on the control board of the MA5616.

Data Plan - LAN

Table 3-1 provides the data plan for configuring outband management over a LAN in the telnet mode.

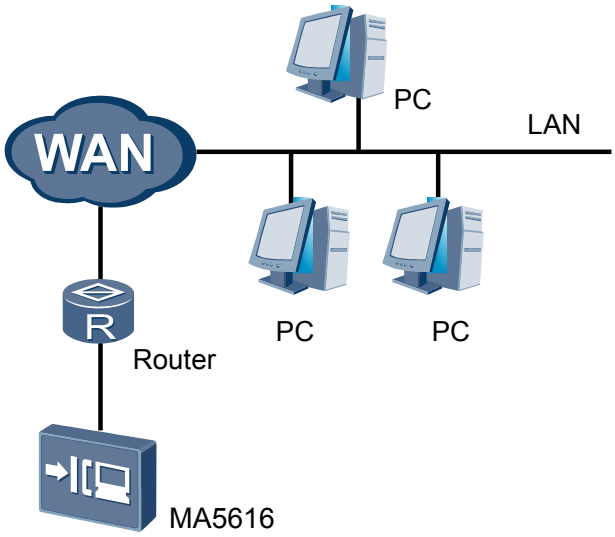
Table 3-1 Data plan for configuring outband management over a LAN in the telnet mode

Item	Data
Maintenance Ethernet port of the MA5616	IP address: 10.10.20.2/24
Ethernet port of the maintenance terminal	IP address: 10.10.20.3/24

Networking - WAN

Figure 3-10 shows an example network for configuring outband management over a WAN in the telnet mode.

Figure 3-10 Example network for configuring outband management over a WAN in the telnet mode



In this example network, the MA5616 is connected to the WAN through the maintenance Ethernet port. You can manage the MA5616 remotely from the maintenance terminal.

Data Plan - WAN

Table 3-2 provides the data plan for configuring outband management over a WAN in the telnet mode.

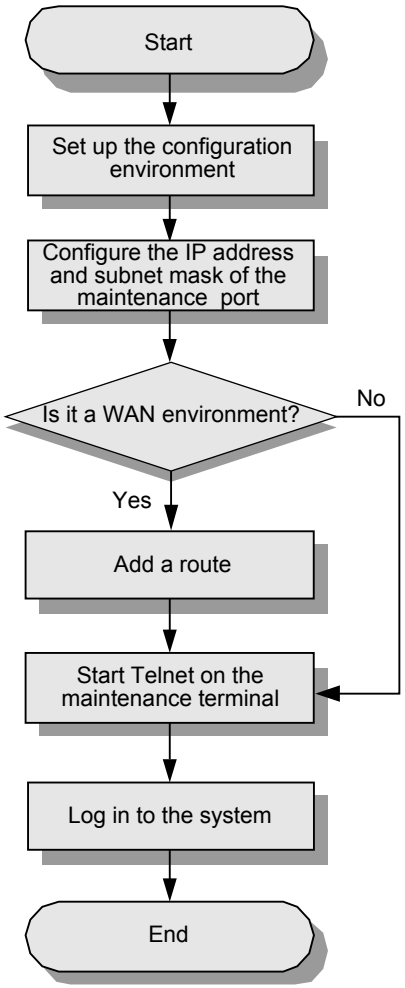
Table 3-2 Data plan for configuring outband management over a WAN in the telnet mode

Item	Data
Maintenance Ethernet port of the MA5616	IP address: 10.10.20.2/24
Ethernet port of the maintenance terminal	IP address: 10.10.21.3/24
Port of the router connected to the MA5616	IP address: 10.10.20.254/24

Configuration Flowchart

Figure 3-11 shows the flowchart for outband management in the telnet mode.

Figure 3-11 Flowchart for outband management in the telnet mode



Procedure

Step 1 Set up the configuration environment.

Figure 3-9 or **Figure 3-10** shows how to set up the configuration environment according to the actual requirements and conditions.

Step 2 In the meth mode, run the **ip address** command to configure the IP address and subnet mask of the maintenance Ethernet port of the MA5616.

NOTE

The default IP address of the maintenance Ethernet port is 10.11.104.2, and the subnet mask is 255.255.255.0. You can configure the IP address of the maintenance Ethernet port based on the actual network planning.

```
huawei(config)#interface meth 0
huawei(config-if-meth0)#ip address 10.10.20.2 24
```

Step 3 Add a route.

- If the configuration environment is set up as shown in **Figure 3-9**, you need not add a route.

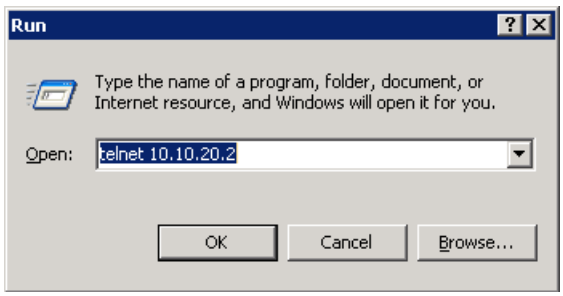
- If the remote WAN management environment is set up as shown in **Figure 3-10**, run the **ip route-static** command to add a route to the next hop.

```
huawei(config-if-meth0)#quit
huawei(config)#ip route-static 10.10.21.0 24 10.10.20.254
```

Step 4 Start Telnet on the maintenance terminal.

Choose **Start** > **Run** on the maintenance terminal. In the **Open** address bar, enter **telnet 10.10.20.2** (10.10.20.2 is the IP address of the maintenance Ethernet port of the MA5616), as shown in **Figure 3-12** (considering the Windows OS as an example). Click **OK**, and the telnet interface is displayed.

Figure 3-12 Starting Telnet



Step 5 Log in to the MA5616.

On the telnet interface, enter the user name and the password. By default, the super user name is **root** and the password is **mduadmin**. When the login is successful, the system displays the following information:

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


  Huawei Integrated Access Software (MA5616).

  Copyright(C) Huawei Technologies Co., Ltd. 2002-2010. All rights reserved.
```

----End

Result

After logging in to the MA5616, you can manage the MA5616. For instructions on CLI, see CLI Operation Characteristics.

3.1.3 Configuring Inband Management (GPON Upstream)

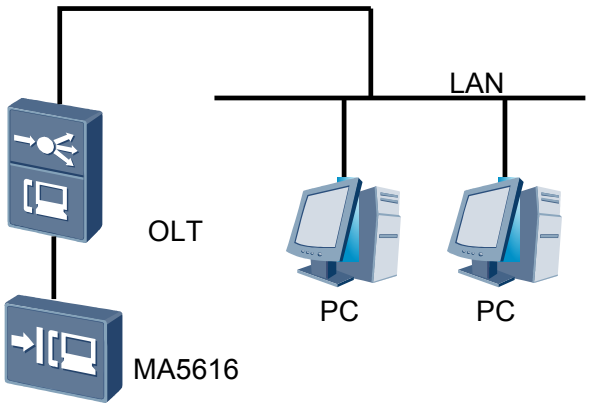
This topic describes how to log in to the MA5616 through an OLT from the maintenance terminal to manage the MA5616.

Prerequisites

- The physical connection between the MA5616 and the OLT must be normal.
- The IP address of the maintenance terminal must be properly configured.

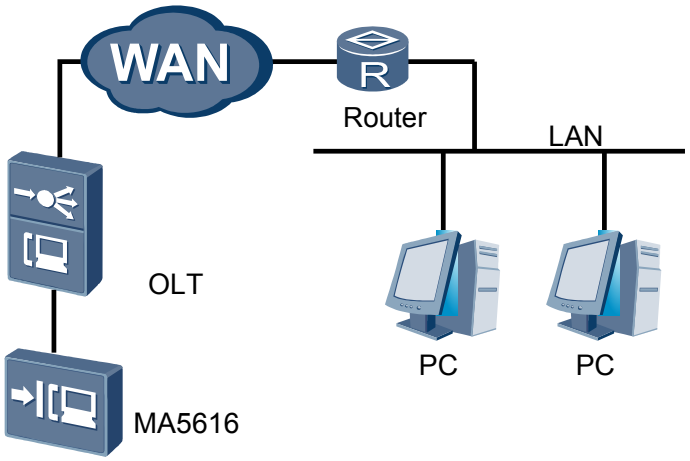
Networking - LAN

Figure 3-13 Example network for configuring inband management over a LAN in the GPON upstream mode



Networking - WAN

Figure 3-14 Example network for configuring inband management over a WAN in the GPON upstream mode



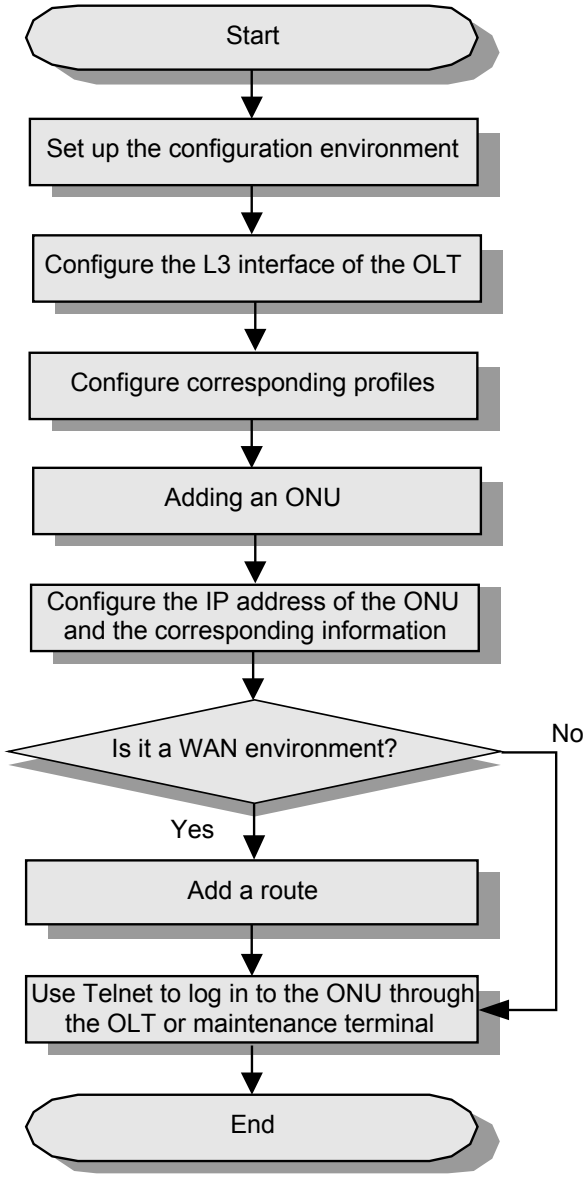
Configuration Flowchart

Figure 3-15 shows the flowchart for managing the MA5616 through an inband channel in the GPON upstream mode.

NOTE

In the GPON upstream mode, the MA5616 and the OLT are interconnected to implement inband management. All required configurations are performed on the OLT. This document provides only the flowchart for configuring the OLT. For the detailed configuration process, see the configuration guide corresponding to the OLT.

Figure 3-15 Flowchart for configuring inband management in the GPON upstream mode



Result

After logging in to the MA5616 through the OLT or maintenance terminal, you can configure the MA5616. For instructions on CLI, see CLI Operation Characteristics.

3.1.4 Configuring Inband Management (GE Upstream)

This topic describes how to use Telnet to log in to the MA5616 through an upstream port (inband management port) of the MA5616 for inband management.

Prerequisites

- You must be logged in to the system through a local serial port. For the configuration process, see **3.1.1 Configuring Management Through a Local Serial Port**.
- The IP address of the maintenance terminal must be properly configured.

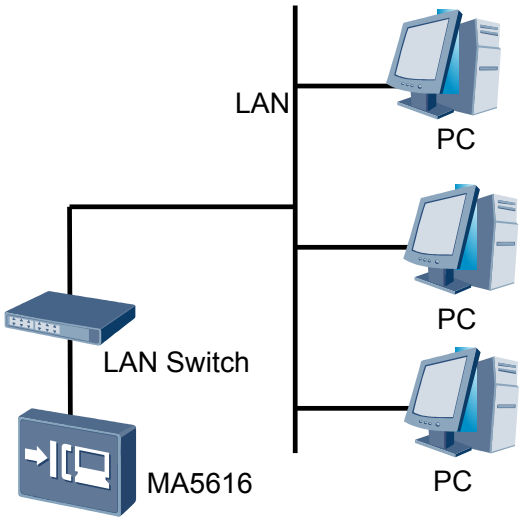
NOTE

In the following operations, the configurations of the MA5616 must be performed through a local serial port.

Networking - LAN

Figure 3-16 shows an example network for configuring inband management over a LAN in the telnet mode.

Figure 3-16 Example network for configuring inband management over a LAN in the telnet mode



Data Plan - LAN

Table 3-3 provides the data plan for configuring inband management over a LAN in the telnet mode.

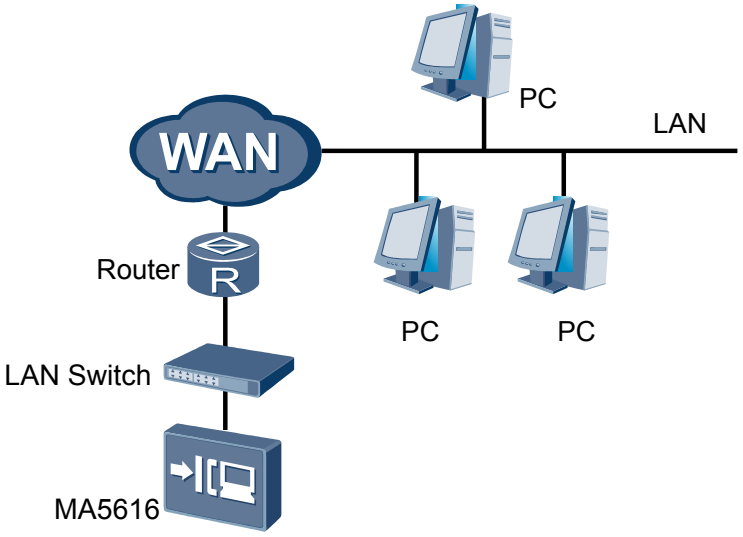
Table 3-3 Data plan for configuring inband management over a LAN in the telnet mode

Item	Data
Upstream port of the MA5616	● VLAN ID: 30 ● Port ID: 0/0/0 ● IP address: 10.10.20.2/24
Ethernet port of the maintenance terminal	IP address: 10.10.20.3/24

Networking - WAN

Figure 3-17 shows an example network for configuring inband management over a WAN in the telnet mode.

Figure 3-17 Example network for configuring inband management over a WAN in the telnet mode



Data Plan - WAN

Table 3-4 provides the data plan for configuring inband management over a WAN in the telnet mode.

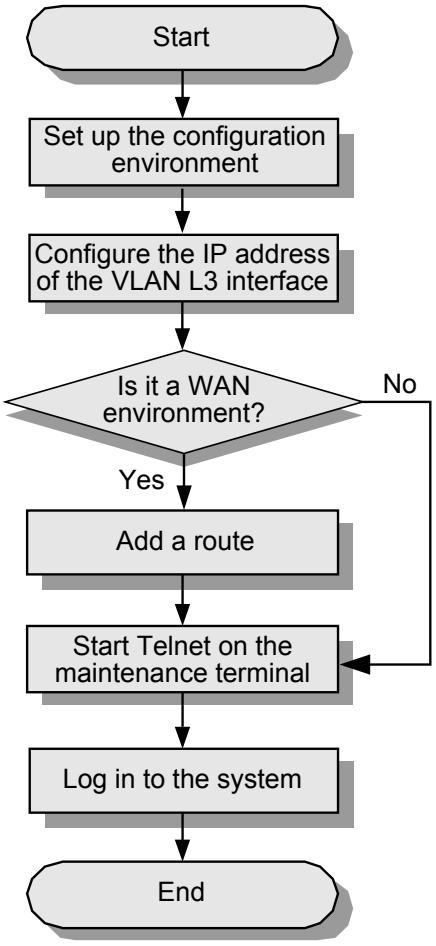
Table 3-4 Data plan for configuring inband management over a WAN in the telnet mode

Item	Data
Upstream port of the MA5616	● VLAN ID: 30 ● Port ID: 0/0/0 ● IP address: 10.10.20.2/24
Ethernet port of the maintenance terminal	IP address: 10.10.21.3/24
Port of the LAN switch connected to the router	IP address: 10.10.20.3/24

Configuration Flowchart

Figure 3-18 shows the flowchart for configuring inband management in the telnet mode.

Figure 3-18 Flowchart for configuring inband management in the telnet mode



Procedure

Step 1 Set up the configuration environment.

Figure 3-16 or **Figure 3-17** shows how to set up the configuration environment according to the actual requirements and conditions.

Step 2 (Optional) Configuring the attributes of the uplink port.

Generally, the uplink port on the 0/0/0 does not need to be set in optical-electrical mode. If the uplink link fails, perform the following steps:

1. Run the **combo-mode** command to switch the Ethernet port mode.
2. Run the **auto-neg 0 disable** command to disable the autonegotiation mode of the port.
3. Run the **speed** command to set the rate of the Ethernet port at the local end so that it is the same as that at the peer end.

For details about how to set the uplink port attributes, see **3.3.1 Configuring an Uplink Ethernet Port**.

Step 3 Configure the IP address of the VLAN L3 interface.

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

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

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

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

3. In the VLANIF mode, run the **ip address** command to configure the IP address and subnet mask of the VLAN L3 interface.

   ```
   huawei(config)#interface vlanif 30
   huawei(config-if-vlanif30)#ip address 10.10.20.2 255.255.255.0
   ```

Step 4 Add a route.

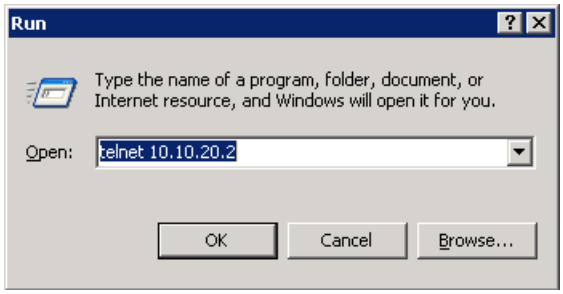
- If the configuration environment is set up as shown in **Figure 3-16**, you need not add a route.
- If the remote WAN management environment is set up as shown in **Figure 3-17**, run the **ip route-static** command to add a route to the next hop.

```
huawei(config-if-vlanif30)#quit
huawei(config)#ip route-static 10.10.21.0 24 10.10.20.3
```

Step 5 Start Telnet.

Choose **Start** > **Run** on the maintenance terminal. In the **Open** address bar, enter **telnet 10.10.20.2** (10.10.20.2 is the IP address of the VLAN L3 interface of the MA5616), as shown in **Figure 3-19** (considering the Windows OS as an example). Click **OK**, and the telnet interface is displayed.

Figure 3-19 Starting Telnet



Step 6 Log in to the MA5616.

On the telnet interface, enter the user name and the password. By default, the super user name is **root** and the password is **mduadmin**. When the login is successful, the system displays the following information:

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


  Huawei Integrated Access Software (MA5616).

  Copyright(C) Huawei Technologies Co., Ltd. 2002-2010. All rights reserved.
```

----End

Result

After logging in to the MA5616, you can manage the MA5616. For instructions on CLI, see CLI Operation Characteristics.

3.2 Configuring the U2000

The MA5616 can be interconnected with Huawei iManager U2000 (hereinafter referred to as U2000). Hence, the administrator can maintain and manage the device through the U2000. The MA5616 can be interconnected with the U2000 in inband or outband networking mode. The following part describes how to configure the inband networking and outband networking based on SNMP V1, SNMP V2c, and SNMP V3 respectively.

3.2.1 Configuring the U2000 (Based on SNMPv1)

When SNMPv1 is used, the MA5616 can be interconnected with the U2000 in inband or outband networking mode.

Prerequisites

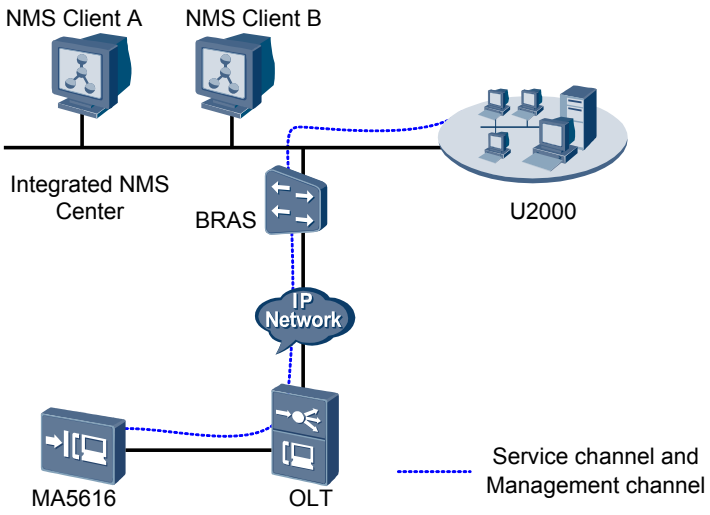
- If the device is interconnected with the NMS in outband networking mode, the communication port (maintenance network port) must be configured. For detailed procedure, see **3.1.2 Configuring Outband Management**.
- If the device is interconnected with the NMS through the PON upstream port in inband networking mode, the communication port (PON upstream port) must be configured. For detailed procedure, see **3.1.3 Configuring Inband Management (GPON Upstream)**.
- If the device is interconnected with the NMS through the GE upstream port in inband networking mode, the communication port (GE upstream port) must be configured. For detailed procedure, see **3.1.4 Configuring Inband Management (GE Upstream)**.

Networking - Inband Networking Mode

As shown in **Figure 3-20**, the SNMP protocol is transmitted through the service channel. Service packets and management packets are transmitted through the same channel. The inband NMS management is implemented through the upstream port.

- The MA5616 supports the GPON/GE upstream port.
- A static route is used between the MA5616 and the U2000.

Figure 3-20 Inband networking

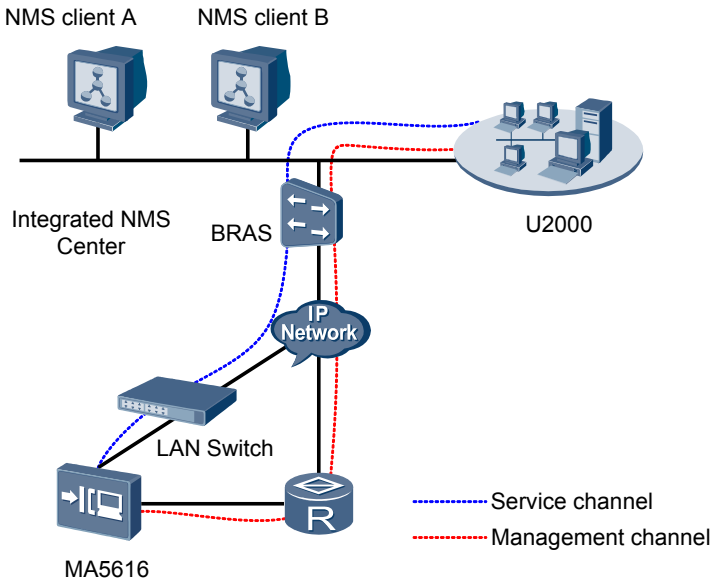


Networking - Outband Networking Mode

As shown in **Figure 3-21**, the SNMP protocol is transmitted through the management channel. Service packets and management packets are transmitted through different channels. The outband NMS management is implemented through the maintenance network port.

- The MA5616 supports the local maintenance network port ETH.
- A static route is used between the MA5616 and the U2000.

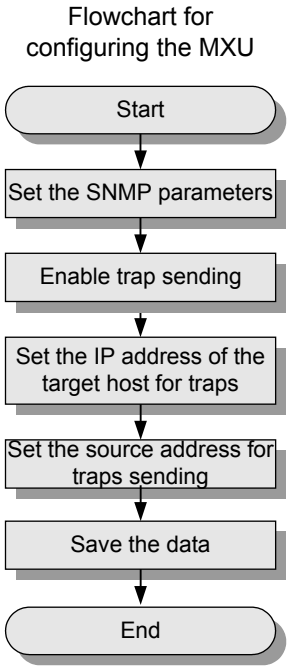
Figure 3-21 Outband networking



Configuration Flowchart

Figure 3-22 shows the flowchart for configuring the NMS.

Figure 3-22 Flowchart for configuring the NMS



Procedure

- Configuration procedure on the device
  1. Configure the SNMP parameters.
     a. Configure the community names and the access rights.

        Run the **snmp-agent community** command to configure the community names and the access rights.

        NOTE

        The read community name is **public**. The write community name is **private**.

        The read community name and the write community name on the device must be the same as those configured on the U2000.

        ```
        huawei(config)#snmp-agent community read public
        huawei(config)#snmp-agent community write private
        ```

     b. (Optional) Set the information about the administrator.

        Run the **snmp-agent sys-info** command to set the contact of the SNMP Agent administrator and the physical position of the device.

        Contact of the administrator: HW-075528780808. Physical position of the device: Shenzhen_China.

        ```
        huawei(config)#snmp-agent sys-info contact HW-075528780808
        huawei(config)#snmp-agent sys-info location Shenzhen_China
        ```

     c. Set the SNMP version.

        Run the **snmp-agent sys-info** command to set the required SNMP version.

        ```
        huawei(config)#snmp-agent sys-info version v1
        ```

        NOTE

        The SNMP version on the device must be the same as that configured on the U2000.

2. Enable the function of sending traps.

   Run the **snmp-agent trap enable** command on the device for sending traps to the NMS.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

3. Configure the IP address of the target host of the traps.

   Run the **snmp-agent target-host** command to configure the IP address of the target host of the traps.

   The host name is huawei, the IP address of the host is 10.10.1.10/24 (that is, the IP address of the U2000), the name of the target host is ABC, the SNMP version is V1, and the security name is private (that 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
   ```

4. Configure the source IP address of the traps.

   Run the **snmp-agent trap source** command to configure the source IP address of the traps.

   - In inband networking mode, the IP address of the upstream port is used as the source IP address of the traps.
   - In outband networking mode, the IP address of the maintenance network port is used as the source IP address of the traps.

   NOTE

   This document considers the outband networking mode as an example.

   ```
   huawei(config)#snmp-agent trap source meth 0
   ```

5. Save the data.

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

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

- Configuration procedure on the NMS

  NOTE

  In inband networking mode, you only need to perform the configuration on the MA5616. This step can be omitted because the MA5616 can be automatically discovered through the OLT.

  In outband networking mode, you need to follow this step to perform the configuration on the NMS.

  1. Add a route from the NMS to the device.

     Configure the IP address of the gateway from the NMS server to network segment 10.50.1.0/24 to 10.10.1.1.

     - In the Solaris operating system (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 NMS port and the IP address of the U2000 are in the same network segment, you need not configure the route.

2. Log in to the U2000.
3. Configure the SNMP parameters.

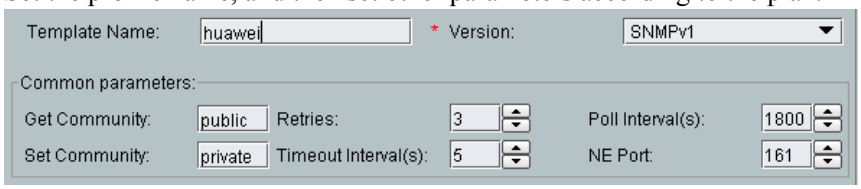
NOTE

A default SNMP profile exists in the system and is used in this example. If you need to configure a new profile, do as follows:

a. Choose **Administration** > **NE Communicate** > **Default Access Protocol Parameters** from the main menu.

b. In **Default Access Protocol Parameters**, click the **SNMPv1 Parameters** tab, and then click **Add**.

c. Set the profile name, and then set other parameters according to the plan.

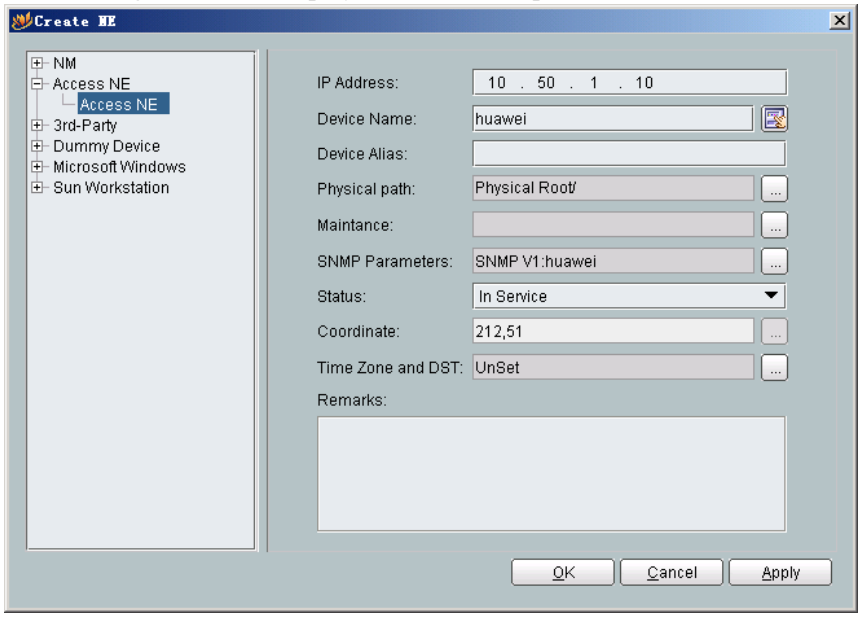


d. Click **OK**. Then, the SNMP parameters are configured.

4. Add a device.

a. Right-click in the main topology, and then choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, set relevant parameters.



NOTE

- The IP address is the management IP address of the MA5616.
- Select the SNMP parameters based on the selected SNMP protocol. This section considers the SNMP V1 default profile as an example. You can select the profile according to the plan.

c. Click **OK**. Several seconds to some 10 minutes are required for uploading the device data. After reading the related data, the system automatically updates the device icon.

----End

Result

You can maintain and manage the MA5616 through the U2000.

Configuration File

The following part provides the script for configuring the outband NMS (on the device).

```
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 part provides the script for configuring the inband NMS (on the device). The management VLAN ID of the upstream port is 30.

```
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 30
save
```

3.2.2 Configuring the U2000 (Based on SNMPv2c)

When SNMPv2c is used, the MA5616 can be interconnected with the U2000 in inband or outband networking mode.

Prerequisites

- If the device is interconnected with the NMS in outband networking mode, the communication port (maintenance network port) must be configured. For detailed procedure, see **3.1.2 Configuring Outband Management**.
- If the device is interconnected with the NMS through the PON upstream port in inband networking mode, the communication port (PON upstream port) must be configured. For detailed procedure, see **3.1.3 Configuring Inband Management (GPON Upstream)**.

- If the device is interconnected with the NMS through the GE upstream port in inband networking mode, the communication port (GE upstream port) must be configured. For detailed procedure, see **3.1.4 Configuring Inband Management (GE Upstream)**.

Networking - Inband Networking Mode

As shown in the inband networking in **3.2.1 Configuring the U2000 (Based on SNMPv1)**, the SNMP protocol is transmitted through the service channel. Service packets and management packets are transmitted through the same channel. The inband NMS management is implemented through the upstream port.

- The MA5616 supports GPON/GE upstream port.
- A static route is used between the MA5616 and the U2000.

Networking - Outband Networking Mode

As shown in the outband networking in **3.2.1 Configuring the U2000 (Based on SNMPv1)**, the SNMP protocol is transmitted through the management channel. Service packets and management packets are transmitted through different channels. The outband NMS management is implemented through the maintenance network port.

- The MA5616 supports the local maintenance network port ETH.
- A static route is used between the MA5616 and the U2000.

Configuration Flowchart

To configure the NMS, see the flowchart for configuring the NMS in **3.2.1 Configuring the U2000 (Based on SNMPv1)**.

Procedure

- Configuration procedure on the device
  1. Configure the SNMP parameters.
     a. Configure the community names and the access rights.

        Run the **snmp-agent community** command to configure the community names and the access rights.

        NOTE

        The read community name is **public**. The write community name is **private**.

        The read community name and the write community name on the device must be the same as those configured on the U2000.

        ```
        huawei(config)#snmp-agent community read public
        huawei(config)#snmp-agent community write private
        ```

     b. (Optional) Set the information about the administrator.

        Run the **snmp-agent sys-info** command to set the contact of the SNMP Agent administrator and the physical position of the device.

        Contact of the administrator: HW-075528780808. Physical position of the device: Shenzhen_China.

        ```
        huawei(config)#snmp-agent sys-info contact HW-075528780808
        huawei(config)#snmp-agent sys-info location Shenzhen_China
        ```

     c. Set the SNMP version.

        Run the **snmp-agent sys-info** command to set the required SNMP version.

```
huawei(config)#snmp-agent sys-info version v2c
```

NOTE

The SNMP version on the device must be the same as that configured on the U2000.

2. Enable the function of sending traps.

   Run the **snmp-agent trap enable** command on the device for sending traps to the NMS.

   ```
   huawei(config)#snmp-agent trap enable standard
   ```

3. Configure the IP address of the target host of the traps.

   Run the command to configure the IP address of the target host of the traps.

   The host name is huawei, the IP address of the host is 10.10.1.10/24 (that is, the IP address of the U2000), the name of the target host is ABC, the SNMP version is V2c, and the security name is private (that 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
   ```

4. Configure the source IP address of the traps.

   Run the **snmp-agent trap source** command to configure the source IP address of the traps.

   - In inband networking mode, the IP address of the upstream port is used as the source IP address of the traps.
   - In outband networking mode, the IP address of the maintenance network port is used as the source IP address of the traps.

   NOTE

   This document considers the outband networking mode as an example.

   ```
   huawei(config)#snmp-agent trap source meth 0
   ```

5. Save the data.

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

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

- Configuration procedure on the NMS

  NOTE

  In inband networking mode, you only need to perform the configuration on the MA5616. This step can be omitted because the MA5616 can be automatically discovered through the OLT.

  In outband networking mode, you need to follow this step to perform the configuration on the NMS.

  1. Add a route from the NMS to the device.

     Configure the IP address of the gateway from the NMS server to network segment 10.50.1.0/24 to 10.10.1.1.

     - In the Solaris operating system (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 NMS port and the IP address of the U2000 are in the same network segment, you need not configure the route.

2. Log in to the U2000.
3. Configure the SNMP parameters.

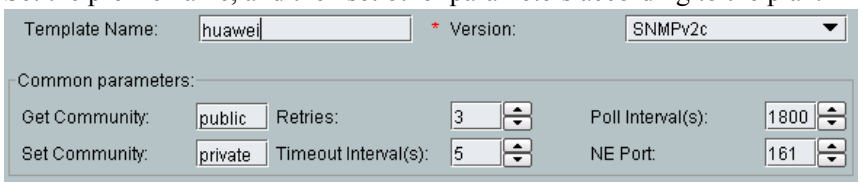
NOTE

A default SNMP profile exists in the system and is considered in this example. If you need to configure a new profile, do as follows:

a. Choose **Administration** > **NE Communicate** > **Default Access Protocol Parameters** from the main menu.

b. In **Default Access Protocol Parameters**, click the **SNMPv2 Parameters** tab, and then click **Add**.

c. Set the profile name, and then set other parameters according to the plan.

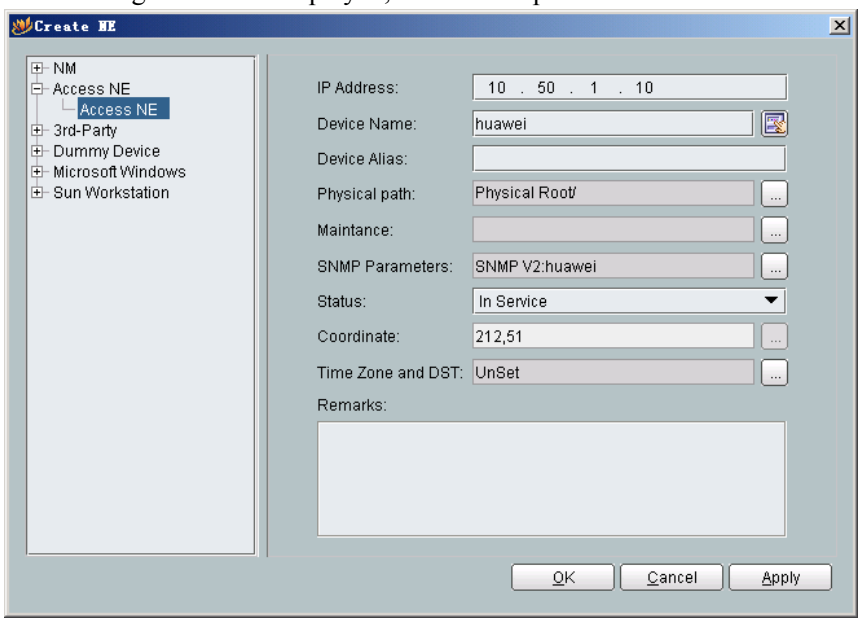


d. Click **OK**. Then, the SNMP parameters are configured.

4. Add a device.

a. Right-click in the main topology, and then choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, set relevant parameters.



NOTE

- The IP address is the management IP address of the MA5616.
- Select the SNMP parameters based on the selected SNMP version. This section considers the SNMP V2c default profile as an example. You can select the profile corresponds to the actual planning.

c. Click **OK**. Several seconds to some 10 minutes are required for uploading the device data. After reading the related data, the system automatically updates the device icon.

----End

Result

You can maintain and manage the MA5616 through the U2000.

Configuration File

The following part provides the script for configuring the outband NMS (on the device).

```
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
```

The following part provides the script for configuring the inband NMS (on the device). The management VLAN ID of the upstream port is 30.

```
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 30
save
```

3.2.3 Configuring the U2000 (Based on SNMPv3)

When SNMPv3 is used, the MA5616 can be interconnected with the U2000 in inband or outband networking mode.

Prerequisites

- If the device is interconnected with the NMS in outband networking mode, the communication port (maintenance network port) must be configured. For detailed procedure, see **3.1.2 Configuring Outband Management**.
- If the device is interconnected with the NMS through the PON upstream port in inband networking mode, the communication port (PON upstream port) must be configured. For detailed procedure, see **3.1.3 Configuring Inband Management (GPON Upstream)**.

- If the device is interconnected with the NMS through the GE upstream port in inband networking mode, the communication port (GE upstream port) must be configured. For detailed procedure, see **3.1.4 Configuring Inband Management (GE Upstream)**.

Networking - Inband Networking Mode

As shown in the inband networking in **3.2.1 Configuring the U2000 (Based on SNMPv1)**, the SNMP protocol is transmitted through the service channel. Service packets and management packets are transmitted through the same channel. The inband NMS management is implemented through the upstream port.

- The MA5616 supports GPON/GE upstream port.
- A static route is used between the MA5616 and the U2000.

Networking - Outband Networking Mode

As shown in the outband networking in **3.2.1 Configuring the U2000 (Based on SNMPv1)**, the SNMP protocol is transmitted through the management channel. Service packets and management packets are transmitted through different channels. The outband NMS management is implemented through the maintenance network port.

- The MA5616 supports the local maintenance network port ETH.
- A static route is used between the MA5616 and the U2000.

Configuration Flowchart

To configure the NMS, see the flowchart for configuring the NMS in **3.2.1 Configuring the U2000 (Based on SNMPv1)**.

Procedure

- Configuration procedure on the device
  1. Configure 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 MD5, 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 md5 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 information about the administrator and the device.

        Run the **snmp-agent sys-info** command to set the contact of the SNMP Agent administrator and the physical position of the device.

        Contact of the administrator: HW-075528780808. Physical position of the device: Shenzhen_China.

        ```
        huawei(config)#snmp-agent sys-info contact HW-075528780808
        huawei(config)#snmp-agent sys-info location Shenzhen_China
        ```

     c. (Optional) Configure the engine ID of the SNMP entity.

Run the **snmp-agent local-engineid** command to configure the engine ID of the SNMP environment to 0123456789.

NOTE

The engine ID of the SNMP environment must be the same as that configured on the U2000.

```
huawei(config)#snmp-agent local-engineid 0123456789
   Info: Modify the local-engineid will disable the configured SNMPv3
user, all
users must be reconfigured, proceed? (y/n)[n]:y
```

d. Set the SNMP version.

Run the **snmp-agent sys-info** command to set the required SNMP version.

```
huawei(config)#snmp-agent sys-info version v3
```

NOTE

The SNMP version on the device must be the same as that configured on the U2000.

2. Enable the function of sending traps.

Run the **snmp-agent trap enable** command on the device for sending traps to the NMS.

```
huawei(config)#snmp-agent trap enable standard
```

3. Configure the IP address of the target host of the traps.

Run the **snmp-agent target-host** command to configure the IP address of the target host of the traps.

The host name is huawei, the IP address of the host is 10.10.1.10/24 (that is, the IP address of the U2000), the name of the target host is ABC, the SNMP version is V3, the security name is user1 (when SNMP V3 is used, the 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
```

4. Configure the source IP address of the traps.

Run the **snmp-agent trap source** command to configure the source IP address of the traps.

- In inband networking mode, the IP address of the upstream port is used as the source IP address of the traps.
- In outband networking mode, the IP address of the maintenance network port is used as the source IP address of the traps.

NOTE

This document considers the outband networking mode as an example.

```
huawei(config)#snmp-agent trap source meth 0
```

5. Save the data.

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

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

- Configuration procedure on the NMS

1. Add a route from the NMS to the device.

Configure the IP address of the gateway from the NMS server to network segment 10.50.1.0/24 to 10.10.1.1.

- In the Solaris operating system (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:

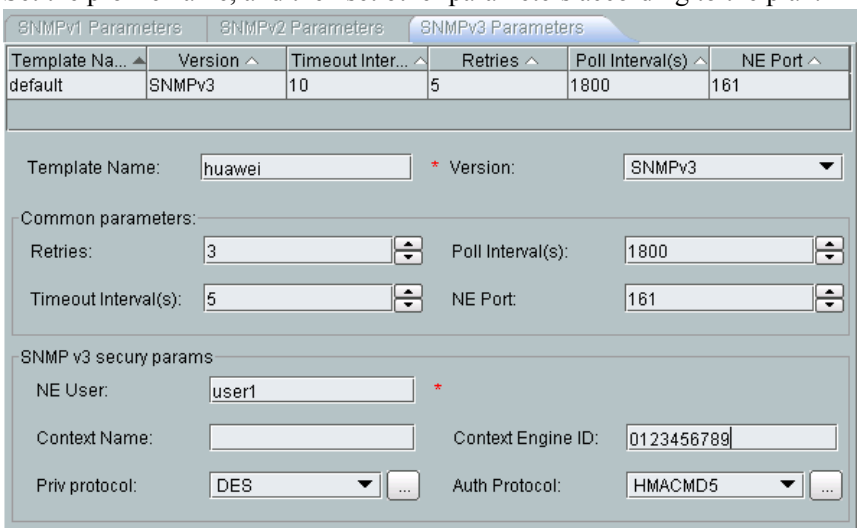
  Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

  Run the **route print** command to query the information about the current routing table.

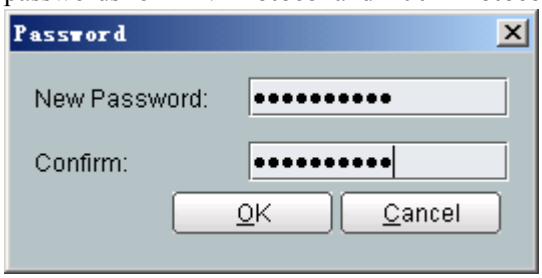
NOTE

If the IP address of the outband NMS port and the IP address of the U2000 are in the same network segment, you need not configure the route.

2. Log in to the U2000.
3. Configure the SNMP parameters.
   a. Choose **Administration** > **NE Communicate** > **Default Access Protocol Parameters** from the main menu.
   b. In **Default Access Protocol Parameters**, click the **SNMPv3 Parameters** tab, and then click **Add**.
   c. Set the profile name, and then set other parameters according to the plan.



   d. Select corresponding protocol type in **Priv Protocol** and **Auth Protocol**, and then click ... behind the parameter. In the **Password** dialog box, set the passwords for **Priv Protocol** and **Auth Protocol**. Then, click **OK**.



NOTE

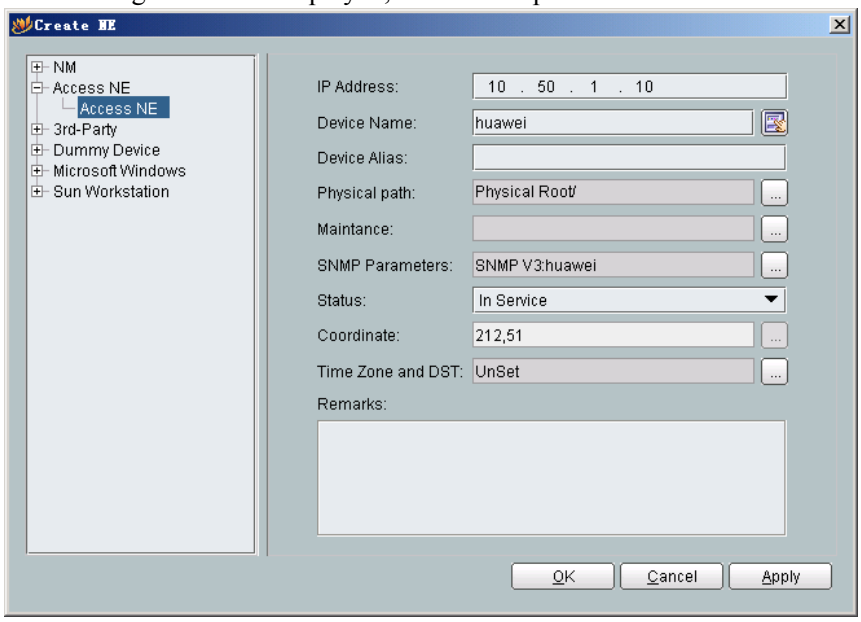
NE User, **Context Engine ID**, **Priv Protocol** and the password, and **Auth Protocol** and the password must be the same as those configured on the MA5616. The **display snmp-agent usm-user** command is used to query the device user, data encryption protocol, and authentication protocol configured on the MA5616. The **display snmp-agent local-engineid** command is used to query the environment engine ID configured on the MA5616.

e. Click **OK**. Then, the SNMP parameters are configured.

4. Add a device.

a. Right-click in the main topology, and then choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, set relevant parameters.



NOTE

- The IP address is the management IP address of the MA5616.
- Select the SNMP parameters based on the selected SNMP version. This section considers the SNMP V3: huawei profile as an example. You can select the profile according to the plan.

c. Click **OK**. Several seconds to some 10 minutes are required for uploading the device data. After reading the related, the system automatically updates the device icon.

----End

Result

You can maintain and manage the MA5616 through the U2000.

Configuration File

The following part provides the script for configuring the outband NMS (on the device).

```
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 local-engineid 0123456789
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
```

The following part provides the script for configuring the inband NMS (on the device). The management VLAN ID of the upstream port is 30.

```
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 local-engineid 0123456789
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 30
save
```

3.3 Configuring the Attributes of the Upstream Port

The MA5616 can be interconnected with the OLT through upstream GPON/GE port. This topic describes how to configure the attributes of upstream GPON/GE port so that the device communicates successfully with the upstream device.

3.3.1 Configuring an Uplink Ethernet Port

This topic describes how to configure a specified Ethernet port so that the system communicates with the upstream device in the normal state.

Context

The MA5616 should be interconnected with the upstream device through the Ethernet port. Therefore, pay attention to the consistency of port attributes.

The MA5616 supports Ethernet cascading network. On the network, multiple devices can be cascaded using GE ports to extend the network coverage and meet the requirements for large access capacity. When two MA5616s are cascaded, set GE port 0 on the upper-layer device as the cascaded port and set GE port 0 on the lower-layer device as the uplink port. For details about the configuration principles, see **Table 3-5**.

Table 3-5 Configuration principles of uplink and cascaded ports on an MA5616

Control Board	Daughter Board on the Control Board	Configuration Principles
CCUB	GP1A	● GE port 0: is set as a cascaded or uplink port. ● GPON port: is always set as an uplink port.
	EP1A	● GE port 0: is set as a cascaded or uplink port. ● EPON port: is always set as an uplink port.
	GE1A	● GE port 0: is set as a cascaded or uplink port. ● GE port 1: is always set as an uplink port.

Default configuration

Table 3-6 lists the default settings of the attributes of an Ethernet port.

Table 3-6 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	GE optical port: 1000 Mbit/s	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the port rate.
Duplex mode	Full-duplex	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 needs to be disabled.

3. (Optional) Configure the duplex mode of the Ethernet port.

   Run the **duplex** command to configure 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 mode. 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 an Ethernet cascaded port.

  1. Run the **network-role** command to set the port as an uplink or cascaded port.

     For details about the configuration principles of uplink or cascaded ports, see **Table 3-5**.

  2. Run the **combo-mode** command to switch the optical/electrical adaptation mode of the Ethernet port.

     On a cascading network, the optical/electrical adaptation mode of a cascaded port must be the same as that of an uplink port. The recommended mode is **autoadaptation** because the setting ensures that the system can select a mode automatically.

     A GE port supports optical and electrical modes:

     - For a CCUB control board, uplink GE port 0 on the daughter board or GE electrical port 0 on the front panel can be selected. Only one port is used at a time.

- Run the **flow-control** command to enable the flow control on the Ethernet port.
- Run the **mirror port** command to mirror the Ethernet port.

----End

Example

Assume that:

- The port rate is 1000 Mbit/s.
- The duplex mode is adopted.
- The flow control is supported.
- The auto-negotiation mode is not supported.

To configure the Ethernet port (optical port) of the MA5616, do as follows:

```
huawei(config)#interface eth 0/0
huawei(config-if-eth-0/0)#auto-neg 1 disable
huawei(config-if-eth-0/0)#speed 1 1000
huawei(config-if-eth-0/0)#duplex 1 full
huawei(config-if-eth-0/0)#flow-control 1
```

3.3.2 Configuring the Attributes of the Upstream PON Port

This topic describes how to query the statistics for the port, set the working mode of the optical transceiver, and set the alarm thresholds for the receive optical power of the optical transceiver through the upstream PON port.

Procedure

- Set the password for registering with the OLT.

  Run the **password** command to set the registration password of the current device that functions as a PON ONU.
- Set the alarm thresholds for the receive optical power of the optical transceiver.

  Run the **optical-module threshold** (in the GPONNNI mode) command to set the alarm thresholds for the receive optical power of the optical transceiver. After the alarm thresholds are set successfully, if the receive optical power of the optical transceiver is beyond the upper or lower threshold, the system immediately generates an alarm indicating that the optical power is abnormal.
- Set the working mode of the optical transceiver of the upstream PON port.

  Run the **laser** (in the GPONNNI mode) command to set the optical transceiver to active, always active, or disabled.
  - When disabling the optical transceiver of the upstream PON port, ensure that the upstream PON port is not carrying any services.
  - After setting the optical transceiver of the upstream PON port to always active, you can test the upstream optical power.
- Query the statistics for the port.

  Run the **display gpon-port statistic** command to query the traffic information and line status of the GPON port.

----End

Example

To set the password for registering with the OLT through the GPON port, set the lower limit for the receive optical power of the optical transceiver to 5 dBm and the upper limit for the receive optical power of the optical transceiver to 50 dBm, set the working mode of the optical transceiver of the upstream PON port to **auto**, do as follows:

```
huawei(config-if-gponnni-0/0/1)#password
{ passwordvalue<S><Length 1-10> }:huawei

  Command:
          password huawei
huawei(config-if-gponnni-0/0/1)#optical-module threshold rx-power lower-limit 5
upper-limit 50
{ <cr>|bias<K>|temperature<K>|tx-power<K>|voltage<K> }:

  Command:
          optical-module threshold rx-power lower-limit 5 upper-limit 50
huawei(config-if-gponnni-0/0/1)#laser auto
```

3.3.3 Configuring the System Energy-Saving Function

This topic describes how to power off an unnecessary board to reduce power consumption and save system energy.

Prerequisites

The board supports power-off and energy-saving modes.

Context

The MA5616 supports manual energy-saving mode. Manual energy-saving allows you to power off a board manually. Specifically, you can manually power off a board that is not used according to data plan to reduce energy consumption. When you are about to provision a service on a board that is manually powered off, the system displays a message indicating that the board is powered off. In this case, power on the board manually. By default, the energy-saving mode is disabled.

Procedure

- Run the **board power-off** command to manually power off a board.
  - When a board is not configured with any service, manually power off the board to reduce energy consumption.
  - After a board is power off manually, run the **board power-on** command to power on the board.

CAUTION

Exercise caution when running this command because this command will interrupt services on a board.

- Run the **broad-service power-off shutdown** command to disable bandwidth services.
  - When an AC-powered device is powered off and is powered by a battery, disable bandwidth services so that narrowband services can be used for a long time.

- Run the **undo broad-service power-off shutdown** command to enable disabled bandwidth services.

----End

Example

To manually power off an ASRB board that is not used and in slot 0/4 of an MA5616 to reduce energy consumption, do as follows:

```
huawei(config)#board power-off 0/4
  Powering off the board will interrupt the running services.
  Are you sure to power off the board?(y/n)[n]y
  The board is powered off successfully
huawei(config)#display board 0
  ------------------------------------------------------------------------------
  SlotID  BoardName  Status           SubType0 SubType1    Online/Offline
  ------------------------------------------------------------------------------
  0       H831CCUB   Active_normal    GP1A     ASDA
  1       H838ASPB   Normal
Online
  2       H835ADLE   Normal
Online
  3
  4       H838ASRB   Shutdown(manual)                      Online
  5       H831PAIA   Normal
  ------------------------------------------------------------------------------
```

3.4 Configuring the Link Aggregation of Upstream Ethernet Port

Port aggregation means aggregating the two upstream GE ports of the MA5616 to increase the bandwidth through load balancing. When a certain aggregated GE port or GE link fails, data is transmitted through another GE port. Thus, the reliability of the transmission is enhanced.

Prerequisites

- The network device and the line must be normal.
- The VLAN of the interface on the upper-layer device of the MA5616 must be consistent with the VLAN configured for the upstream port on the MA5616.

Context

- The parameters configured for two aggregation ports need to be the same.
- No static MAC address is allowed on the aggregation ports. You can run the **display mac-address** command to query the configuration.
- The ports to be aggregated cannot be destination mirroring ports.

Procedure

Step 1 Configure the Ethernet port aggregation.

Run the **link-aggregation** command to configure the Ethernet port aggregation.

Step 2 Query the information about the aggregation group.

Run the **display link-aggregation all** command to query the type, number and working mode of the aggregated Ethernet ports.

----End

Result

In ETH mode, the PC can still access the Internet through PPPoE dialup after you run the **shutdown** command to deactivate port 0/0/0 or 0/0/1.

Example

Assume that two upstream ports 0/0/0 and 0/0/1 on the same CCUC board of the MA5616 is to be configured as an aggregation group, and each port sends packets according to the source MAC address in the static LACP aggregation mode. To perform the preceding configuration, do as follows:

```
huawei(config)#link-aggregation 0/0 0-1 ingress workmode lacp-static
huawei(config)#display link-aggregation all
  ------------------------------------------------------------------------------
  Master port  Link aggregation mode  Port NUM  Work mode  Max link number
  ------------------------------------------------------------------------------
  0/0/0       ingress                       2  lacp-static              -
  ------------------------------------------------------------------------------
  Total: 1 link aggregation(s)
```

3.5 Configuring the ANCP

Access Node Control Protocol (ANCP) is used to implement the functions such as topology discovery, line configuration, and Layer 2 Control (L2C) OAM on the user ports. The MA5616 establishes an ANCP session according to the communication IP address of the General Switch Management Protocol (GSMP) that is used by the network access server (NAS).

Context

- The MA5616 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 MA5616 and the NAS. The NAS functions as the server of the TCP connection, and the MA5616 functions as the client of the TCP connection.
- After the TCP connection is created successfully between the MA5616 and the NAS, an ANCP session is created between the MA5616 and the NAS. After the ANCP session is created successfully, the MA5616 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 communication IP address for an ANCP session: 0.0.0.0
  - ANCP session capability set: topology-discovery, line-config, and oam
  - ANCP packet sending priority: 6
  - GSMP TCP communication port ID 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 session** command to enter the ANCP session mode.

NOTE

Currently, the system supports only two ANCP sessions.

Step 2 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 3 (Optional) Run the **ancp capability** command to configure the capability set of the ANCP session. The default value is all, that is, the three capabilities (topology discovery, line configuration, and L2C OAM) are supported.

- Supports topology discovery. When you select **topology-discovery** parameter, the DSLAM automatically reports the line parameters to the NAS.
- Supports line configuration. When you select **line-config** parameter, the DSLAM responds to the line configuration that is sent by the NAS.
- Supports the OAM. When you select **oam** parameter, the DSLAM responds to the line testing information that is sent by the NAS.
- Supports the preceding three types of capabilities, when you select **all**.

Step 4 (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.

NOTE

After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 5 (Optional) Run the **ancp nas-tcp-port** command to set the GSMP TCP communication port ID for the ANCP session on the NAS. By default, the GSMP TCP communication port ID is 6068.

The GSMP TCP communication port ID on the MA5616 must be the same as that on the NAS.

Step 6 (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 1s.

NOTE

After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 7 (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 25s.

NOTE

After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 8 Run the **ancp enable** command to enable the ANCP function. By default, the ANCP function is disabled.

NOTE

Before an ANCP session is enabled, related parameters can be modified. After an ANCP session is enabled, related parameters cannot be modified.

Step 9 Run the **quit** command to quit the ANCP mode.

Step 10 Run the **display ancp session** command to query the information about the ANCP session.

----End

Example

Assume that:

- The GSMP communication IP address for an ANCP session is 10.10.10.10.
- The interval for sending packets during the initial stage of an ANCP session is 2s.
- The ANCP session capability set is topology-discovery.
- The ANCP packet sending priority is 7.
- The GSMP TCP communication port ID on the NAS side in an ANCP session is 6000.
- The interval for sending packets during the ANCP session stage is 7s.
- The ANCP function is enabled.

To perform the preceding configurations, do as follows:

```
huawei(config)#ancp session 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 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
  Configured AN name                    : -
  AN name                               : -
  NAS name                              : -
  NAS IP                                : 10.10.10.10
  Local IP                              : -
  AN instance                           : -
  NAS instance                          : -
  Config capabilities                   : TopologyDiscovery
  Negotiate capabilities                : -
  ANCP-8021P                            : 7
  NAS TCP port                          : 6000
  Startup time(0.01s)                   : -
  Discontinuity time(0.01s)             : -
  Init interval(0.1s)                   : 20
  Keepalive interval(0.1s)              : 70
  PartitionID                           : 0
  Bandwidth CAC status                  : Disable
  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
```

3.6 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.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Scenario

VLAN application is specific to user types. For details on the VLAN application, see **Table 3-7**.

Table 3-7 VLAN application and planning

User Type	Application Scenario	VLAN Planning
• Residential user of the Internet access service • 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 subscribers are converged to the same VLAN.	VLAN type: smart VLAN attribute: common 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 type: smart Attribute: stacking VLAN forwarding mode: by S+C
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	VLAN type: smart VLAN attribute: QinQ VLAN forwarding mode: by VLAN+MAC or S+C.

Default Configuration

Table 3-8 lists the default parameter settings of VLAN.

Table 3-8 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart 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.
Default attribute of a new VLAN	Common	-
VLAN forwarding mode	VLAN+MAC	-

Procedure

Step 1 Create a VLAN.

Run the **vlan** command to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 3-9 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. One standard VLAN contains multiple upstream ports. Ethernet ports in one 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 device subtending.
Smart VLAN	To add a smart VLAN, run the **vlan *vlanid* smart** command.	One smart VLAN may contain multiple upstream ports and service ports. The service ports in one smart VLAN are isolated from each other. The service ports in different VLANs are also isolated. One VLAN provides access for multiple users and thus saves VLAN resources.	Smart VLANs are applicable to FE or xDSL service access. For example, Smart VLANs can be used in residential users.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
MUX VLAN	To add a MUX VLAN, run the **vlan *vlanid* mux** command.	One MUX VLAN may contain multiple upstream ports but only one service port. The service ports in different VLANs are isolated. 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 FE or xDSL service access. For example, MUX VLANs can be used to identify users.

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.

Step 2 (Optional) 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 3-10 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, or MUX 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 packets from a QinQ VLAN contain two VLAN tags, that is, inner VLAN tag from the private network and outer VLAN tag from the MA5616. Through the outer VLAN, an L2 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 a MUX VLAN.	The packets from a stacking VLAN contain two VLAN tags, that is, inner VLAN tag and outer VLAN tag from the MA5616. 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 L2 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 tag of the service port, run the **stacking label** command. You can run the **stacking outer-ethertype** command to set the type of outer Ethernet protocol supported by VLAN stacking on the MA5616. You can also run the **stacking inner-ethertype** command to set the type of inner Ethernet protocol supported by VLAN stacking. To ensure that Huawei device is interconnected with the device of other vendors, the type of inner/outer Ethernet protocol must be the same as that of the interconnect device.

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.

Step 3 (Optional) Configure VLAN description.

To configure VLAN description, run the **vlan desc** command. You can configure VLAN description to facilitate maintenance. The general VLAN description includes the usage and service information of the VLAN.

Step 4 (Optional) Configure the VLAN forwarding policy.

vlan-connect corresponds to the S+C forwarding policy, which ensures higher security by solving the problems of insufficiency in the MAC address space, MAC address aging, and MAC address spoofing and attacks.

To configure the VLAN forwarding policy in the VLAN service profile, 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 policy 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 created in **4.1**.

----End

Example

Assume that a QinQ VLAN with ID of 100 is to be configured for an enterprise user to ensure higher security and the VLAN forwarding policy is S+C. For the VLAN, description needs to be configured for easy maintenance. To configure such a VLAN, do as follows:

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 q-in-q
huawei(config)#vlan desc 100 description qinqvlan/forhuawei
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#forwarding vlan-connec
  Info: Please use the commit command to make modifications take effect
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 100 profile-id 1
```

3.7 Configuring the xDSL Profile

Configuring the xDSL profile is a prerequisite for configuring an xDSL access service. This topic describes how to configure an ADSL2+ profile, an SHDSL profile, and a VDSL2 profile.

3.7.1 Configuring the ADSL2+ Profile

This topic describes how to configure an ADSL2+ line profile and an ADSL2+ line alarm profile.

Prerequisites

Run the switch adsl mode to rfc4706 command to switch to the ADSL mode NGADSL.

Context

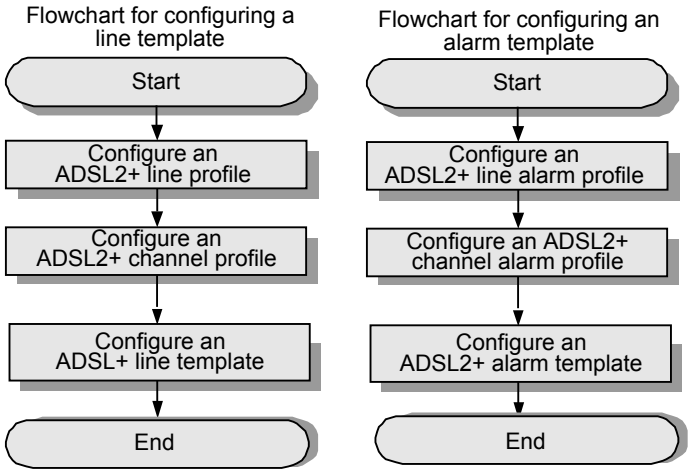
The MA5616 supports two ADSL modes, that is, ADSL mode and NGADSL mode. The two modes can be switched by running a command.

In this document, the configuration specified is based on the NGADSL mode. By default, the system supports the ADSL 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 3-23 shows the flow for configuring an ADSL2+ template.

Figure 3-23 Flowchart for configuring an ADSL2+ template



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** and **Transmission mode** (in interactive mode): 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 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 interleave depth increases directly to the interleave delay. In the interleave mode, higher interleave depth indicates more powerful error correction capability but longer interleave delay.
   - **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, it indicates that 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+ line alarm template.
  1. Run the **adsl alarm-profile quickadd** command to quickly add an ADSL2+ line alarm profile, or run the interactive **adsl alarm-profileadd** command to add an ADSL2+ line alarm profile.
  2. Run the **adsl channel-alarm-profile quickadd** command to quickly add an ADSL2 + 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+ line alarm template, or run the interactive **adsl alarm-templateadd** command to add an ADSL2+ line 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
```

3.7.2 Configuring the SHDSL Profile

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 3-11 lists the default SHDSL profiles.

Table 3-11 Default SHDSL profiles

Parameter	Default Setting
SHDSL line profile	Profile IDs: 1, 100, 101, 102, and 103 Profile 1 is used to activate the 2-wire ATM SHDSL port. Profile 100 is used to activate the 4-wire ATM SHDSL port. Profile 101 is used to activate the 6-wire ATM SHDSL port. Profile 102 is used to activate the 8-wire ATM SHDSL port. Profile 103 is used to activate the EFM-bonding SHDSL port.
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 **shdsl line-profile add** command to interactively add an SHDSL line profile.

  Main parameters:

  - **ptm**: If the SHDSL channel mode is the ATM mode, do not select **ptm**. If the SHDSL channel mode is the PTM mode, select **ptm**.
  - **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

The H832SHLH board supports G.SHDSL.BIS and the maximum rate can be 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 **shdsl line-profile add** command to interactively 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
```

3.7.3 Configuring the VDSL2 Profile

This topic describes how to configure the VDSL2 line profile and alarm profile.

Context

The MA5616 supports two VDSL2 modes, normal mode and TI mode, which are selected by running a command. By default, the system supports the normal VDSL2 mode.

In the two modes, the alarm profiles are the same but the line profiles are different:

- 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 spectrum profile, VDSL2 UPBO profile, VDSL2 DPBO profile, VDSL2 SNR margin profile, and VDSL2 delay INP profile.

In the two modes, the line parameters are the same. You can select a mode according to the configuration requirement.

3.7.3.1 Configuring the VDSL2 Profile (Normal Mode)

This topic describes how to configure the VDSL2 line profile and alarm profile in the normal mode.

Prerequisites

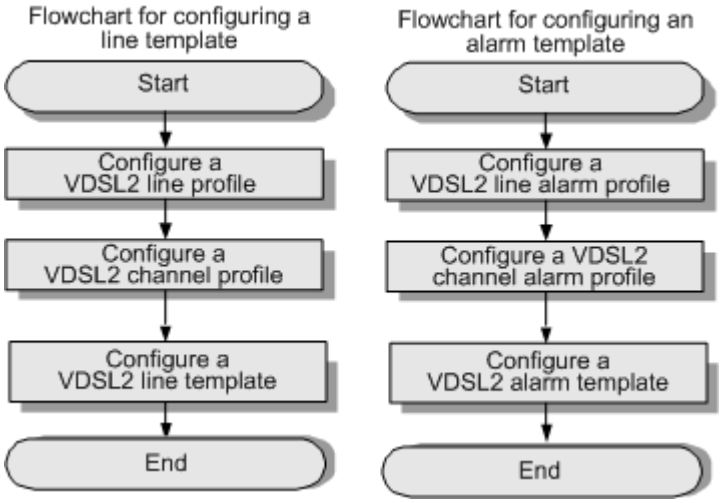
Run the switch vdsl mode to tr129 command to switch to the VDSL2 mode normal.

Context

- A VDSL2 line template consists of a VDSL2 line profile and a VDSL2 channel profile.
- Before activating a VDSL2 port, bind a VDSL2 line template to the port.
- A VDSL2 alarm template consists of a VDSL2 line alarm profile and a VDSL2 channel alarm profile.
- Bind a VDSL2 alarm template rather than a VDSL2 line alarm profile or a VDSL2 channel alarm profile to a VDSL2 port.

Figure 3-24 provides the configuration flow of a VDSL2 profile.

Figure 3-24 Flowchart for configuring a VDSL2 profile



Procedure

- Configure a VDSL2 line template.
  1. Run the **vdsl line-profile quickadd** command to quickly add a VDSL2 line profile, or run the **vdsl line-profile add** command to interactively add a VDSL2 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**: 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 VDSL2 channel profile, or run the **vdsl channel-profile add** command to interactively add a VDSL2 channel profile.

     Main parameters:

     - **path-mode**: indicates the path mode. There are two VDSL2 path modes: ATM mode and PTM mode. By default, the system supports both modes. If the default mode is used, the system can automatically adapt to the path mode of the peer end

and therefore the setting of the path mode is not required in this case. To set the ATM mode as the VDSL2 path mode, select **atm**. To set the PTM mode as the VDSL2 path mode, select **ptm**. The default setting **both** is recommended. When **both** is selected, both modes are supported.

- **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, it indicates that 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 **vdsl line-template add** command to interactively 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 **vdsl alarm-profile add** command to interactively 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 **vdsl channel-alarm-profile add** command to interactively add a VDSL2 channel alarm profile.
  3. Run the **vdsl alarm-template quickadd** command to quickly add a VDSL2 alarm template, or run the **vdsl alarm-template add** command to interactively add a VDSL2 alarm template.

     A VDSL2 alarm template consists of a VDSL2 line alarm profile and a VDSL2 channel alarm profile. Bind a VDSL2 alarm template rather than a VDSL2 line alarm profile or a VDSL2 channel alarm profile to a VDSL port.

----End

Example

To add VDSL2 profile 3 with these parameters, assume that:

- Downstream rate: 2048 kbit/s
- Channel mode: interleave mode
- Downstream maximum interleave delay: 8 ms
- Upstream maximum interleave delay: 2 ms

- SNR margin: 6 dB
- Downstream minimum INP: 4
- Upstream minimum INP: 2

```
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
```

3.7.3.2 Configuring the VDSL2 Profile (TI Mode)

This topic describes how to configure the VDSL2 line profile and alarm profile in the TI mode.

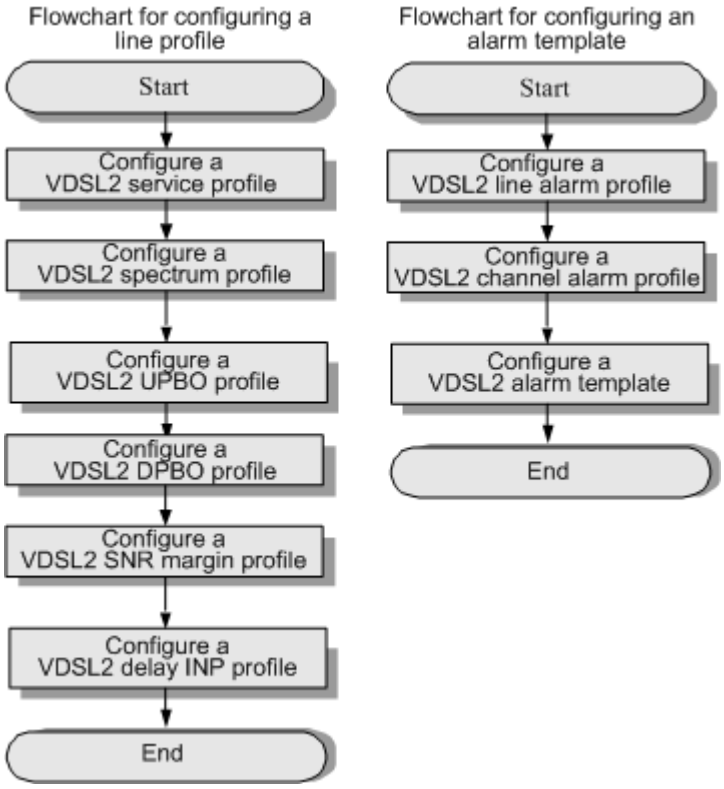
Prerequisites

Run the switch vdsl mode to timode command to switch to the VDSL2 mode TI.

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 3-25** provides the configuration flow of a VDSL2 profile.

Figure 3-25 Flowchart for configuring a VDSL2 profile



Procedure

- Configure a VDSL2 line profile.
  1. Run the **vdsl service-profile quickadd** command to quickly add a VDSL2 service profile, or run the **vdsl service-profile add** command to interactively 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 VDSL2 path modes: ATM mode and PTM mode. To set the ATM mode as the VDSL2 path mode, select **atm**. To set the PTM mode as the VDSL2 path mode, select **ptm**.
     - **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 **vdsl delay-inp-profile add** command to interactively add a VDSL2 delay INP profile. Main parameters:
     - **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, it indicates that 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 **vdsl noise-margin-profile add** command to interactively add a VDSL2 SNR margin profile. Main parameter:

     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 **vdsl spectrum-profile add** command to interactively add a VDSL2 spectrum profile. Main parameter:

     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 **vdsl upbo-profile add** command to interactively add a VDSL2 UPBO profile.
  6. Run the **vdsl dpbo-profile quickadd** command to quickly add a VDSL2 DPBO profile, or run the **vdsl dpbo-profile add** command to interactively 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 **vdsl alarm-profile add** command to interactively 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 **vdsl channel-alarm-profile add** command to interactively add a VDSL2 channel alarm profile.
  3. Run the **vdsl alarm-template quickadd** command to quickly add a VDSL2 alarm template, or run the **vdsl alarm-template add** command to interactively add a VDSL2 alarm template.

     A VDSL2 alarm template consists of a VDSL2 line alarm profile and a VDSL2 channel alarm profile. Bind a VDSL2 alarm template rather than a VDSL2 line alarm profile or a VDSL2 channel alarm profile to a VDSL port.

----End

Example

Assume the following configurations:

- 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 profiles with index 3, 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
```

3.8 Configuring the System Clock

This topic describes how to configure the system clock to restrict the clock frequency and phase of each node on a network within the preset tolerance scope. This prevents the deterioration of the TDM service quality caused by inaccurate signal timing at both the transmit and receive ends in the digital transmission system.

Context

- The IP-based development is the trend of future network and service development. Currently, certain difficulties exist in the transition of the access network (AN) from the traditional network to the IP-based Ethernet bearer network. One of the difficulties is how to carry the traditional TDM service on the IP network.

- On the traditional telecommunications network, the TDM service carried on the AN is mainly the voice service. Cumulative inconsistency between the clocks at both ends of the bearer network over a long time causes frame slip, which reduces the quality of the voice service. Moreover, the wireless application has more 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. Therefore, clock synchronization is very important in the TDM voice service.

3.8.1 Configuring the Reference Source of the System Clock

This topic describes how to configure the clock reference sources so that the system clock can select a reference source when needed.

Context

- To ensure that the MA5616 and other devices on a network use the unified time, the clock signals of a certain port must be specified as the reference source of the system clock. The system clock is also used as the system output clock.
- The system supports a maximum of ten clock reference sources. The system selects a reference source according to the priority level of each reference source.
- The reference sources of the system clock include the adaptive clock, and line clock.
  - The adaptive clock restores a clock from the PHS service at the upper layer as the reference source of the system clock.
  - The line clocks supported by the system include the GE line clock, GPON line clock, . That is, the system receives a line clock transferred by the upper-layer device through the GE/GPONuplink interface, and restores the line clock as the reference source of the system clock, thus implementing clock synchronization with the upper-layer device.

3.8.1.1 Configuring the Adaptive Clock Reference Source

The In the PHS service, the UA5000 sends a unidirectional E1 clock packet to the MA5616. The MA5616 can use the clock in the packet as the clock reference source.

Procedure

Step 1 Run the **vlan** command to create the VLAN for carrying clock packets.

Step 2 Run the **ip address** command to set the IP address of the Layer 3 VLAN.

Step 3 Run the **port vlan** command to add an uplink port to the VLAN.

Step 4 Run the **acm-clock-ip** command to set the IP address of the Layer 3 interface for receiving adaptive clock method (ACM) clock packets.

NOTE

The IP address of the Layer 3 interface configured to receive ACM clock packets cannot be used as the IP address of the NMS interface.

Step 5 Run the **clock source** command to set the ACM clock as the clock source of the system.

----End

Example

To configure system clock resource 0 for receiving ACM clock packets from Layer 3 interface whose IP address is 20.20.20.20 (assume that the subnet mask length is 24), run the following commands:

```
huawei(config)#vlan 14
huawei(config)#interface vlanif 14
huawei(config-if-vlanif14)#ip address 20.20.20.20 24
huawei(config-if-vlanif14)#quit
huawei(config)#port vlan 14 0/0 0
huawei(config)#acm-clock-ip 20.20.20.20 0/2
huawei(config)#clock source 0 acm-clock 0/2/
```

3.8.1.2 Configuring the Line Clock Reference Source

The MA5616 supports tracing of the uplink GE, GPON line clock. The clock synchronized through the physical layer and restored from the line code stream can serve as the reference source of the system clock.

Procedure

Step 1 Run the **clock source** *srcindex frameid/slotid/portid* command to configure the clock restored at a certain GE, GPON, or port as the reference source of the system clock.

Step 2 Run the **display clock source** command to check whether the line clock source information is consistent with the data plan.

----End

Example

To configure clock source 0, set the reference source to the GPON line clock, and set the reference source port to 0/0/1, do as follows:

```
huawei(config)#clock source 0 0/0/1
  Clock source set succeeded
huawei(config)#clock priority system 0
  Clock source priority set succeeded
huawei(config)#display clock source
  ------------------------------------------------------------------------
  Index  Config   Type   Source      State     Priority   Output
  ------------------------------------------------------------------------
    0    YES      line   0/ 0/ 0     Failed    0          ---
    1    NO       --     -/ -/ -     ---       ---        ---
    2    NO       --     -/ -/ -     ---       ---        ---
    3    NO       --     -/ -/ -     ---       ---        ---
    4    NO       --     -/ -/ -     ---       ---        ---
    5    NO       --     -/ -/ -     ---       ---        ---
    6    NO       --     -/ -/ -     ---       ---        ---
    7    NO       --     -/ -/ -     ---       ---        ---
    8    NO       --     -/ -/ -     ---       ---        ---
    9    NO       --     -/ -/ -     ---       ---        ---
  ------------------------------------------------------------------------
  The current system clock source: local , index: 255
```

3.8.2 Configuring the Priority of the System Clock

This topic describes how to configure the priority for the clock reference source of the system. The MA5616 selects the system clock according to the configured clock priorities.

Prerequisites

The system clock reference source must be configured.

Context

- The added system clock source can be used in the system only after it is configured with a priority.
- The priority of the clock source takes effect immediately after it is configured. This operation, however, may cause the clock switching in the system.
- The system does not determine the quality of the clock source. Therefore, you need to configure the clock reference source of high quality with a high priority.

Procedure

- Run the **clock priority** command to configure the priority of the clock source.

  The system supports 10 priorities for the clock reference source. The priorities are represented in the form of *p0/p1/p2/p3/p4/p5/p6/p7/p8/p9*, in which p0 indicates the highest priority and p9 indicates the lowest priority. For example, if p0-p9 is set to 3/7/8, it indicates that the priority of the clock reference source with index 3 is the highest, the priority of the reference source with index 7 is lower, and the priority of the reference source with index of 8 is the lowest.

----End

Example

To configure the priority of clock reference source 0 to the highest priority and the priority of clock reference source 1 to the second highest priority, do as follows:

```
huawei(config)#clock priority system 0/1
  Clock source priority set succeeded
```

3.9 Configuring the System Time

This topic describes the feature of the NTP protocol and how to configure NTP time on the MA5616.

3.9.1 Configuring the NTP Time

Configuring the NTP protocol to keep the time of all devices in the network synchronized, so that the Context implement 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 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 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: broadcast mode, multicast mode, unicast server mode, and peer mode. The MA5616 supports all these modes.

Default Configuration

Table 3-12 provides the default configuration for NTP.

Table 3-12 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

3.9.1.1 (Optional) Configuring NTP Authentication

This topic describes how to configure NTP authentication. After NTP authentication is configured, the function can be enabled in the network that has high requirements on security to improve the network security and prevent unauthorized users from modifying the clock.

Prerequisites

Before configuring the NTP authentication, make sure that the network interface and the routing protocol of the MA5616 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.

Precaution

- 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 need not 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
aNiceKey
huawei(config)#ntp-service reliable authentication-keyid 42
```

3.9.1.2 Configuring the NTP Broadcast Mode

This topic describes how to configure the MA5616 for clock synchronization in the NTP broadcast mode. After the configuration is complete, the server periodically broadcasts clock synchronization packets through a specified port, and functions as a client to snoop on the broadcast packets sent from the server and synchronizes the local clock according to the received broadcast packets.

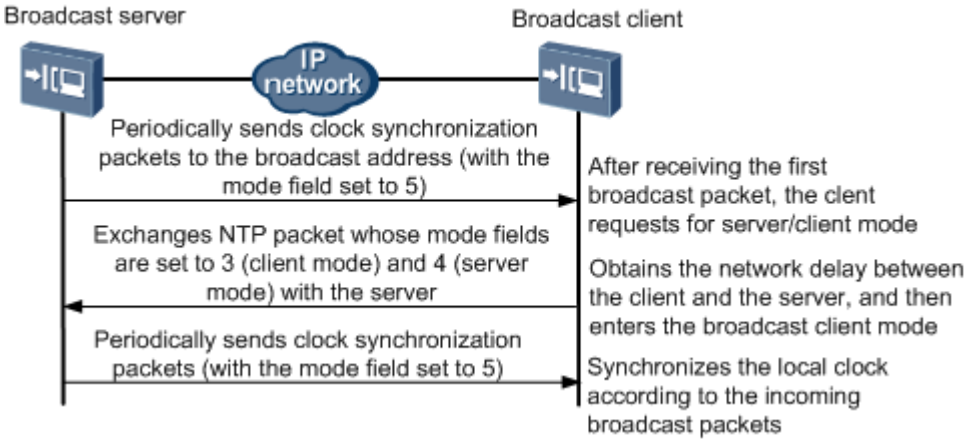
Prerequisites

Before configuring the NTP broadcast mode, make sure that the network interface and the routing protocol of the MA5616 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 snoops on the broadcast packets sent from the server. After receiving the first broadcast packet, the client exchanges NTP packet whose interaction mode fields are set to 3 (on the client) and 4 (on the server) with the server to obtain the network delay between the client and the server. The client then enters the broadcast client mode, continues to snoop on the incoming broadcast packets, and synchronizes the local clock according to the incoming broadcast packets, as shown in **Figure 3-26**.

Figure 3-26 NTP broadcast mode



Precaution

1. In the broadcast mode, you need to configure both the NTP server and the NTP client.
2. The clock stratum of the synchronizing device must be smaller than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

- 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 L3 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 vlanif** command to create a VLAN interface, and then enter the VLAN interface mode to configure the L3 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 L3 forwarding.

3. Run the **ntp-service broadcast-client** command to configure the host as the NTP broadcast client.

----End

Example

Assume the following configurations: MA5616 functions as the NTP client, snooping on the broadcast packets sent from the server through IP address 10.10.10.20/24 of the L3 interface of VLAN 2 and synchronizing the local clock with the clock on the broadcast server. To perform these configurations, do as follows:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 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
```

3.9.1.3 Configuring the NTP Multicast Mode

This topic describes how to configure the MA5616 for clock synchronization in the NTP multicast mode. After the configuration is complete, the server periodically multicasts clock synchronization packets through a specified port, and functions as a client to listen to the multicast packets sent from the server and synchronizes the local clock according to the received multicast packets.

Prerequisites

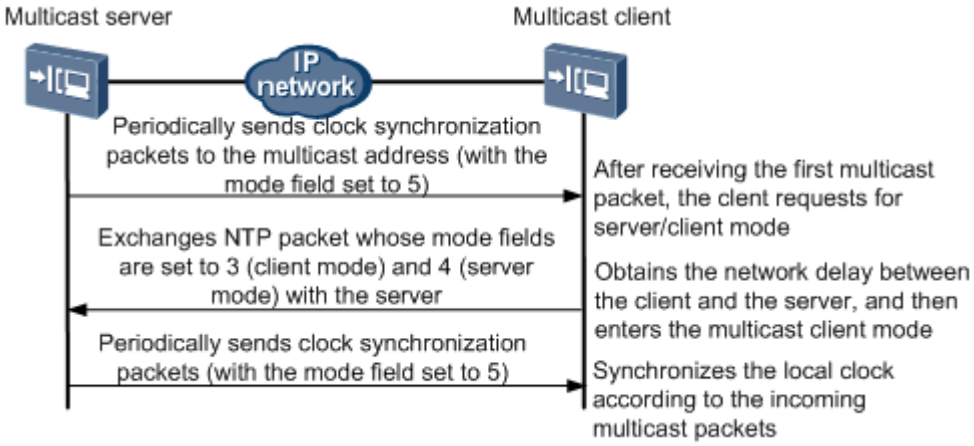
Before configuring the NTP multicast mode, make sure that the network interface and the routing protocol of the MA5616 are configured so that the server and the client are reachable to each other at the network layer.

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 3-27**.

Figure 3-27 NTP multicast mode



Precaution

1. In the multicast mode, you need to 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 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 L3 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 vlanif** command to create a VLAN interface, and then enter the VLAN interface mode to configure the L3 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 L3 forwarding.

3. Run the **ntp-service multicast-client** command to configure the host as the NTP multicast client.

----End

Example

Assume the following configurations: MA5616 functions as the NTP client, listening to the multicast packets sent from the server through IP address 10.10.10.20/24 of the L3 interface of VLAN 2 and synchronizing the local clock with the clock on the multicast server. To perform these configurations, do as follows:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 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
```

3.9.1.4 Configuring the NTP Unicast Server Mode

This topic describes how to configure the MA5616 as the NTP client to synchronize with the NTP server in the network.

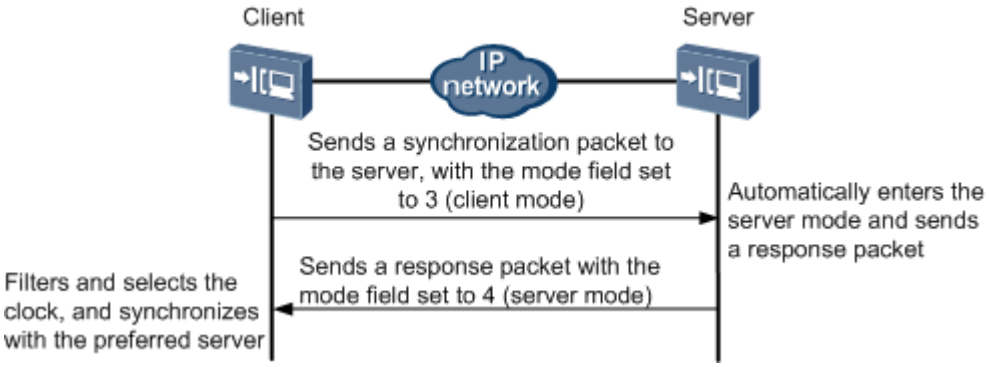
Prerequisites

Before configuring the NTP client/server mode, make sure that the network interface and the routing protocol of the MA5616 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 3-28**.

Figure 3-28 NTP client/server mode



Precaution

1. In the client/server mode, you need to configure only the client, and need not 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 L3 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 vlanif** command to create a VLAN interface, and then enter the VLAN interface mode to configure the L3 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 L3 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 L3 interface. Only the IP packet from the clock server is allowed to access the L3 interface. Other unauthorized packets are not allowed to access the L3 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: The IP address of the NTP server is 10.20.20.20/24, MA5616 (IP address of the L3 interface of VLAN 2: 10.10.10.10/24 and gateway IP address: 10.10.10.1) functions as the NTP client, the NTP client sends the clock synchronization request

packet through the VLAN L3 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 L3 interface. To perform these configurations, do as follows:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 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 3010
huawei(config-acl-adv-3010)#rule deny ip source any destination 10.10.10.10
0.0.0.0
huawei(config-acl-adv-3010)#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-3010)#quit
huawei(config)#packet-filter inbound ip-group 3010 port 0/0/0
```

3.9.1.5 Configuring the NTP Peer Mode

This topic describes how to configure the MA5616 for clock synchronization in the NTP peer mode. In the peer mode, configure only the active peer, and the passive peer need not 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.

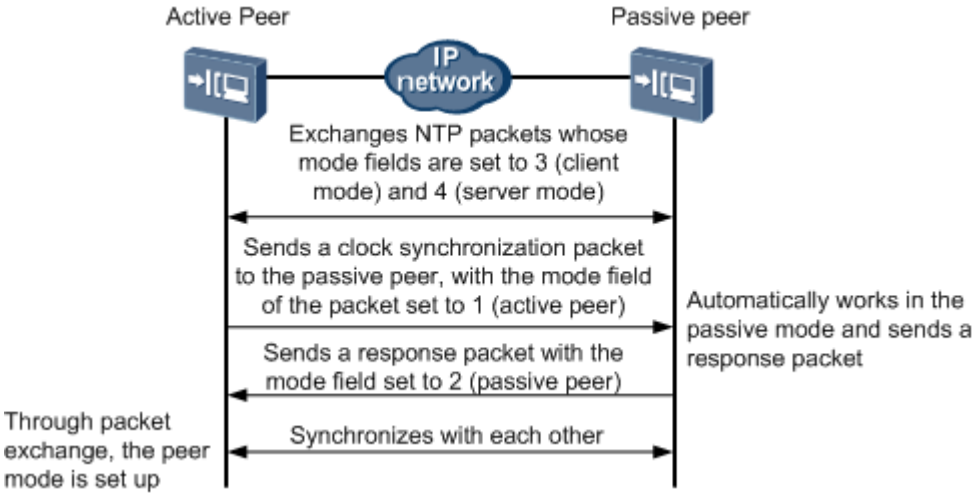
Prerequisites

Before configuring the NTP peer mode, make sure that the network interface and the routing protocol of the MA5616 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 3-29**.

Figure 3-29 NTP peer mode



Precaution

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 L3 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 vlanif** command to create a VLAN interface, and then enter the VLAN interface mode to configure the L3 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 L3 forwarding.

----End

Example

Assume the following configurations: One MA5616 functions as the NTP active peer (IP address of the L3 interface of VLAN 2: 10.10.10.10/24) and works on clock stratum 4, the other MA5616 (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 L3 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 0/0 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
```

3.10 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, thus protecting the user account against theft and roaming.
- DHCP option82: The user physical location information is added to the option82 field in the DHCP request sent by the user. The information is used by the upper-layer authentication server for authenticating the user, thus 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, thus ensuring the security of the authentication.
- MAC address binding: The MAC address is bound to the service port, thus 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 3-13 lists the default settings of the user security mechanism.

Table 3-13 Default settings of the user security mechanism

Parameter	Default Setting	Remarks
PITP	Global function: disabled VLAN-level function: enabled	The PITP function can be enabled only when the functions at all levels are enabled.

Parameter	Default Setting	Remarks
DHCP option82	Global function: disabled VLAN-level function: enabled	The DHCP option82 function can be enabled only when the functions at all levels are enabled.
Anti-IP spoofing	Global function: disabled VLAN-level function: disabled	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.

3.10.1 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 L2 P2P communication. PITP can be used for transferring the user physical port information and protecting the user account against theft and roaming.

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, thus 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).

- PPPoE+ mode: It means during the PPPoE negotiation between the users and BRAS, the device adds TAG to PPPoE packets and transmits the port information to the BRAS.
- VBRAS mode: It means during the PPPoE negotiation between the users and BRAS, the BRAS sends VBRAS enquiry packets to the device to request the device to report the port information. The device sends the port information to the BRAS by VBRAS response packets.

PITP is applicable to the networking of a standalone MA5616 and the networking of subtended MA5616s.

- In the networking of a standalone MA5616: Two PCs (PC1 and PC2) are connected to different ports of the MA5616 for the dialup access.
- In the networking of subtended MA5616s: Two PCs (PC1 and PC2) are connected to different MA5616s (PC1 is connected to the MA5616, and PC2 is connected to the MA5616 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 MA5616. 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 thus rejects the dialup access request of PC2.

Default Configuration

Table 3-14 lists the default settings related to PITP.

Table 3-14 Default settings related to PITP

Parameter	Default Setting
PITP function	Global function: disabled VLAN-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.

- 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 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.

In other modes, the RID format is fixed and therefore it need not be configured manually.

Step 2 Configure the PITP function.

The PITP function can be enabled or disabled at two levels. The PITP function is enabled only when it is enabled at both levels.

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. (Optional) 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 service profile configured in **2.2.a** to the VLAN.

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, shelf 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+MA5616 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 on the OLT.
  2. When the PITP function is enabled only on the MA5616, the tag of the PADI packet contains only the information about the user port on the MA5616.
  3. If the PITP function is enabled on both the OLT and the MA5616, 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 on the OLT.
     - When this function is disabled, subscribers connected to the service port fail to dial a number. That is, the PADI packet (PITP P mode) cannot be transmitted.

- Run the **raio sub-option 0x90** 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 link type and encapsulation information. 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: shelf ID/slot ID/port ID:VPI.VCI
- CID format for the Ethernet access mode: shelf ID slot ID port ID:VLAN ID

To enable the PITP P function for the traffic stream with VLAN ID 30, 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 rid atm plabel
huawei(config)#raio-format pitp-pmode rid eth plabel
huawei(config)#pitp enable pmode
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#pitp enable
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 30 profile-id 1
```

To set the Ethernet protocol type of VBRAS packets to be the same as the Ethernet protocol type of the upper-layer BRAS, namely, 0x8500, enable the PITP V function for the traffic stream with VLAN ID 30, and configure the RAIO mode to common, do as follows:

```
huawei(config)#raio-mode common pitp-vmode
huawei(config)#pitp enable vmode
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#pitp enable
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 30 profile-id 1
```

3.10.2 Configuring Anti-Theft and Roaming of User Accounts Through DHCP

DHCP improves the user authentication security by adding the user physical location information to the option82 field of the DHCP request packets initiated by the user, so as to prevent theft and roaming of the user account.

Context

The option82 field contains the circuit ID (CID), remote ID (RID), and sub-option 90 field (optional), which provides the information such as the user shelf ID, slot ID, port ID, VPI, and VCI.

The MA5616 can work in the L2 DHCP forwarding mode. In the mode, anti-theft and roaming of user accounts through DHCP option82 can be configured.

Table 3-15 lists the default settings related to DHCP option82.

Table 3-15 Default settings related to DHCP option82

Parameter	Default Setting
Status of the DHCP option82 function	Global status: disabled VLAN-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 information option (RAIO). Before using the DHCP function, you must configure the RAIO.

Run the **raio-mode** command to set the RAIO mode.

- Select **dhcp-option82** 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-option82** 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.
- In other modes, the RID format is fixed and therefore it need not be configured manually.

Step 2 (Optional) Set the service port to allow or prohibit the user-side DHCP packets that carry the option82 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 option82 information.

  The system adds the device name, shelf ID, slot ID, and port ID to the option82 field of DHCP packets to generate new packets. If the service port is set to allow the packets carrying the option82 information, tagged packets are forwarded. If the service port is set to prohibit the packets carrying the option82 information, tagged packets are dropped.

Step 3 Enable or disable the DHCP option82 function.

Run the **dhcp option82** command to enable the DHCP option82 function on the port. By default, the DHCP option82 function is disabled globally.

The DHCP option82 function can be enabled or disabled at two levels. The DHCP option82 function takes effect only when it is enabled at both levels.

1. Global DHCP option82 function: Run the **dhcp option82** command to enable the DHCP option82 function globally. By default, the DHCP option82 function is disabled globally.
2. VLAN-level DHCP option82 function:

a. (Optional) 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 option82 function. By default, the DHCP option82 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 **3.2.a** to the VLAN.

----End

Example

Assume the following configuration:

- RAIO mode: user-defined mode
- CID format for the Ethernet access mode: shelf ID/slot ID/sub slot ID/port ID:VLAN ID
- CID format for the ATM access mode: shelf ID/slot ID/port ID:VPI.VCI
- RID format for all access modes: label of the service port

To enable the DHCP option82 function, do as follows:

```
huawei(config)#raio-mode user-defined dhcp-option82
huawei(config)#raio-format dhcp-option82 cid eth anid eth frame/slot/subslot/
port:vlanid
huawei(config)#raio-format dhcp-option82 cid atm anid frame/slot/port:vpi.vci
huawei(config)#raio-format dhcp-option82 rid eth splabel
huawei(config)#raio-format dhcp-option82 rid atm splabel
huawei(config)#dhcp option82 enable
```

3.10.3 Configuring the Anti-IP Address Attack

This topic describes how to configure IP address binding and anti-IP address spoofing to prevent malicious users from attacking devices or authorized users by forging the IP addresses of the authorized users.

Context

IP address binding refers to binding an IP address to a service port. After the binding, only the upstream packets whose source IP address is the bound IP address can be sent through the service port. The packets whose source IP addresses are different from the bound IP address are discarded.

The anti-IP address spoofing function dynamically triggers IP address binding, preventing unauthorized users from forging the IP addresses of authorized users. When the anti-IP address spoofing function is enabled, the IP address is bound to the user port after the user goes online. Then, the users with other IP addresses cannot go online on this user port. In addition, the users with the forged IP address cannot go online on this user port either.

Procedure

- The procedure for binding an IP address is as follows:

  Run the **bind ip** command to bind an IP address.

After the configuration, only the users with specified IP addresses can access the network, preventing malicious users from forging the IP addresses of authorized users.

- The procedure for configuring anti-IP address spoofing is as follows:

  Anti-IP address spoofing can be enabled or disabled at two levels. This function takes effect only when it is enabled at both levels.

  - Global level:

    Run the **security anti-ipspoofing** command to configure global anti-IP address spoofing. By default, this level is disabled.

  - VLAN level:

    1. Run the **vlan service-profile** command to create a virtual local area network (VLAN) service profile and enter VLAN service profile mode.
    2. Run the **security anti-ipspoofing** command to configure VLAN-level anti-IP address spoofing. By default, this level 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 exit the VLAN service profile mode.
    5. Run the **vlan bind service-profile** command to bind the VLAN service profile created in step 1 to the VLAN.

  NOTE

  If a user goes online before anti-IP address spoofing is enabled, the system does not bind the IP address of this user. As a result, the service of this user will be interrupted, and this user needs to go offline and then go online again. Only the IP address of the user who goes online after anti-IP address spoofing is enabled can be bound.

----End

Example

To bind IP address 10.1.1.245 to service port 2 so that service port 2 allows only the packets with IP address 10.1.1.245 to pass, do as follows:

```
huawei(config)#bind ip service-port 2 10.1.1.245
```

To enable anti-IP address spoofing in 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
```

3.10.4 Configuring the Anti-MAC Address Attack

This topic describes how to configure MAC address binding and anti-MAC address spoofing to prevent malicious users from attacking devices or authorized users by forging the MAC addresses of the authorized users.

Context

MAC address binding refers to binding a MAC address to a service port. After the binding, only the user with the specified MAC address can access the network through the service port. The

MA5616 does not support direct binding of a MAC address to a port. Instead, you need to configure static MAC address entries for the port and set its maximum number of learnable MAC addresses to 0.

The anti-MAC address spoofing function prevents unauthorized users from forging the MAC addresses of authorized users. This function protects the services of authorized users. Anti-MAC address spoofing is mainly used for Point-to-Point Protocol over Ethernet (PPPoE) and Dynamic Host Configuration Protocol (DHCP) access users.

Procedure

- The procedure for binding a MAC address is as follows:
  1. Run the **mac-address static** command to configure a static MAC address for a port.
  2. Run the **mac-address max-mac-count** command to set the maximum number of learnable MAC addresses of the port to 0.

     The maximum number of learnable MAC addresses of a port limits the maximum number of MAC addresses that can be learned under the same account. This parameter also limits the maximum number of PCs that can access the network by using the same account.
- The procedure for configuring anti-MAC address spoofing is as follows:

  NOTE

  It is recommended that anti-MAC address spoofing be enabled to ensure device security.

  Anti-MAC address spoofing can be enabled or disabled at tow levels. This function takes effect only when it is enabled at both the tow levels.

  - Global level:

    Run the **security anti-macspoofing** command to configure global anti-MAC address spoofing. By default, this level is disabled.
  - VLAN level:
    1. Run the **vlan service-profile** command to create a virtual local area network (VLAN) service profile and enter VLAN service profile mode.
    2. Run the **security anti-macspoofing** command to configure VLAN-level anti-MAC address spoofing. By default, this level 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 exit the VLAN service profile mode.
    5. Run the **vlan bind service-profile** command to bind the VLAN service profile created in step **1** to the VLAN.

  NOTE

  If a user goes online before anti-MAC address spoofing is enabled, the system does not bind the MAC address of this user. As a result, the service of this user will be interrupted, and this user needs to go offline and then go online again. Only the MAC address of the user who goes online after anti-MAC address spoofing is enabled can be bound.

----End

Example

Assume that:

- The index of the service port is 1.
- The static MAC address of this service port is 1010-1010-1010.
- The maximum number of learnable MAC addresses of this service port is 0.

To bind MAC address 1010-1010-1010 to service port 1 so that service port 1 allows only the packets with source MAC address 1010-1010-1010 to pass, 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 address spoofing in VLAN 10 and set the maximum number of learnable MAC addresses of service port 2 in this VLAN to 7, do as follow:

```
huawei(config)#security anti-macspoofing enable
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#security anti-macspoofing enable
  Info: Please use the commit command to make modifications take
effect
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
huawei(config)#vlan bind service-profile 10 profile-id 3
huawei(config)#security anti-macspoofing max-mac-count service-port 2 7
```

3.11 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 MA5616 can be protected against the attacks from the network side or user side, and therefore the MA5616 can run stably in the network.

- ACL/Packet filtering firewall
- Blacklist
- Anti-DoS attack
- MAC address filtering
- User-side ring network detection
- Allowed/Denied address segment

Table 3-16 lists the default settings of system security.

Table 3-16 Default settings of system security

Parameter	Default Setting
Firewall blacklist	Disabled
Anti-DoS attack	Disabled
User-side ring network detection	Disabled

3.11.1 Configuring Firewall

Configuring system firewall can control the packets that go through the management port of the device so that unauthorized operators cannot access the system through the inband or outband channel.

Context

Firewall includes the following items:

- Blacklist: The blacklist function can be used to screen the packets sent from a specific IP address. A major feature of the blacklist function is that entries can be dynamically added or deleted. When firewall detects the attack attempt of a specific IP address according to the characteristics of packets, firewall actively adds an entry to the blacklist and then filters the packets from this IP address.
- ACL/Packet filtering firewall: Configure an ACL to filter data packets. To set a port to allow only one type of packets to go through, use the ACL to implement the packet filtering function.

  For example, to allow only the packets from source IP address 1.1.1.1 to go through a port in the inbound direction, do as follows:

  1. Configure an ACL **rule1**, which allows the packets with source IP address 1.1.1.1 to pass.
  2. Configure an ACL **rule2**, which denies all packets.
  3. Run the **firewall packet-filter** command, and bind rule2 first and then rule1 to the inbound direction.

     NOTE

     On the MA5616, an ACL can be activated in two modes. In two modes, the execution priorities on the sub-rules in one ACL are different.

     - Run the **firewall packet-filter** command to activate an ACL. This mode is mainly applied to the NMS. For the sub-rules in one ACL, the execution priority is implemented by software. The earlier the execution priority of the sub-rules in one ACL is configured, the higher the priority.
     - Run the **packet-filter** command to activate an ACL. For the sub-rules in one ACL, the execution priority is implemented by hardware. The later the execution priority of the sub-rules in one ACL is configured, the higher the priority.

CAUTION

To ensure device security, firewall must be configured. This is to control the packets that go through the management port of the device.

Procedure

- Configure a firewall blacklist.

  Two modes are supported: configuring a firewall blacklist by using ACLs or by adding the source IP addresses of untrusted packets. Choose either mode, or both.

  When two modes are configured, the priority of the firewall blacklist function is higher than the priority of ACLs. That is, the system checks the firewall blacklist first, and then matches ACLs.

NOTE

The firewall blacklist function only takes effect to the service packets that are sent from the user side.

- Configure the firewall blacklist function by using advanced ACLs.
  1. Run the **acl** command to create an ACL. Only advanced ACLs can be used when the black list function is enabled. Therefore, the range of the ACL ID is 3000-3999.
  2. Run the **rule(adv acl)** command to create an advanced ACL.
  3. Run the **quit** command to return to the global config mode.
  4. Run the **firewall blacklist enable acl-number** ***acl-number*** command to enable the firewall blacklist function.
- Configure the firewall blacklist function by adding the source IP addresses of untrusted packets.
  1. Run the **firewall blacklist item** command to add the source IP addresses of untrusted packets to the blacklist.
  2. Run the **firewall blacklist enable** command to enable the firewall blacklist function.

- Configure the firewall (filtering packets based on the ACL).
  1. Run the **acl** command to create an ACL. Only basic ACLs and advanced ACLs can be used when packet filtering by firewall is configured. Therefore, the range of the ACL ID is 2000-3999.
  2. Run different commands to create different types of ACLs.
     - Basic ACL: Run the **rule(basic acl)** command.
     - Advanced ACL: Run the **rule(adv acl)** command.
  3. Run the **quit** command to return to the global config mode.
  4. Run the **firewall enable** command to enable the firewall blacklist function. By default, the firewall blacklist function is disabled.

     To filter the packets of a port based on the basic ACL, enable the firewall blacklist function.
  5. Run the **firewall packet-filter** command to apply firewall packet filtering rules to an interface.

----End

Example

To add IP address 192.168.10.18 to the firewall blacklist with the aging time of 100 min, do as follows:

```
huawei(config)#firewall blacklist item 192.168.10.18 timeout 100
huawei(config)#firewall blacklist enable
```

To add the IP addresses in network segment 10.10.10.0 to the firewall blacklist and bind ACL 3000 to these IP addresses, do as follows:

```
huawei(config)#acl 3000
huawei(config-acl-adv-3000)#rule deny 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
```

To deny the users in network segment 172.16.25.0 to access the maintenance Ethernet port with IP address 172.16.25.28 on the device, 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
```

3.11.2 Preventing the Access of Invalid Users

This topic describes how to configure the IP address/MAC address binding to ensure the security of user authentication and prevent the access of illegal 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.

MAC address binding refers to binding a 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 MA5616 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.

Procedure

- Bind an IP address.

  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.
- Bind a MAC address.
  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. By default, the maximum number of learnable MAC addresses of a port in the system is 600.

     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.

----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 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
```

3.11.3 Preventing the Attack of Invalid Users

This topic describes how to configure anti-IP spoofing and anti-MAC spoofing to prevent malicious users from attacking legal users by forging the IP address and MAC address of the legal users.

Context

Anti-IP spoofing is to dynamically trigger the IP address binding, thus 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.

The major function of anti-MAC spoofing is to prevent illegal users from forging the MAC address of legal users. The purpose is to ensure that the service of legal users is not affected. Anti-MAC spoofing is mainly applied to PPPoE and DHCP access users.

Procedure

- Configure anti-IP spoofing.

  The anti-IP spoofing function can be enabled or disabled at two levels. The anti-IP spoofing function is enabled only when it is enabled at both levels.

  - Global function: Run the **security anti-ipspoofing** command to configure the global function. By default, the global function is disabled.
  - 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 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 service profile configured in **1** to the VLAN.

  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.

- Configure anti-MAC spoofing.

CAUTION

To ensure device security, it is recommended that you enable this 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.
- 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-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 service profile configured in **1** to the VLAN.
- 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 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 anti-MAC-duplicate function is disabled.

  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 enable anti-IP spoofing for 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
```

To enable anti-MAC spoofing for VLAN 10, and set the maximum number of MAC addresses that can be bound to service port 2 to 7, do as follows:

```
huawei(config)#security anti-macspoofing enable
huawei(config)#vlan service-profile profile-id 2
huawei(config-vlan-srvprof-2)#security anti-macspoofing 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-macspoofing max-mac-count service-port 2 7
```

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-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
```

3.12 Configuring AAA

This topic describes how to configure the AAA on the MA5616, including configuring the MA5616 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

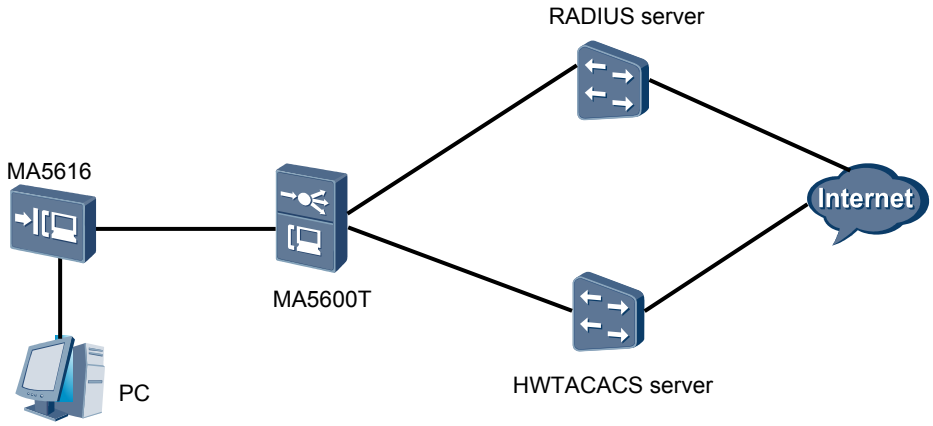
AAA is generally applied to the users that access the Internet in the PPPoA, PPPoE, 802.1x, VLAN, WLAN, ISDN, or Admin Telnet (associating the user name and the password with the domain name) mode.

NOTE

In the existing network, 802.1x and Admin Telnet correspond to the local AAA, that is, the MA5616 functions as a local AAA server; PPPoE corresponds to the remote AAA, that is, the MA5616 functions as the client of a remote AAA server.

Figure 3-30 shows an example network of the AAA application.

Figure 3-30 Example network of the AAA application



The preceding figure shows that the AAA function can be implemented on the MA5616 in the following three ways:

- The MA5616 functions as a local AAA server. In this case, the local AAA needs to be configured. The local AAA does not support accounting.
- The MA5616 functions as the client of a remote AAA server, and is connected to the HWTACACS server through the HWTACACS protocol, thus implementing the AAA.
- The MA5616 functions as the client of a remote AAA server, and is connected to the RADIUS server through the RADIUS protocol, thus implementing the AAA. The RADIUS protocol, however, does not support authorization.

Table 3-17 lists the differences between HWTACACS and RADIUS.

Table 3-17 Differences between HWTACACS and RADIUS

HWTACACS	RADIUS
Uses TCP to realize 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.

3.12.1 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 local authentication mode.
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
```

3.12.2 Configuring the Remote AAA (Based on the RADIUS Protocol)

The MA5616 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).
- Working principles 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 MA5616, 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 MA5616 and the RADIUS server. To make the essential parameters take effect, the RADIUS server group should be referenced in a certain domain.

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 quit the Authen 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 MA5616 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 MA5616 is in the normal state.
   - Make sure that the configuration of the RADIUS service port of the MA5616 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. (Optional) Run the **radius-server shared-key** command to configure the shared key of the RADIUS server.

   NOTE

   - The RADIUS client (MA5616) 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 5 seconds.

   The MA5616 sends the request packets to the RADIUS server. If the RADIUS server does not respond within the response timeout time, the MA5616 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 MA5616 considers that its communication with the RADIUS server is interrupted, and thus transmits the RADIUS request packets to another RADIUS server.

7. (Optional) 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 MA5616 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 common domain name for login cannot exceed 15 characters, and the domain name for 802.1x authentication 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 RADIUS protocol for authentication and accounting. The accounting interval is 10 minutes, the authentication password is a123456, RADIUS server 129.7.66.66 functions as the primary authentication and accounting server, and RADIUS server 129.7.66.67 functions as the standby authentication and accounting server. On the RADIUS 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-aaa)#quit
huawei(config)#radius-server template hwtest
huawei(config-radius-hwtest)#radius-server authentication 129.7.66.66 1812
huawei(config-radius-hwtest)#radius-server authentication 129.7.66.67 1812
secondary
huawei(config-radius-hwtest)#radius-server accounting 129.7.66.66 1813
huawei(config-radius-hwtest)#radius-server accounting 129.7.66.67 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
```

3.12.3 Configuring the Remote AAA (Based on the HWTACACS Protocol)

The MA5616 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 (MA5616) 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 MA5616 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 hwtacacs** 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 MA5616 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 MA5616 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 MA5616 is in the normal state.
   - Make sure that the HWTACACS server port of the MA5616 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 (MA5616) 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 MA5616 and the current HWTACACS server is considered 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 MA5616 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 common domain name for login cannot exceed 15 characters, and the domain name for 802.1x authentication 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 **radius-server template** 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 129.7.66.66 functions as the primary authentication, authorization, and accounting server, and HWTACACS server 129.7.66.67 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-aaa)#quit
huawei(config)#hwtacacs-server template hwtest
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 129.7.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 129.7.66.67
secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 129.7.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 129.7.66.67 secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 129.7.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 129.7.66.67 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
```

3.12.4 Configuration Example of the Authentication Based on the RADIUS Protocol (Device Management Users)

The MA5616 allows the management user of the device to log in to the system by preferring the RADIUS authentication mode. Local authentication can be used only when the RADIUS server is unreachable. This feature provides ISPs with flexible authentication strategies.

Prerequisites

- The route from the MA5616 to the RADIUS server must be configured.
- The management user information (user name@domain and password) must be configured on the RADIUS server.

Service Requirements

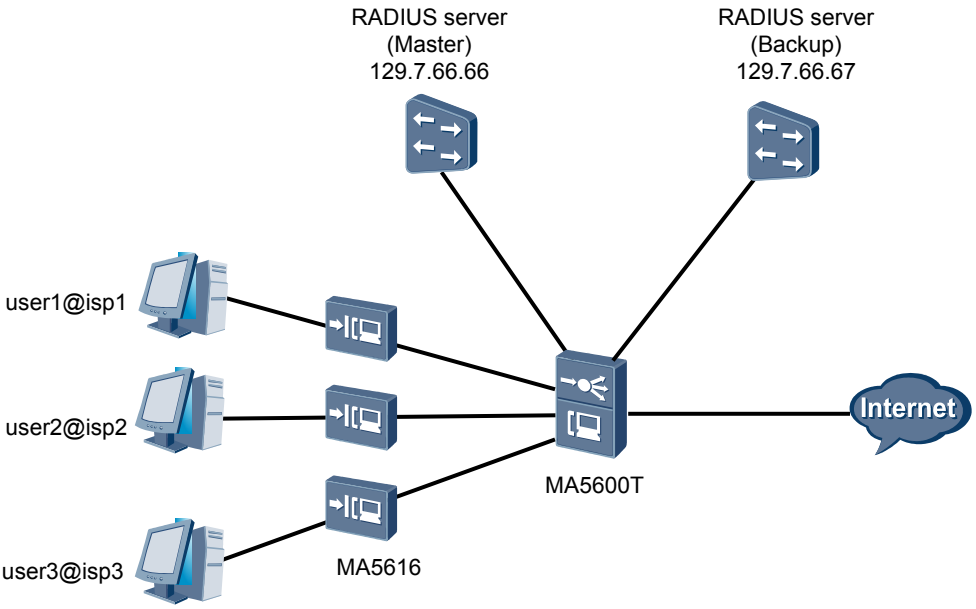
- Prefer the RADIUS server to authenticate management user of domain **isp1**.
- Local authentication can be used when the RADIUS server is unreachable.
- The user logs in to the server carrying the domain name.
- The RADIUS server with the IP address 129.7.66.66 functions as the primary server for authentication.

- The RADIUS server with the IP address 129.7.66.67 functions as the secondary server for authentication.
- The authentication port ID is 1812.
- Other parameters adopt the default settings.

Networking

Figure 3-31 shows the example network of RADIUS authentication.

Figure 3-31 Example network of RADIUS authentication



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **login-auth** (users are authenticated through RADIUS protocol).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme login-auth
huawei(config-aaa-authen-login-auth)#authentication-mode radius
huawei(config-aaa-authen-login-auth)#quit
huawei(config-aaa)#quit
```

Step 2 Configure the RADIUS protocol.

Create RADIUS server template named **test-login** with RADIUS server 129.7.66.66 as the primary authentication server, and RADIUS server 129.7.66.67 as the secondary authentication server.

```
huawei(config)#radius-server template test-login
huawei(config-radius-test-login)#radius-server authentication 129.7.66.66 1812
huawei(config-radius-test-login)#radius-server authentication 129.7.66.67 1812
secondary
huawei(config-radius-test-login)#quit
```

Step 3 Create a domain named **isp1**.

NOTE

- A domain is a group of users of the same type.
- When the user name is in the format of **userid@domain-name** (for example, **huawei20041028@isp1.net**), "domain-name" followed by "@" is the domain name, and "userid" is the user name used for authentication.
- The common domain name for login cannot exceed 15 characters, and the domain name for 802.1x authentication 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 RADIUS server template **test-login** to the user.

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 test-login
huawei(config-aaa-domain-isp1)#quit
```

Step 6 Configure the authentication mode of the management user.

In the global config mode, run the **terminal user authentication-mode** command to configure the authentication of the management user to remote AAA.

NOTE

- Only the **root** user can run this command.
- After the authentication of the management user is configured to remote AAA, the system prefers RADIUS authentication (the **root** user is still forcible local authentication).

```
huawei(config)#terminal user authentication-mode aaa isp1
```

Step 7 (Optional) Configure the local management user of the device.

If the RADIUS server is unreachable, local authentication can be used to log in to the system. If the RADIUS server is reachable, none of the management users can log in to the system through local authentication, except the **root** user.

CAUTION

Ensure that the user name and password of the local management user are the same as those specified on the RADIUS server. Otherwise, login to the system fails.

```
huawei(config)#terminal user name
  User Name(length<6,15>):user01       //Management user name:
user01
  User Password(length<6,15>):         //Password: test01pwd, same as that on the
RADIUS server
  Confirm Password(length<6,15>):
  User profile name(<=15 chars)[root]:
  User's Level:
     1. Common User  2. Operator  3. Administrator:2
```

```
  Permitted Reenter Number(0--4):4
  User's Appended Info(<=30 chars): aaa
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n
```

----End

Result

- When the RADIUS server is reachable, the management user can log in to the MA5616 through Telnet. After entering the user name and password specified on the RADIUS server, the management user can successfully log in to the MA5616.
- When the RADIUS server is unreachable:
  - If the local management user is configured through the **terminal user name** command, the management user can successfully log in to the MA5616 through Telnet by entering the user name and password specified on the RADIUS server.
  - If the local management user is not configured through the **terminal user name** command, the management user cannot log in to the MA5616 through Telnet by entering the user name and password specified on the RADIUS server.

Configuration File

```
aaa
authentication-scheme login-auth
authentication-mode radius
quit
quit
radius-server template test-login
radius-server authentication 129.7.66.66 1812
radius-server authentication 129.7.66.67 1812 secondary
quit
aaa
domain isp1
authentication-scheme login-auth
radius-server test-login
quit
quit
terminal user authentication-mode aaa test-login
terminal user name
test01
  User Password(length<6,15>):    //password test01pwd, same as that on the RADIUS
server
  Confirm Password(length<6,15>):
```

3.12.5 Configuration Example of the Authentication Based on the HWTACACS Protocol (Device Management Users)

The MA5616 allows the management user of the device to log in to the system by preferring the HWTACACS authentication mode. Local authentication can be used only when the HWTACACS server is unreachable. This feature provides ISPs with flexible authentication strategies.

Prerequisites

- The route from the MA5616 to the HWTACACS server must be configured.
- The management user information (user name@domain and password) must be configured on the HWTACACS server.

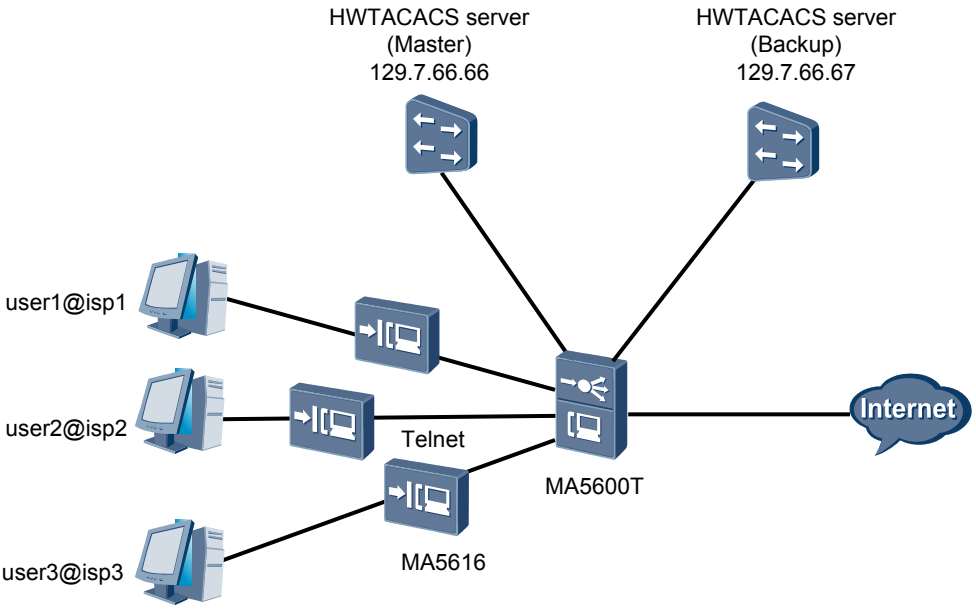
Service Requirements

- Prefer the HWTACACS server to authenticate management user of domain **isp1**.
- Local authentication can be used when the HWTACACS server is unreachable.
- The user logs in to the server carrying the domain name.
- The HWTACACS server with the IP address 129.7.66.66 functions as the primary server for authentication.
- The HWTACACS server with the IP address 129.7.66.67 functions as the secondary server for authentication.
- The authentication port ID is 1812.
- Other parameters adopt the default settings.

Networking

Figure 3-32 shows the example network of HWTACACS authentication.

Figure 3-32 Example network of HWTACACS authentication



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **login-auth** (users are authenticated through HWTACACS protocol).

```
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 **test-login** with HWTACACS server 129.7.66.66 as the primary authentication server, and HWTACACS server 129.7.66.67 as the secondary authentication server.

```
huawei(config)#hwtacacs-server template test-login
  Create a new HWTACACS-server template
huawei(config-hwtacacs-test-login)#hwtacacs-server authentication 129.7.66.66 1812
huawei(config-hwtacacs-test-login)#hwtacacs-server authentication 129.7.66.67 1812
secondary
huawei(config-hwtacacs-test-login)#quit
```

Step 3 Create a domain named **isp1**.

NOTE

- A domain is a group of users of the same type.
- When the user name is in the format of **userid@domain-name** (for example, **huawei20041028@isp1.net**), "domain-name" followed by "@" is the domain name, and "userid" is the user name used for authentication.
- The common domain name for login cannot exceed 15 characters, and the domain name for 802.1x authentication 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 **test-login** to the user.

You can use a HWTACACS server template in a domain only after the HWTACACS server template is created.

```
huawei(config-aaa-domain-isp1)#hwtacacs-server test-login
```

Step 6 Configure the authentication mode of the management user.

In the global config mode, run the **terminal user authentication-mode** command to configure the authentication of the management user to remote AAA.

NOTE

- Only the **root** user can run this command.
- After the authentication of the management user is configured to remote AAA, the system prefers RADIUS authentication (the **root** user is still forcible local authentication).

```
huawei(config)#terminal user authentication-mode aaa isp1
```

Step 7 (Optional) Configure the local management user of the device.

If the HWTACACS server is unreachable, local authentication can be used to log in to the system. If the HWTACACS server is reachable, none of the management users can log in to the system through local authentication, except the **root** user.

CAUTION

Ensure that the user name and password of the local management user are the same as those specified on the HWTACACS server. Otherwise, login to the system fails.

```
huawei(config)#terminal user name
  User Name(length<6,15>):user01       //Management user name:
user01
  User Password(length<6,15>):         //Password:
test01pwd
  Confirm Password(length<6,15>):
  User profile name(<=15 chars)[root]:
  User's Level:
     1. Common User  2. Operator  3. Administrator:2
  Permitted Reenter Number(0--4):4
  User's Appended Info(<=30 chars): aaa
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n
```

----End

Result

- When the HWTACACS server is reachable, the management user can log in to the MA5616 through Telnet. After entering the user name and password specified on the HWTACACS server, the management user can successfully log in to the MA5616.
- When the HWTACACS server is unreachable:
  - If the local management user is configured through the **terminal user name** command, the management user can successfully log in to the MA5616 through Telnet by entering the user name and password specified on the HWTACACS server.
  - If the local management user is not configured through the **terminal user name** command, the management user cannot log in to the MA5616 through Telnet by entering the user name and password specified on the HWTACACS server.

Configuration File

```
aaa
authentication-scheme login-auth
authentication-mode hwtacacs
quit
quit
hwtacacs-server template test-login
hwtacacs-server authentication 129.7.66.66 1812
hwtacacs-server authentication 129.7.66.67 1812 secondary
quit
aaa
domain isp1
authentication-scheme login-auth
hwtacacs-server test-login
quit
quit
terminal user authentication-mode aaa isp1
terminal user name
user1
  User Password(length<6,15>):      //Password test01pwd, same as that on the
HWTACACS server
  Confirm Password(length<6,15>):
```

3.13 Configuring the ACL for Packet Filtering

This topic describes the type, rule, and configuration of the ACL on the MA5616.

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 QoS or user security.

Table 3-18 lists the ACL types.

Table 3-18 ACL types

Type	Value Range	Feature
Basic ACL	2000-2999	The rules of a standard ACL are only defined according to the L3 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 TCP source port, TCP destination port, and 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.

When a packet reaches the port and matches two or more ACL rules, the matching sequence is as follows:

- If the rules of an ACL are activated at the same time, the rule configured earlier has priority over the one configured later.
- If the rules of an ACL are activated one by one, the rule activated later has priority over the one activated earlier.
- If the rules are issued to the port from different ACLs, the rule activated later has priority over the one activated earlier.

Precaution

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 DHCP module and IPoA module) . In this case, the hardware resources are limited and may be insufficient. To prevent the failure of enabling 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.

3.13.1 Configuring the Basic ACL for Packet Filtering

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 ACL is in the range of 2000-2999.

A basic ACL is only defined according to the L3 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.
- Perform the QoS operation. For details, see **Configuring Traffic Management Based on ACL Rules**.

----End

Example

To configure that from 00:00 to 12:00 on Fridays, port 0/1/0 on the MA5616 receives only the packets from 2.2.2.2, and discards 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 0/1/0
huawei(config)#save
```

3.13.2 Configuring the Advanced ACL for Packet Filtering

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 source port of the TCP, destination port of the TCP, and ICMP type of the data packets.

Context

The number of an advanced ACL is in the range of 3000-3999.

An advanced 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.
- Perform the QoS operation. For details, see **3.14.3 Configuring Traffic Management Based on ACL Rules**.

----End

Example

Assume that the service board of the MA5616 resides in slot 1 and belongs to a VLAN, and the IP address of the VLAN L3 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-adv-3001)rule 1 deny icmp destination 10.10.10.101 0
huawei(config-acl-adv-3001)rule 2 deny tcp destination 10.10.10.101 0 destination-
port eq telnet
huawei(config-acl-adv-3001)quit
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/1/0
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/1/0
huawei(config)#save
```

3.13.3 Configuring the Link Layer ACL for Packet Filtering

This topic describes how to classify traffic according to the link layer information such as source MAC address, source VLAN ID, L2 protocol type, and destination MAC address.

Context

The number of a link layer ACL is in the range of 4000-4999.

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 QoS operation. For details, see **3.14.3 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
```

3.14 Configuring QoS

This topic describes how to configure quality of service (QoS) on the MA5616 to provide end-to-end quality assurance for user services.

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 MA5616, 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, thus implementing QoS inside the system.

In addition to the preceding key points, the MA5616 supports 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 **3.13 Configuring the ACL for Packet Filtering**), and then QoS can be implemented for traffic streams.

3.14.1 Configuring Traffic Management

This topic describes how to configure traffic management on the MA5616.

Overview

The MA5616 supports traffic management for the inbound and outbound traffic streams of the system.

NOTE

For details on configuring traffic classification, see **5.4 Creating an xDSL Service Port**.

In addition, the MA5616 supports rate limit on the Ethernet port and traffic suppression on inbound broadcast packets and unknown (multicast or unicast) packets.

3.14.1.1 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 ip** 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 3-19 lists the traffic parameters defined in the IP traffic profiles.

Table 3-19 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 PIR: peak information rate PBS: peak burst size **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. It is recommended that you configure only CIR. ● The system marks the service packets with colors according to the four parameters. The red packet is discarded directly, and the packets of the other two colors are marked on their DEI field in the VLAN tag, the yellow color indicated as 1 and the green color indicated as 0.

Item	Parameter Description
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 upstream 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 upstream packet. ● user-tos: Copy the ToS priority in the packet to the 802.1p priority in the VLAN tag of the upstream packet.
Scheduling policies	There are two types of scheduling policies, which are available only to the downstream packet: ● 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.

NOTE

Upstream in this document refers to the direction from the user side to the network side, and downstream refers to the direction from the network side to the user side.

Procedure

Step 1 Run the **display traffic table ip** 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. If a proper traffic profile exists, select the profile by specifying the profile ID. If the existing traffic profiles do not meet the requirements, create a new IP traffic profile.

Step 2 Run the **traffic table ip** command to create a traffic profile.

For the usage and parameters of this command, see the description in the Command Reference in the related link. The following part describes only the key information in the configuration:

- 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 upstream 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 upstream packet.
- Keyword **priority-policy** must be entered to specify a scheduling policy for the downstream packet. For details about the scheduling policies, see **Table 3-19**.

Step 3 Run the **service-port** command to bind a proper traffic profile.

For the usage and parameters of this command, see the description in the Command Reference in the related link. The following part describes only the key information in the configuration:

- You need to enter parameters **rx-cttr** and **tx-cttr** and set values for the two parameters:
  - **rx-cttr**: Indicates the traffic ID in the connection receiving direction (from the network side to the user side). When you need to set the traffic profile in the connection receiving direction, use this parameter.
  - **tx-cttr**: Indicates the traffic ID in the connection transmitting direction (from the user side to the network side). When you need to set the traffic profile in the connection transmitting direction, use this parameter.
- (Optional) Enter keyword **traffic-table** to add or modify the traffic profile referenced by the service port.
- (Optional) Enter keyword **user-encap** to select the encapsulation type of the packets on the user side:
  - When the encapsulation type of the packets on the user side is IPoE, select **ipoe**.
  - When the encapsulation type of the packets on the user side is PPPoE, select **pppoe**.

----End

Example

Assume that the CIR is 2048 kbit/s, 802.1p priority of the upstream packet is 6, and the scheduling policy of the downstream 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        : -
  CTAG Mapping Priority: -
  CTAG Default Priority: 0
  Priority Policy      : tag-pri
  CIR                  : 2048 kbps
  CBS                  : 67536 bytes
  PIR                  : 4096 kbps
  PBS                  : 133072 bytes
  Color Mode           : color-blind
  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        : -
```

```
  CTAG Mapping Priority: -
  CTAG Default Priority: 0
  Priority Policy      : tag-pri
  CIR                  : 2048 kbps
  CBS                  : 67536 bytes
  PIR                  : 4096 kbps
  PBS                  : 133072 bytes
  Color Mode           : color-blind
  Referenced Status    : not used
  ------------------------------------------------
```

3.14.1.2 Configuring Rate Limitation on an Ethernet Port

This topic describes how to configure upstream 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 upstream rate limitation on a specified Ethernet port.

The main parameters are as follows:

- inbound: Indicates the input direction of a port.
- outbound: Indicates the output direction of a port.
- target-rate: Indicates the limited rate of the port, in the unit of kbit/s.
- port: Indicates the shelf 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 0/0/1 to 6400 kbit/s, do as follows:

```
huawei(config)#line-rate outbound 6400 port 0/0/1
huawei(config)#display qos-info line-rate port 0/0/1

line-rate:
port 0/0/1:
  Outbound:
      line rate: 6400 Kbps
```

3.14.1.3 Configuring User-based Rate Limitation

In the user-based rate limitation, the voice service, IPTV service, and Internet access service of each user share a total user bandwidth. When either of the services carries no traffic, the other

services can hold a burst of the total user bandwidth so that the total user bandwidth can be managed in a unified manner.

Context

The voice service, IPTV service, and Internet access service of each user share a total user bandwidth. The service with the highest class of service (CoS) priority is ensured first. When other services carry no traffic, the only service can hold a burst of the total user bandwidth. The multicast bandwidth is determined by the bandwidth of ordered programs. The total bandwidth of ordered programs cannot exceed the total user bandwidth. The voice service uses a fixed bandwidth.

Procedure

- 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 triple play 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 band width.

  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. Here, 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 band width.

   The CoS priorities of services are voice service, 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 ADSL port 0/2/0, a user is provided with the VoIP, IPTV, and Internet access services. Set the total user bandwidth to 10 Mbit/s (that is, set the downstream maximum rate to 10 Mbit/s in the channel configuration profile). 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 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 10
huawei(config-if-adsl-0/2)#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 0/2/0 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 0/2/0 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 0/2/0 vpi 0 vci 35 multi-service user-
vlan 40 rx-cttr 12 tx-cttr 12
huawei(config)#queue-scheduler strict-priority
```

3.14.1.4 Configuring Traffic Suppression

This topic describes how to configure traffic suppression. The purpose of traffic suppression is to ensure the provisioning of the normal service of system users by suppressing the broadcast, unknown multicast, and unknown unicast packets received by the system.

Context

Traffic suppression can be configured based on the port of a board.

Procedure

Step 1 Run the **interface eth** command to enter the ETH mode.

Step 2 Query the thresholds of traffic suppression.

Run the **display traffic-suppress all** command to check whether the thresholds of traffic suppression meets the service requirements.

Step 3 Run the **traffic-suppress** command to suppress the traffic of the port.

The main 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 2.

----End

Example

To suppress the broadcast packets according to traffic suppression level 8 on port 0 on the ETH board in slot 0/3, do as follows:

```
huawei(config)#interface eth 0/3
huawei(config-if-eth-0/3)#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                 7
        1                   7                   7                 7
        2                   7                   7                 7
        3                   7                   7                 7
        4                   7                   7                 7
        5                   7                   7                 7
        6                   7                   7                 7
        7                   7                   7                 7
```

```
  ------------------------------------------------------------------------
huawei(config-if-eth-0/3)#traffic-suppress all broadcast value 8
huawei(config-if-eth-0/3)#display traffic-suppress 0

  Command:
          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       :  8
  Current traffic suppression index of multicast       :  7
  Current traffic suppression index of unknown unicast :  7
  ------------------------------------------------------------------------
```

3.14.2 Configuring Queue Scheduling

This topic describes how to configure the queue scheduling so that the services with different priorities have different scheduling policies. Then, the corresponding QoS of these services can be ensured.

Context

The queue scheduling policy of the MA5616 is configured according to the service type. That is, the VoIP service priority is usually set to 6, the video service priority is usually set to 4, and the Internet service priority is usually set to 0. When congestion occurs, the system ensures that the traffic stream with a higher priority is processed in time, and also ensures the QoS of services with a lower priority.

3.14.2.1 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 MA5616 supports the three queue scheduling modes: strict-priority queue (PQ), weighted round robin (WRR), and PQ+WRR.

- PQ

  The PQ gives preference to packets in a queue with a higher priority. The packets of a lower priority queue can be transmitted only when a queue with a higher priority is empty.

  By default, the system adopts the PQ mode.

- WRR

The system supports WRR for eight queues. Each queue has a weight value (w7, w6, w5, w4, w3, w2, w1, and w0 in a descending order) for resource acquisition. In the WRR scheduling mode, the queues are scheduled in turn, which ensures that each queue can be scheduled.

Table 3-20 lists the mapping between the queue weights and the actual queues.

Table 3-20 Mapping between the queue weights and the actual queues

Queue Number	Configured Weight	Actual Queue Weight (Port Supporting Eight Queues)	Actual Queue Weight (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 the queues (except the queue with weight value 255) must be equal to 0 or 100, where 0 indicates that the strict PQ scheduling mode is used and 255 indicates that the queue is not used.

- PQ+WRR
  - The system schedules some queues by PQ and schedules the other queues by WRR. When the specified WRR value is 0, it indicates that the queue is scheduled in the PQ mode.
  - The queue scheduled in the PQ mode should be the queue that has the highest priority.
  - The weight sum of the scheduled queues 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 information about the queue scheduling mode.

----End

Example

To adopt the WRR scheduling mode and set the weight values of the eight queues to 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 adopt the PQ+WRR scheduling mode and set the weight values of the six queues to 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                     --
  ---------------------------------
```

3.14.2.2 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 3-21**.

Table 3-21 Mapping between the queue and the 802.1p priority

Queue Number	Actual Queue Number (Port Supporting Eight Queues)	Actual Queue Number (Port Supporting Four Queues)	802.1p Priority
7	7	3	7
6	6	3	6
5	5	2	5
4	4	2	4

Queue Number	Actual Queue Number (Port Supporting Eight Queues)	Actual Queue Number (Port Supporting Four Queues)	802.1p Priority
3	3	1	3
2	2	1	2
1	1	0	1
0	0	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
  ------------------------
```

3.14.2.3 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, thus 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 3-22** lists the default queue depths of the system.

Table 3-22 Queue depth allocation

Queue Number	Queue Depth (Port Supporting Eight Queues)	Actual Queue Number (Port Supporting Four Queues)
7	L7 (default: 6)	-
6	L6 (default: 25)	-
5	L5 (default: 12)	-
4	L4 (default: 12)	-
3	L3 (default: 13)	L7+L6 (default: 31)
2	L2 (default: 13)	L5+L4 (default: 24)
1	L1 (default: 6)	L3+L2 (default: 26)
0	L0 (default: 13)	L1+L0 (default: 18)

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

3.14.3 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.

3.14.3.1 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.

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 limit is 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.

Packets are discarded when the received traffic on a port exceeds the limit.

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, do as follows:

```
huawei(config)#traffic-limit inbound ip-group 2001 512 port 0/2/0
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: drop
```

3.14.3.2 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 match the specified priority. The priority tag type can be ToS or 802.1p.

Prerequisite

The ACL and the rule of the ACL are configured, and the port for traffic priority is working in the normal state.

Context

The traffic priority is only valid to permit rules of an ACL.

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 0/2/0, and the local priority of the traffic is 0 , do as follows:

```
huawei(config)#traffic-priority inbound ip-group 2001 local-precedence 0 port 0/2/0
huawei(config)#display qos-info traffic-priority port 0/2/0

traffic-priority:
port 0/2/0:
 Inbound:
   Matches: Acl 2001 rule 5  running
     Priority action: local-precedence 0
```

3.14.3.3 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, thus 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 0/0/1, do as follows:

```
huawei(config)#traffic-statistic inbound ip-group 2001 port 0/0/1
```

```
huawei(config)#display qos-info traffic-statistic port 0/0/1

traffic-statistic:
port 0/0/1:
 Inbound:
   Matches: Acl 2001 rule 5     running
     0 packet
```

3.14.3.4 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 mirror is 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 0/2/0 to port 0/0/1, do as follows:

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/2/0 to port 0/0/1
huawei(config)#display qos-info traffic-mirror port 0/2/0

traffic-mirror:
port 0/2/0:
 Inbound:
   Matches: Acl 2001 rule 5     running
   Mirror to: port 0/0/1
```

3.15 Configuring Environment Monitoring

This topic provides concepts associated with environment monitoring and describes how to configure environment monitoring on the MA5616.

3.15.1 Configuring Monitoring Through the ESC

This topic describes how to configure the H831VESC and the MiniESC on the MA5616.

3.15.1.1 Configuring the Monitoring Through the H831VESC

You can monitor the environment status of the MA5616 through its built-in virtual EMU H831VESC. This topic describes how to configure the H831VESC.

Context

- The H831VESC is a built-in virtual EMU of the control board on the MA5616, and the ALARM port on the control board is connected to the external sensor through a cable such as a environment monitoring cable.
- The EMU ID of the H831VESC, and the ID of its subnode connected to the shelf are default settings in the system. Therefore, you cannot change them.
- The H831VESC supports four digital parameters, all of which can be defined by users. Among the four digital parameters,
  - Digital parameter 0: Empty by default.
  - Digital parameter 1: Indicates the cabinet door by default.
  - Digital parameter 2: Indicates the lightning arrester by default.
  - Digital parameter 3: Indicates the MDF by default.

  By default, the valid levels of default digital parameters are all high levels.

Procedure

Step 1 Query the status of the H831VESC.

Run the **display emu** command to query the status of the H831VESC.

Step 2 Configure the digital parameters.

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

Step 3 Query the environment information about the H831VESC.

Run the **display esc environment info** command to query the environment information about the H831VESC.

Step 4 Save the data.

Run the **quit** command to quit the H831VESC mode, and then run the **save** command to save the data.

----End

Result

After the configuration, the H831VESC works in the normal state and monitors the digital parameters set on the MA5616. When the actual level of a monitored digital parameter is different from the valid level preset in the system, the MA5616 reports an alarm.

Example

Table 3-23 shows the parameter plan for configuring the H831VESC.

Table 3-23 Data plan for configuring the H831VESC

Item	Data	Remarks
Digital parameters	Digital parameter ID: 0	In the F01S50 and F01S100 cabinets, digital parameter 0 is used to monitor the temperature. In the F01E50 cabinet, digital parameter 0 does not take effect.
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the MA5616 does not report an alarm in the case of low level.
	Name of digital parameter 0: Temperature	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the temperature sensor is set to monitor the temperature.
	User-defined alarm ID of digital parameter 0: 5	When the temperature in the cabinet is between 67°C and 73°C, the MA5616 reports an alarm. The meanings of the alarm IDs are as follows: 0: smoke ; 1: door; 2: arrester; 3: wiring; 4: the AC power is off; 5: digital user-defined alarm
	Digital parameter ID: 1	In the F01S50, F01S100, and F01E50 cabinets, digital parameter 1 is used to monitor door status.
	Valid level of digital parameter 1: high level	When the high level represents the valid level, the MA5616 does not report an alarm in the case of high level.
	Name of digital parameter 1: Door	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the door sensor is set to monitor the door status.
	User-defined alarm ID of digital parameter 1: 1	When the cabinet door is open, the MA5616 reports an alarm.
	Digital parameter ID: 2	In the F01S50, F01S100, and F01E50 cabinets, digital parameter 2 is used to monitor the lightning arrester.
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the MA5616 does not report an alarm in the case of low level.

Item	Data	Remarks
	Name of digital parameter 2: Arrester	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the lightning arrester status sensor is set to monitor the arrester status.
	User-defined alarm ID of digital parameter 2: 2	When the lightning arrester is faulty, the MA5616 reports an alarm.
	Digital parameter ID: 3	In the F01S50 cabinet, digital parameter 3 does not take effect. In the F01S100 cabinet, digital parameter 3 is used to monitor the MDF.
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the MA5616 does not report an alarm in the case of low level.
	Name of digital parameter 3: Fan	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the fan status sensor is set to monitor the fan status.
	User-defined alarm ID of digital parameter 3: 5	When the fan is faulty, the MA5616 reports an alarm.

```
huawei(config)#display emu 0

  EMU ID: 0
  ------------------------------------------------------------------------------
  EMU name    : H831VESC
  EMU type    : H831VESC
  Used or not : Used
  EMU state   : Normal
  Frame ID    : 0
  Subnode     : 1
  COM port    : -
  ------------------------------------------------------------------------------
huawei(config)#interface emu 0
huawei(config-if-h831vesc-0)#esc digital 0 available-level low-level digital-alarm
5 name Temperature
huawei(config-if-h831vesc-0)#esc digital 1 available-level high-level digital-
alarm 1 name Door
huawei(config-if-h831vesc-0)#esc digital 2 available-level low-level digital-alarm
2 name Arrester
huawei(config-if-h831vesc-0)#esc digital 3 available-level low-level digital-alarm
5 name Fan
huawei(config-if-h831vesc-0)#display esc environment info
  EMU ID: 0                          ESC environment state
  ---------------------------Digital environment info-------------------------
  ID Name                State  Value |ID Name                State  Value
  0  Temperature         Normal 0     |1  Door                Alarm  0
  2  Arrester            Normal 0     |3  Fan                 Normal 0
  ------------------------------------------------------------------------------
huawei(config-if-h831vesc-0)#quit
huawei(config)#save
```

3.15.1.2 Configuring the Monitoring Through the ESCM

The ESCM is an EMU that integrates the environment monitoring board, terminal blocks, and DIP switches. The ESCM monitors the environment parameters such as smoke, water, door status, wiring, temperature, and humidity of the device, and also provides extended monitoring ports. This topic provides the basic information about the ESCM and describes how to configure analog and digital parameters of the ESCM.

Prerequisites

- The ESCM must be connected to the ESC port of the control board on the MA5616 through a straight-through cable.
- The setting of the hardware DIP switch on the ESCM must be the same as the configured EMU subnode ID.

  NOTE

  For details about the settings of DIP switches, see ESCM EMU.
- The sixth DIP switch on the ESCM must be set to on, which indicates that the baud rate is 19200 bit/s.

Context

- The differences between an analog parameter and a digital parameter are as follows:
  - An analog parameter is a consecutive parameter, such as the temperature, voltage, and current.
  - A digital parameter is a discrete value that indicates a state.
- The ESCM requires an RS-485 serial port for data communication.
- In the case of the ESCM, the system supports the following analog and digital parameters:
  - Analog parameters 0-1: invariably allocated by the system. You cannot modify any parameter in these two analog parameters, except the upper and lower alarm thresholds.
  - Analog parameters 2-3: user-defined.
  - Digital parameters 0, 1, 8, and 9: invariably allocated by the system. You cannot modify any parameter in these digital parameters, except the valid level.

    NOTE

    Digital parameter 9 **Water_Alarm**: unavailable.
  - Digital parameters 2-7: user-defined.

Mapping Between Monitoring Parameters and Device Ports

Table 3-24 describes the mapping between the monitoring parameters displayed on the host and the ports on the ESCM.

Table 3-24 Mapping between the monitoring parameters displayed on the host and the ports on the ESCM

Monitoring Parameter on Host	Device Port
Temperature	Temperature
Input_-48V_0	Voltage

Monitoring Parameter on Host	Device Port
Analog 2	N/A
Analog 3	N/A
Wiring	JTP1 (MDF)
Door0	JTM1 (door status)
Digital 2	JTD1
Digital 3	JTD2
Digital 4	JTD3
Digital 5	JTD4
Digital 6	JTD5
Digital 7	JTD6
Smoke	JTD7 (smoke)
Water_Alarm	JTS1 (water)

NOTE

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

Procedure

Step 1 Add an EMU.

Run the **emu add** command to add an EMU to monitor the environment parameters of the device so that the device runs in a stable environment.

The EMU ID is 3, the type is ESCM (MiniESC on the CLI), the subnode ID is 8, and the serial port type isRS485.

Step 2 Configure the analog parameters.

Run the **esc analog** command to configure the upper/lower alarm thresholds and measurement thresholds, thus supporting the real-time monitoring of the device through the analog parameters.

Step 3 Configure the digital parameters.

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

Step 4 Query the environment information about the ESCM.

Run the **display esc environment info** command to query the environment information about the ESCM.

Step 5 Save the data.

Run the **quit** command to quit the miniesc mode, and then run the **save** command to save the data.

----End

Result

After the configuration, the ESCM works in the normal state and monitors the analog and digital parameters set on the MA5616.

- When an analog parameter measured is not within the upper and lower alarm thresholds preset in the system, the MA5616 reports an alarm.
- When the actual level of a monitored digital parameter is different from the valid level preset in the system, the MA5616 reports an alarm.

Example

Table 3-25 shows the data plan for configuring the ESCM.

Table 3-25 Data plan for configuring the ESCM

Item	Data	Remarks
EMU	Type: ESCM (MiniESC)	The ESCM is displayed as **MiniESC** on the CLI.
	SN: 3	-
	Subnode ID: 8 **NOTE** The hardware DIP switch on the ESCM ranges from 0–15 and therefore the subnode ID ranges from 0–15. Ensure that the hardware DIP switch on the ESCM is set the same as that of the EMU subnode on the device. This topic uses value 8 as an example.	The hardware DIP switch on the ESCM is set to 8.
Analog parameters	Analog parameter ID: 0	This analog parameter is set according to the actual requirements. The built-in analog parameter is set here to monitor the ambient temperature of the device. For values and details of this parameter, see the **esc analog** command.
	Upper alarm threshold of analog parameter 0: 54°C	When the ambient temperature of the device is higher than 54°C, the device reports an alarm.
	Lower alarm threshold of analog parameter 0: 6°C	When the ambient temperature of the device is lower than 6°C, the device reports an alarm.

Item	Data	Remarks
	Analog parameter ID: 2	The user-defined humidity monitoring analog parameter is added to monitor the ambient humidity of the device. For values and details of this parameter, see the **esc analog** command.
	Upper alarm threshold of analog parameter 2: 75% RH	When the ambient humidity of the device is higher than 75% RH, the device reports an alarm.
	Lower alarm threshold of analog parameter 2: 5% RH	When the ambient humidity of the device is lower than 5% RH, the device reports an alarm.
	Name of analog parameter 2: humidity	-
	Alarm ID of analog parameter 2: 2	The user-defined humidity alarm of the system is used.
	Unit of analog parameter 2: % RH	-
	Sensor type of analog parameter 2: voltage type	-
Digital parameters	Digital parameter ID: 1	This parameter is invariably allocated by the system, and is used to monitor the door status of the telecommunications room. You cannot modify any parameter of this digital parameter, except the valid level.
	Valid level of digital parameter 1: high level	When the high level represents the valid level, the device does not report an alarm in the case of high level.
	Digital parameter ID: 2	-
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the device does not report an alarm in the case of low level.
	Name of digital parameter 2: Fan	It is a user-defined digital parameter and is set according to the actual requirements. The monitoring digital parameter of the fan unit is set here to monitor the fan unit.

Item	Data	Remarks
	User-defined alarm ID of digital parameter 2: 6	When the fan unit is faulty, the device reports an alarm. The meanings of the alarm IDs are as follows: 1: AC voltage; 2: AC switch; 3: battery voltage; 4: battery fuse; 5: load fuse; 6: rectifier module; 7: DC power; 8: room door; 9: thief; 10: wiring ; 11: fan; 12: fire; 13: fog; 14: power supply; 15: water; 16: diesel; 17: smell 18: air-condition; 19: arrester; 20: DC voltage; 21 output switch; 22: digital user-defined alarm

```
huawei(config)#emu add 3 MINIESC 0 8 RS485 MiniESC
huawei(config)#interface emu 3
huawei(config-if-miniesc-3)#esc analog 0 alarm-upper-limit 54 alarm-lower-limit 6
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-miniesc-3)#
  Execute command successful
huawei(config-if-miniesc-3)#esc analog 2 alarm-upper-limit 75 alarm-lower-limit
5 name humidity sensor-type 0:voltage analog-alarm 2 unit %RH
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-miniesc-3)#
  Execute command successful
huawei(config-if-miniesc-3)#esc digital 1 available-level high-level
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-miniesc-3)#
  Execute command successful
huawei(config-if-miniesc-3)#esc digital 2 available-level low-level
digital-alarm 11 name Fan
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-miniesc-3)#
  Execute command successful
huawei(config-if-miniesc-3)#display esc environment info
  EMU ID: 3                          ESC environment state
  ---------------------------Analog environment info--------------------------
  ID Name                State    Value   AlmUpper   AlmLower   Unit
  0  Temperature         Normal   30.00      54         6        C
  1  Input_-48V_0        Normal   54.00      60         45       Volt
  2  Humidity            Low      -128.00    75         5        %RH
  3  -                   Normal   -128.00    127        -128     -
  ---------------------------Digital environment info-------------------------
  ID Name                State  Value |ID Name                State  Value
  0  Wiring              Normal 1     |1  Door0               Alarm  0
  2  Fan                 Normal 0     |3  -                   Normal 1
  4  -                   Normal 1     |5  -                   Normal 1
  6  -                   Normal 1     |7  -                   Normal 1
  8  Fog                 Normal 1     |9  Water_Alarm         Normal 1
  ------------------------------------------------------------------------------

huawei(config-if-miniesc-3)#quit
huawei(config)#save
```

3.15.2 Configuring Monitoring Through the Power System

This topic describes how to configure the Power4830 and H831PMU on the MA5616.

3.15.2.1 Configuring the Monitoring Through the EPS30-4815AF

The EPS30-4815AF system converts the input 220 VAC into the -48 VDC to provide the -48 VDC power. In addition, the EPS30-4815AF system can manage one VRLA battery set and monitor other environment parameters through its EPMU03 monitoring module. This topic provides the basic information about the EPS30-4815AF and describes how to configure data associated with environment monitoring.

Prerequisites

- The EPS30-4815AF must be connected to the ESC port of the control board on the MA5616 through a straight-through cable.
- The setting of the hardware DIP switch on the EPS30-4815AF must be the same as the setting of the EMU subnode in the environment configuration.
- The sixth DIP switch on the EPS30-4815AF must be set to off, which indicates that the baud rate is 19200 bit/s.

Context

- The differences between an analog parameter and a digital parameter are as follows:
  - An analog parameter is a consecutive parameter, such as the temperature, voltage, and current.
  - A digital parameter is a discrete value that indicates a state.
- The EPS30-4815AF requires an RS-485 serial port for data communication.

Mapping Between Monitoring Parameters and Device Ports

Table 3-26 describes the mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box.

Table 3-26 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter on 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 digital monitoring parameter, make sure that the port corresponding to this analog or digital monitoring parameter is properly connected with an environment monitoring cable.

Procedure

Step 1 Add the EPS30-4815AF, namely, Power4830.

Run the **emu add** command to add the Power4830.

Step 2 In the environment monitoring configuration mode, run the **display power system parameter** command to query the default configuration.

Step 3 Configure the parameters of the lead battery.

Run the **power battery parameter** command to configure battery parameters, including battery management parameters, charging parameters and battery set power-off parameters, and battery high-temperature power-off parameters. You can also use the default settings.

Step 4 Configure the parameter of the rectifier unit.

Run the **power module-num** command to configure the parameter of the rectifier unit.

Step 5 Configure the environment parameters for power supply monitoring.

Run the **power environment** command to configure the upper and lower alarm thresholds and measurement thresholds of temperature or humidity for power monitoring. In this manner, the power module generates alarms when it works in a condition that does not meet the present requirements.

Step 6 Configure the external extended digital parameter for power supply monitoring.

Run the **power outside_digital** command to configure the external extended digital parameter for power supply monitoring.

Step 7 Query configuration parameters and environment parameters of the power system.

Run the **display power system parameter** command to query configuration parameters of the power monitoring unit.

Step 8 Run the **display power alarm** command to query the alarm. Ensure that no alarm (except the door status alarm) for the monitoring parameter is generated.

Step 9 Save the data.

Run the **quit** command to quit the Power4830 mode, and then run the **save** command to save the data.

----End

Result

After the configuration, the EPS30-4815AF works in the normal state and monitors parameters set on the MA5616. When a monitored parameter is abnormal, the MA5616 reports an alarm.

Example

Table 3-27 provides the data plan for configuring the power monitoring through the EPS30-4815AF.

Table 3-27 Data plan for configuring the power monitoring through the EPS30-4815AF

Item	Data	Remarks
EMU	Type: Power4830 (Pwr4830)	The selected type of the EPS30-4815AF is Power4830 (Pwr4830).
	SN: 2	-
	Subnode ID: 4 **NOTE** The hardware DIP switch on the EPS30-4815AF ranges from 0–31 and therefore the subnode ID ranges from 0–31. Ensure that the hardware DIP switch on the EPS30-4815AF is set the same as that of the EMU subnode on the device. This topic uses value 4 as an example.	The DIP switch on the EPS30-4815AF is set to 4.
Battery management parameters	Current-limiting coefficient for battery charging: 0.15	You can change the configuration by running the **power battery** command according to the actual requirements. The MA5616 can be installed in the F01E2OOE, F01E400, or F01S300 cabinet. A 26 AH battery set is configured for the F01E200E cabinet, a 75 AH battery set is configured for the F01E400 cabinet, and a 50 or 92 AH battery set is configured for the F01S300 cabinet. **NOTE** When a 92 AH battery set is configured for the F01S300 cabinet, the charging current-limiting coefficien of the battery must be set to 0.1.
	Interval of battery equalized charging: 60 days	
	Number of battery sets: 1	
	Capacity of the battery set: 75AH	
	Upper measurement threshold of the battery set temperature: 80°C	
	Lower measurement threshold of the battery set temperature: -20° C	
	Upper alarm threshold of the battery set temperature: 50°C	
	Lower alarm threshold of the battery set temperature: 0°C	
	Temperature compensation coefficient of the battery set: 80 mV	
Charging parameters of the battery	Charging mode of the battery: automatic	In this topic, the default settings are adopted. You can run the **power charge** command to modify parameters according to actual conditions.
	Equalized charging voltage of the battery: 56.5 V	
	Float charging voltage of the battery: 53.5 V	

Item	Data	Remarks
Battery set power-off parameters	Battery set power-off permission status: permit	You can change the configuration by running the **power charge** command according to the actual requirements.
	Battery set power-off voltage: 43 V	
High-temperature power-off parameters of the battery	Battery high-temperature power-off permission status: forbid	You can change the configuration by running the **power charge** command according to the actual requirements.
	Temperature for battery high-temperature power-off: 53°C	
Rectifier unit parameter	Number of rectifier units: 2	The EPS30-4815AF supports up to two rectifier units.
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C	You can change the configuration by running the **power environment** command according to the actual requirements.
	Lower alarm threshold of the temperature: -5°C	
	Upper measurement threshold of the temperature: 80°C	
	Lower measurement threshold of the temperature: -20°C	
	Upper alarm threshold of the humidity: 80% RH	
	Lower alarm threshold of the humidity: 10% RH	
	Upper measurement threshold of the humidity: 100% RH	
	Lower measurement threshold of the humidity: 0% RH	
External extended digital parameter of the power	Extended digital parameter ID: 1	-
	Valid level of extended digital parameter 1: low level	When the low level represents the valid level, the device does not report an alarm in the case of low level.
	Name of extended digital parameter 1: Fan	It is a user-defined digital parameter and is set according to the actual requirements. The monitoring digital parameter of the fan status sensor is set to monitor the fan status.

Item	Data	Remarks
	User-defined alarm ID of extended digital parameter 1: 11	When the fan is faulty, the MA5616 reports an alarm. The meanings of the alarm IDs are as follows: 1: AC voltage; 2: AC switch; 3: battery voltage; 4: battery fuse; 5: load fuse; 6: rectifier; 7: DC power; 8: room door; 9: thief; 10: wiring ; 11: fan; 12: fire; 13: smoke; 14: power supply; 15: water; 16: diesel; 17: smell 18: air-condition; 19: arrester; 20: DC voltage; 21 output switch; 22: digital user-defined alarm
	Extended digital parameter ID: 3	-
	Valid level of extended digital parameter 3: low level	When the low level represents the valid level, the device does not report an alarm in the case of low level.
	Name of extended digital parameter 3: SPD	It is a user-defined digital parameter and is set according to the actual requirements. The monitoring digital parameter of the SPD status sensor is set to monitor the SPD status.
	User-defined alarm ID of extended digital parameter 3: 19	When the lightning arrester is faulty, the MA5616 reports an alarm.

```
huawei(config)#emu add 2 POWER4830 0 4 RS485 POWER4830
huawei(config)#interface emu 2
huawei(config-if-power4830-2)#display power system parameter
  EMU ID: 2                          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
  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 : 2
  module 0 address: 1   module 0 switch state   : On
  module 1 address: 2   module 1 switch state   : On
  Battery high-temperature-off permit     : Forbid
  Battery high-temperature-off temperature: 53 C
  ------------------------------------------------------------------------------
huawei(config-if-power4830-2)#display power environment parameter

  EMU ID: 2                          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        Available Level|DigitalID Name        Available Level
     0     -                     1     |   1     -                     1
     2     -                     1     |   3     -                     1
     4     -                     1     |   5     -                     1
     6     -                     1
  ------------------------------------------------------------------------------
huawei(config-if-power4830-2)#power battery parameter 1 0.15 60 75
huawei(config-if-power4830-2)#power module-num 2
huawei(config-if-power4830-2)#power temperature-off battery-off-state permit
huawei(config-if-power4830-2)#power environment humidity 80 10 100 0
  This command is invalid unless in the condition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-power4830-2)#power environment temperature 68 -5 80 -20
  This command is invalid unless in the condition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-power4830-2)#power outside_digital 1 available-level low-level
digital_alarm 11 name Fan
huawei(config-if-power4830-2)#power outside_digital 3 available-level low-level
digital_alarm 19 name SPD
huawei(config-if-power4830-2)#display power system parameter

  EMU ID: 2                            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
  battery temperature test upper :  80C  battery temperature test lower: -20C
  temperature redeem quotiety    : 80mV
  battery temperature alarm upper:  50C  battery temperature alarm lower: 0C
  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 : 2
  module 0 address: 1   module 0 switch state   : On
  module 1 address: 2   module 1 switch state   : On
  Battery high-temperature-off permit     : Permit
  Battery high-temperature-off temperature: 53 C
  ------------------------------------------------------------------------------
huawei(config-if-power4830-2)#display power environment parameter

  EMU ID: 2                            Power environment configuration 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     available Level   |DigitalID Name     available Level
     0     -                     1     |   1     Fan                   0
     2     -                     1     |   3     SPD                   0
     4     -                     1     |   5     -                     1
     6     -                     1
  ------------------------------------------------------------------------------
huawei(config-if-power4830-2)#display power alarm
  EMU ID: 2                            Power alarm information
  ------------------------------------------------------------------------------
  Mains supply yes : yes            Mains supply lack : normal
  Total vol lack   : Normal
  Load fuse 0      : Connect
  Load off         : on             battery off       : on
  Battery 1 loop   : connect
  Environment Temperature : Normal         Environment Humidity    : Normal
  Door alarm       : Alarm          Water alarm                  : Normal       //
The "Door alarm" alarm is generated because the door of the cabinet is not closed.
  Fog alarm        : Normal         Battery Temperature alarm      : Normal
  Wiring alarm     : Normal         Acinput air switch             : Normal
  Battery 1 Temp-Sensor     : Invalid  Environment 1 Temp-Sensor     : Invalid
  Environment Humidity-Sensor : Invalid
```

```
  module 0         : normal
  module 1         : normal
    ------------------------------------------------------------------------------
  DigitalID Name             Alarm State|DigitalID Name            Alarm State
     0     -                 Normal  |   1     Fan                  Normal
     2     -                 Normal  |   3     SPD                  Normal
     4     -                 Normal  |   5     -                    Normal
     6     -                 Normal
    ------------------------------------------------------------------------------
huawei(config-if-power4830-2)#quit
huawei(config)#save
```

3.15.2.2 Configuring the Monitoring Through the H831PMU (Backup Power Using the VRLA Battery)

The H831PMU is a power monitoring control module and it works with the PAIB power board to monitor relevant information about the power system. In addition, the H831PMU can manage a VRLA battery set. This topic provides the basic information about the H831PMU and describes how to configure data associated with environment monitoring.

Context

The H831PMU requires an RS-485 serial port for data communication.

Procedure

Step 1 Run the **emu add** command to add an environment monitoring unit (EMU).

Step 2 Configure the battery management parameters.

Run the **power battery parameter** command to configure battery parameters, such as charging current-limiting coefficient, timed equalized charging time, number of battery sets, and capacity of the battery set.

Step 3 Configure the battery charging parameters.

Run the **power charge** command to configure the battery charging mode and the equalized charging voltage or floating charging voltage to charge the battery.

Step 4 Run the **power off** command to configure the power supply load power-off and battery set power-off parameters.

Step 5 Run the **power supply-parameter** command to configure the power distribution parameters.

Step 6 Run the **display power system parameter** command to query the configuration parameters of the power system.

Step 7 Save the data.

Run the **quit** command to quit the H831PMU mode, and then run the **save** command to save the data.

----End

Result

After the configuration is completed, the H831PMU works in the normal state and monitors parameters set on the MA5616. When a monitored parameter is abnormal, the MA5616 reports an alarm.

Example

Table 3-28 provides the data plan for configuring the power monitoring through the H831PMU.

Table 3-28 Data plan for configuring the power monitoring through the H831PMU

Item	Data	Remarks
EMU	Type: H831PMU	-
	SN: 3	-
	Subnode ID: 0	-
Battery management parameters	Number of battery sets: 1	For values and details of the parameters, see the **power battery** command.
	Current-limiting coefficient for battery charging: 0.15	
	Interval of battery equalized charging: 90 days	
	Capacity of the battery set: 12 AH	
Charging parameters of the battery	Charging mode of the battery: floating	For values and details of the parameters, see the **power charge** command. When setting the equalized and float charging voltages 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.
	Equalized charging voltage of the battery: 56.8 V	
	Float charging voltage of the battery: 53.5 V	
Battery set power-off parameters	Battery set power-off permission status: permit	For values and details of the parameters, see the **power off** command.
	Battery set power-off voltage: 44 V	
Power distribution parameters	DC overvoltage alarm threshold: 59 V	For values and details of the parameters, see the **power supply-parameter** command.
	DC undervoltage alarm threshold: 48 V	

```
huawei(config)#emu add 3 H831PMU 0 0 RS485
huawei(config)#interface emu 3
huawei(config-if-h831pmu-3)#power battery parameter 1 0.15 90 12
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-h831pmu-3)#
  Execute command successful
huawei(config-if-h831pmu-3)#power charge mode floating
  Send command to environment monitor board ,please waiting for the ack
```

```
huawei(config-if-h831pmu-3)#
  Execute command successful
huawei(config-if-h831pmu-3)#power charge voltage equalizing-voltage 56.8 floating-
voltage 53.5
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-h831pmu-3)#
  Execute command successful
huawei(config-if-h831pmu-3)#power off battery-off-state permit battery-off-voltage
44
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-h831pmu-3)#
  Execute command successful
huawei(config-if-h831pmu-3)#power supply-parameter 59 48
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-h831pmu-3)#
  Execute command successful
huawei(config-if-h831pmu-3)#display power system parameter

  EMU ID: 3                          Power system information
  ---------------------------------------------------------------------------
  Charge control state: Remote control
  Equalizing voltage  : 56.80V      Floating voltage      : 53.50V
  Charge Lmt quotiety : 0.15        Equalizing time       : 90 days
  Battery number      : 1           Battery 0 capacity    : 12  AH
  Battery off permit  : Permit      Battery off voltage   : 44.00V
  DC over alarm volt  : 59 V        DC lack alarm voltage : 48 V
  Power-cut-close-Broad-service : On
  ---------------------------------------------------------------------------
huawei(config-if-h831pmu-3)#quit
huawei(config)#save
```

3.15.2.3 Configuring the Monitoring Through the EPS30-4815AF (Backup Power Using the PBL 02A Fe-lithium Battery)

The EPS30-4815AF can convert the 220 V AC power into the -48 V DC power to provide the -48 V DC power. In addition, the EPS30-4815AF can manage a Fe-lithium battery set. This topic describes how to configure the power monitoring through the EPS30-4815AF (backup power using the Fe-lithium battery).

Prerequisites

- The setting of the hardware DIP switch on the EPS30-4815AF must be the same as the setting of the EMU subnode in the environment configuration.
- The sixth DIP switch on the EPS30-4815AF must be set to off, which indicates that the baud rate is 19200 bit/s.
- The EPS30-4815AF must be connected to the ESC port on the control board of the MA5616 through a straight-through cable.
- The Fe-lithium battery must be connected to the serial port on the MA5616 through a 1-in-2-out cable.

Context

The MA5616 supports a Fe-lithium battery set for power backup. Compared with the lead-acid battery, the Fe-lithium battery features long lifespan, large capacity, optimized discharging function, fast charging, and flexible environment adaptability. In addition, it supports intelligent management so that the battery can be automatically charged or discharged.

The Fe-lithium battery is connected to the input port of the power system through a power cable and connected to the MA5616 through an RS485 serial port cable. When detecting a Fe-lithium battery, the MA5616 issues a command to the power system to adjust the voltage. The charging mode of a Fe-lithium battery is the equalizing mode.

When the mains supply fails, the Fe-lithium battery provides power for the MA5616 to ensure the normal running of the device in a certain period. When the mains supply recovers, the Fe-lithium battery stops discharging and starts charging.

Procedure

Step 1 Add the EPS30-4815AF, namely, Power4830.

Run the **emu add** command to add the Power4830.

Step 2 Configure the parameter of the rectifier unit.

Run the **power module-num** command to configure the parameter of the rectifier unit.

Step 3 Configure the environment parameters for power supply monitoring.

Run the **power environment** command to configure the upper and lower alarm thresholds and measurement thresholds of temperature or humidity for power monitoring. In this manner, the power module generates alarms when it works in a condition that does not meet the present requirements.

Step 4 Configure the external extended digital parameter for power supply monitoring.

Run the **power outside_digital** command to configure the external extended digital parameter for power supply monitoring.

Step 5 Query configuration parameters and environment parameters of the power system.

Run the **display power system parameter** command to query configuration parameters of the power monitoring unit.

Step 6 Run the **display power alarm** command to query the alarm. Ensure that no alarm (except the door status alarm) for the monitoring parameter is generated.

Step 7 Save the data.

Run the **quit** command to quit the Power4830 mode, and then run the **save** command to save the data.

Step 8 Configure the Fe-lithium battery monitoring unit.

1. Run the **emu add** command to add a Fe-lithium battery monitoring unit.
2. (Optional) Run the **power batteryinstall** command to set the time for installing the battery.
3. Run the **display power run info** command to query the battery running information, such as the charging status and remaining power.
4. (Optional) Run the **display power batteryinstalltime** command to query the time for installing the battery.
5. Run the **save** command to save the data.

   NOTE

   The subnode ID of the Fe-lithium battery is invariably 23.

----End

Example

Assume that:

- The EMU ID of the Power4830 is 2 and the subnode ID is 4.
- The number of rectifier modules is 2.
- The environment parameters of the power monitoring are as follows: The upper temperature alarm threshold is 68°C; the lower temperature alarm threshold is -5°C; the upper test temperature threshold is 80°C; the lower test temperature threshold is -20°C; the upper humidity alarm threshold is 80% RH; the lower humidity alarm threshold is 10% RH; the upper test humidity threshold is 100% RH; the lower humidity test threshold is 0% RH.
- The EMU ID of the Fe-lithium battery is 4 and the subnode ID is 23.
- The time for installing the battery is 2010-08-20.

To configure the power monitoring through the Power4830 (backup power using the Fe-lithium battery) with such configurations, do as follows:

```
huawei(config)#emu add 2 POWER4830 0 4 RS485 POWER4830
huawei(config)#interface emu 2
huawei(config-if-power4830-2)#power module-num 2
huawei(config-if-power4830-2)#power environment humidity 80 10 100 0
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-power4830-2)#power environment temperature 68 -5 80 -20
  This command is invalid unless in the condition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-power4830-2)#quit
huawei(config)#emu add 3 liBATTERY 0 23 rs485 battery1
huawei(config)#interface emu 3
huawei(config-if-libattery-3)#power batteryinstall 2010-08-20
huawei(config-if-libattery-3)#display power run info
  EMU ID: 3                          LiBattery run information
  ---------------------------------------------------------------------------
  Battery charge state: Charge
  Battery voltage: 54.01V
  Battery current: 0.82A
  Battery temperature: 29°C
  Battery capacity specification: 10A
  Battery capacity remained percentage: 97%
  Battery charge or discharge number: 13
  The sum of discharge capacity: 106Ah
  ---------------------------------------------------------------------------
huawei(config-if-libattery-3)#quit
huawei(config)#save
```

3.15.2.4 Configuring the Monitoring Through the H831PMU (Backup Power Using the PBL 02A Fe-lithium Battery)

The H831PMU is a power monitoring control module and it works with the PAIB power board to monitor relevant information about the power system. In addition, the H831PMU can manage a Fe-lithium battery set. This topic describes how to configure the power monitoring through the H831PMU (backup power using the Fe-lithium battery).

Prerequisites

The Fe-lithium battery must be connected to the serial port on the MA5616 through a 1-in-2-out cable.

Context

The MA5616 supports a Fe-lithium battery set for power backup. Compared with the lead-acid battery, the Fe-lithium battery features long lifespan, large capacity, optimized discharging function, fast charging, and flexible environment adaptability. In addition, it supports intelligent management so that the battery can be automatically charged or discharged.

The Fe-lithium battery is connected to the input port of the power system through a power cable and connected to the MA5616 through an RS485 serial port cable. When detecting a Fe-lithium battery, the MA5616 issues a command to the power system to adjust the voltage. The charging mode of a Fe-lithium battery is the equalizing mode.

When the mains supply fails, the Fe-lithium battery provides power for the MA5616 to ensure the normal running of the device in a certain period. When the mains supply recovers, the Fe-lithium battery stops discharging and starts charging.

Procedure

Step 1 Run the **emu add** command to add an environment monitoring unit (EMU).

Step 2 Run the **power supply-parameter** command to configure the power distribution parameters.

Step 3 Run the **display power system parameter** command to query the configuration parameters of the power system.

Step 4 Save the data.

Run the **quit** command to quit the H831PMU mode, and then run the **save** command to save the data.

Step 5 Configure the Fe-lithium battery monitoring unit.

1. Run the **emu add** command to add a Fe-lithium battery monitoring unit.
2. (Optional) Run the **power batteryinstall** command to set the time for installing the battery.
3. Run the **display power run info** command to query the battery running information, such as the charging status and remaining power.
4. (Optional) Run the **display power batteryinstalltime** command to query the time for installing the battery.
5. Run the **save** command to save the data.

   NOTE

   The subnode ID of the Fe-lithium battery is invariably 23.

----End

Example

Assume that:

- The EMU ID of the H831PMU is 3 and the subnode ID is 0.
- The power parameters are as follows: The DC overvoltage alarm threshold is 59 V and the DC undervoltage alarm threshold is 48 V.
- The EMU ID of the Fe-lithium battery is 4 and the subnode ID is 23.
- The time for installing the battery is 2010-08-20.

To configure the power monitoring through the H831PMU (backup power using the Fe-lithium battery) with such configurations, do as follows:

```
huawei(config)#emu add 3 H831PMU 0 0 RS485
huawei(config)#interface emu 3
huawei(config-if-h831pmu-3)#power supply-parameter 59 48
  Send command to environment monitor board ,please waiting for the ack

huawei(config-if-h831pmu-3)#
  Execute command successful
huawei(config-if-h831pmu-3)#quit
huawei(config)#emu add 4 liBATTERY 0 23 rs485 battery1
huawei(config)#interface emu 4
huawei(config-if-libattery-4)#power batteryinstall 2010-08-20
huawei(config-if-libattery-4)#display power run info
  EMU ID: 4                          LiBattery run information
  ---------------------------------------------------------------------------
  Battery charge state: Charge
  Battery voltage: 54.01V
  Battery current: 0.82A
  Battery temperature: 29°C
  Battery capacity specification: 10A
  Battery capacity remained percentage: 97%
  Battery charge or discharge number: 13
  The sum of discharge capacity: 106Ah
  ---------------------------------------------------------------------------
huawei(config-if-libattery-4)#quit
huawei(config)#save
```

3.15.3 Configuring the Monitoring Through the Fan

This topic describes how to configure the speed adjustment mode and the alarm function of the fan. Thus, the fan speed of the MA5616 can be adjusted automatically, and the fan tray of the MA5616 can be monitored.

Context

The fan tray requires the RS-232 serial port for data communication.

The subnode ID of the fan tray is invariably 2.

Procedure

Step 1 Add an EMU.

Run the **emu add** command to add an EMU.

Step 2 Configure the speed adjustment mode of the fan.

Run the **fan speed** command to configure the speed adjustment mode of the fan. 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 adjust** command to set the fan speed. The speed level can be 0, 1, 2, 3, 4, or 5. Here, 5 stands for the highest level, and 0 stands for the lowest level.

Step 3 Configure whether alarms associated with the fan tray are reported.

Run the **fan alarmset** command to configure the reporting of alarms related to the fan tray.

Step 4 Query the configuration parameters of the fan tray.

Run the **display fan system parameter** command to query the configuration parameters of the fan tray.

Step 5 Save the data.

Run the **quit** command to quit the FAN mode, and then run the **save** command to save the data.

----End

Example

Table 3-29 shows the data plan for configuring the speed adjustment mode and monitoring of the fan.

Table 3-29 Data plan for configuring monitoring through the fan

Item	Data	Remarks
EMU	Type: FAN	-
	SN: 1	-
	Subnode ID: 2	-
Fan parameters	Fan speed adjustment mode: automatic	In this mode, the fan speed is automatically adjusted according to the temperature.
	Whether to report an alarm when the fan stops rotation because of being blocked: permit	When the fan stops rotation because of being blocked, the device reports an alarm automatically.
	Whether to report an alarm when the temperature is very high: permit	When the temperature of the fan tray is very high, the device reports an alarm automatically.

```
huawei(config)#emu add 1 FAN 0 2 RS485 FAN
huawei(config)#interface emu 1
huawei(config-if-fan-1)#fan speed mode automatic
huawei(config-if-fan-1)#fan alarmset block permit
  Execute command successful
huawei(config-if-fan-1)#fan alarmset tem-high permit
  Execute command successful
huawei(config-if-fan-1)#display fan system parameter

  EMU ID: 1
  FAN configration parameter:
  ---------------------------------------------------------------------------
  FAN timing mode: Auto timing by temperature
  ---------------------------------------------------------------------------
  Alarm_name                      Permit/Forbid
  Fan block                           Permit
  Temperature high                    Permit
  ---------------------------------------------------------------------------

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

4 Configuring the Ethernet CFM OAM

On the Ethernet network, Ethernet connectivity fault management (CFM) OAM is defined as connectivity fault management in IEEE 802.1ag to implement the OAM function of connectivity detection on the Ethernet bearer network. Ethernet CFM OAM is applicable to the end-to-end (E2E) network with a large scale and it is the network-level OAM.

Prerequisites

- Network devices and lines must be in the normal state.
- The OLT must support the Ethernet CFM OAM function.

Context

OAM is a key method of reducing network maintenance cost.

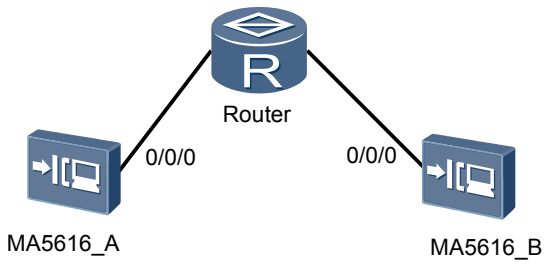
Ethernet is a widely used local area network (LAN) technology. It provides rich bandwidth, features low cost, and supports plug-and-play and multipoint operations. As the Ethernet technology is developing from carriers' networks to metropolitan area networks (MANs) and wide area networks (WANs), the network management and maintenance are increasingly important. Currently, however, Ethernet does not support carrier-class management, and thus L2 network faults cannot be detected on Ethernet networks.

Ethernet CFM OAM is an E2E fault detection technology, which can be used to monitor, diagnose, and troubleshoot the Ethernet.

Networking

Figure 4-1 shows the example network of the Ethernet CFM OAM function.

Figure 4-1 Example network of the Ethernet CFM OAM function



Procedure

Step 1 Create a VLAN.

Run the **vlan** command to create a VLAN that is associated with the object managed by a maintenance association (MA).

Each MA corresponds to one VLAN. The Ethernet CFM checks the connectivity for each MA.

Step 2 Configure a maintenance domain (MD).

An MD can be a network or a part of a network on which the Ethernet CFM is performed. All the MDs are managed by a unified Internet service provider (ISP).

- Run the **cfm md** command to create an MD.
- Run the **display cfm md** command to query the configuration information about an MD.

Step 3 Configure an MA.

An MA is a part of an MD. An MD can be divided into one or more MAs. Each MA corresponds to one VLAN. The Ethernet CFM checks the connectivity for each MA.

- Run the **cfm ma** command to create an MA and configure the parameters of the MA.
- Run the **cfm ma** *mdindex/maindex* **vlan** *vlanid* command to configure the VLAN associated with an MA.
- Run the **cfm ma** *mdindex/maindex* **meplist** *mepid* command to configure the maintenance end point (MEP) list of an MA.
- Run the **display cfm ma** command to query the configuration information about an MA.

Step 4 Configure an MEP.

An MEP is the end point of a maintenance channel. Ethernet OAM tests the link connectivity by using the MEPs on the two ends of a maintenance channel.

Run the **cfm mep** command to create an MEP.

NOTE

When configuring an MEP, note that the objects managed by the MEP are in two directions, namely, up and down.

- Up refers to the direction facing packet forwarding at the device layer. That is, packets are forwarded through the device.
- Down refers to the reverse direction of the up direction. That is, packets are directly forwarded through the MEP port, instead of being forwarded through the device.

Step 5 Enable the local CFM function globally.

Run the **cfm enable** function to enable the local Ethernet CFM OAM function globally.

By default, the Ethernet CFM OAM function is disabled globally.

Step 6 Enable the remote CFM function globally.

Run the **cfm remote-mep-detect enable** function to enable the remote Ethernet CFM OAM function globally.

By default, the remote Ethernet CFM OAM function is disabled globally.

Step 7 Query the configuration result.

- Run the **display cfm** command to query the configuration information about the CFM globally.
- Run the **display cfm mep** command to query the configuration information about an MEP.

----End

Example

Assume that:

- MA5616_A: VLAN 10 is associated with the MA; the MEP port is 0/0/0; the local MEP is 0/0/1; the remote MEP is 0/0/2; the name of the object managed by the MA is huawei-1; the name of the object managed by the MD is huawei; the level of the object managed by the MD is 7.
- MA5616_B: VLAN 10 is associated with the MA; the MEP port is 0/0/0; the local MEP is 0/0/2; the remote MEP is 0/0/1; the name of the object managed by the MA is huawei-1; the name of the object managed by the MD is huawei; the level of the object managed by the MD is 7.

Configure *MA5616_A*

```
huawei(config)#vlan 10 smart   //Create a VLAN that is associated with the MA.
huawei(config)#port vlan 10 0/0 0
huawei(config)#cfm md 0 name-format string huawei level 7
huawei(config)#cfm ma 0/0 name-format string huawei-1
huawei(config)#cfm ma 0/0 vlan 10   //Configure the VLAN to be associated with the
MA.
huawei(config)#cfm ma 0/0 meplist 1    //Configure the MEP list of the MA.
huawei(config)#cfm ma 0/0 meplist 2
huawei(config)#cfm mep 0/0/1 direction down port 0/0/0
huawei(config)#cfm enable   //Enable the local CFM function globally.
huawei(config)#cfm remote-mep-detect enable   //Enable the remote CFM function.
huawei(config)#save
```

To query the configuration information about the MA, do as follows:

```
huawei(config)#display cfm ma 0/0
  ------------------------------------------------------------------------
  MA Index             : 0/0
  MA NameType          : string
  MA Name              : huawei-1
  MA CC Interval       : 1m
  MA Remote-mep-detect : enable
  MA VlanID            : 10        //VLAN 10 associated with the MA.
  MHF Creation         : defer-mhf
  MEP List             : 1,2
  ------------------------------------------------------------------------
```

To query the configuration information about the MD, do as follows:

```
huawei(config)#display cfm md 0
  ------------------------------------------------------------------------
  MD Index     : 0
  MD NameType  : string
  MD Name      : huawei
  MD Level     : 7
  MHF Creation : no-mhf
  ------------------------------------------------------------------------
```

To query the configuration information about the MEP, do as follows:

```
huawei(config)#display cfm mep mdindex/maindex/mepid 0/0/1
  ------------------------------------------------------------------------
  MEP                  : 0/0/1
  MEP Direction        : down
  MEP Port             : 0/0/0
```

```
  VLAN Tag1            : -
  VLAN Tag2            : -
  MEP Admin Status     : enable
  MEP CC Status        : enable
  MEP Priority         : 7
  MEP Alarm Status     : None
  Alarm lowest priority: 2
  Alarm Time           : 2500(ms)
  Reset Time           : 10000(ms)
  MEP IfType           : port
  Remote MEP ID/MAC    : 2/0000-0000-0000
  ------------------------------------------------------------------------
```

Configure *MA5616_B*

```
huawei(config)#vlan 10 smart   //Create a VLAN that is associated with the MA.
huawei(config)#port vlan 10 0/0 0
huawei(config)#cfm md 0 name-format string huawei level 7
huawei(config)#cfm ma 0/0 name-format string huawei-1
huawei(config)#cfm ma 0/0 vlan 10
huawei(config)#cfm ma 0/0 meplist 1
huawei(config)#cfm ma 0/0 meplist 2
huawei(config)#cfm mep 0/0/2 direction down port 0/0/0
huawei(config)#cfm enable
huawei(config)#cfm remote-mep-detect enable
huawei(config)#save
```

5 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, PPPoA, or 802.1X mode. This topic describes how to configure an xDSL Internet access service on the MA5616.

Prerequisite

PPPoE or PPPoA Internet access mode:

- Configure the AAA function.
  - To enable the AAA function on the device, see **3.12 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 MA5616 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 xDSL profile for the Internet access service must be created.
  - **3.7.1 Configuring the ADSL2+ Profile**
  - **3.7.2 Configuring the SHDSL Profile**
  - **3.7.3.1 Configuring the VDSL2 Profile (Normal Mode)**
  - **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**

IPoE or IPoA Internet access mode:

- **3.7.1 Configuring the ADSL2+ Profile**
- **3.7.2 Configuring the SHDSL Profile**
- **3.7.3.1 Configuring the VDSL2 Profile (Normal Mode)**
- **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**

Data preparation

Before configuring an xDSL Internet access service, plan the data items as listed in **Table 5-1**.

Table 5-1 Data plan for the xDSL Internet access service

Item	Data	Remarks
MA5616	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 thus 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 MA5616 on L2. The VLAN ID must be consistent with the VLAN ID of the upstream service packets of the MA5616.	-

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. 5.1 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.
2. 5.2 Configuring an Upstream Port
   This topic describes how to add an upstream port for an Internet access service to a VLAN.
3. 5.3 Configuring an xDSL Port
   An xDSL can transmit services only when it is activated. This topic describes how to activate an xDSL port and bind the port with an xDSL profile.
4. 5.4 Creating an xDSL Service Port
   A service port is a service channel connecting the user side to the network side. To provide services, a service port must be created.
5. 5.5 (Optional) Configuring the xPoA-xPoE Protocol Conversion
   Configuring protocol conversion is required only when the encapsulation mode is IPoA or PPPoA; it is not required when the encapsulation mode is IPoE or PPPoE.

5.1 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.

Prerequisites

The ID of the planned VLAN is not occupied.

Application Scenario

VLAN application is specific to user types. For details on the VLAN application, see **Table 5-2**.

Table 5-2 VLAN application and planning

User Type	Application Scenario	VLAN Planning
● Residential user of the Internet access service ● 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 subscribers are converged to the same VLAN.	VLAN type: smart VLAN attribute: common 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 type: smart Attribute: stacking VLAN forwarding mode: by S+C
Commercial user of the transparent transmission service	Applicable only to the transparent transmission service of a commercial user.	VLAN type: smart VLAN attribute: QinQ VLAN forwarding mode: by VLAN+MAC or S+C.

Default Configuration

Table 5-3 lists the default parameter settings of VLAN.

Table 5-3 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart 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.
Default attribute of a new VLAN	Common	-
VLAN forwarding mode	VLAN+MAC	-

Procedure

Step 1 Create a VLAN.

Run the **vlan** command to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 5-4 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. One standard VLAN contains multiple upstream ports. Ethernet ports in one 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 device subtending.
Smart VLAN	To add a smart VLAN, run the **vlan *vlanid* smart** command.	One smart VLAN may contain multiple upstream ports and service ports. The service ports in one smart VLAN are isolated from each other. The service ports in different VLANs are also isolated. One VLAN provides access for multiple users and thus saves VLAN resources.	Smart VLANs are applicable to FE or xDSL service access. For example, Smart VLANs can be used in residential users.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
MUX VLAN	To add a MUX VLAN, run the **vlan *vlanid* mux** command.	One MUX VLAN may contain multiple upstream ports but only one service port. The service ports in different VLANs are isolated. 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 FE or xDSL service access. For example, MUX VLANs can be used to identify users.

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.

Step 2 (Optional) 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 5-5 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, or MUX 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 packets from a QinQ VLAN contain two VLAN tags, that is, inner VLAN tag from the private network and outer VLAN tag from the MA5616. Through the outer VLAN, an L2 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 a MUX VLAN.	The packets from a stacking VLAN contain two VLAN tags, that is, inner VLAN tag and outer VLAN tag from the MA5616. 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 L2 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 tag of the service port, run the **stacking label** command. You can run the **stacking outer-ethertype** command to set the type of outer Ethernet protocol supported by VLAN stacking on the MA5616. You can also run the **stacking inner-ethertype** command to set the type of inner Ethernet protocol supported by VLAN stacking. To ensure that Huawei device is interconnected with the device of other vendors, the type of inner/outer Ethernet protocol must be the same as that of the interconnect device.

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.

Step 3 (Optional) Configure VLAN description.

To configure VLAN description, run the **vlan desc** command. You can configure VLAN description to facilitate maintenance. The general VLAN description includes the usage and service information of the VLAN.

Step 4 (Optional) Configure the VLAN forwarding policy.

vlan-connect corresponds to the S+C forwarding policy, which ensures higher security by solving the problems of insufficiency in the MAC address space, MAC address aging, and MAC address spoofing and attacks.

To configure the VLAN forwarding policy in the VLAN service profile, 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 policy 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 created in **4.1**.

----End

Example

Assume that a QinQ VLAN with ID of 100 is to be configured for an enterprise user to ensure higher security and the VLAN forwarding policy is S+C. For the VLAN, description needs to be configured for easy maintenance. To configure such a VLAN, do as follows:

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 q-in-q
huawei(config)#vlan desc 100 description qinqvlan/forhuawei
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#forwarding vlan-connec
  Info: Please use the commit command to make modifications take effect
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 100 profile-id 1
```

5.2 Configuring an Upstream Port

This topic describes how to add an upstream port for an Internet access service to a VLAN.

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 **3.3.1 Configuring an Uplink Ethernet Port**.

Step 3 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 **3.4 Configuring the Link Aggregation of Upstream Ethernet Port** .

----End

Example

Assume that the 0/0/1 and 0/0/0 upstream ports are to be added to VLAN 50. The 0/0/1 and 0/0/0 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 0/0 0
huawei(config)#port vlan 50 0/0 1
huawei(config)#interface eth 0/0
huawei(config-if-eth-0/0)#duplex 0 full
huawei(config-if-eth-0/0)#duplex 1 full
huawei(config-if-eth-0/0)#speed 0 100
huawei(config-if-eth-0/0)#speed 1 100
huawei(config-if-eth-0/0)#quit
huawei(config)#link-aggregation 0/0 0 0/0 1 egress-ingress workmode lacp-static
```

5.3 Configuring an xDSL Port

An xDSL can transmit services only when it is activated. This topic describes how to activate an xDSL port and bind the port with an xDSL profile.

Prerequisites

The xDSL profile is already created.

- **3.7.1 Configuring the ADSL2+ Profile**
- **3.7.2 Configuring the SHDSL Profile**
- **3.7.3.1 Configuring the VDSL2 Profile (Normal Mode)**
- **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**

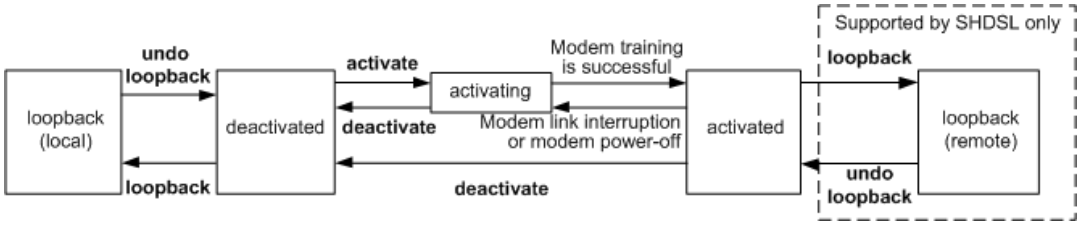
Context

- 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 5-1** shows the inter-conversion between xDSL port states.

Figure 5-1 Inter-conversion between xDSL port states



NOTE

By default, the port is disconnected with the modem and is in the activating state. To bind a profile to the port, you must deactivate port.

Procedure

- ADSL access mode
  1. Run the **interface adsl** command to enter the ADSL mode.
  2. Run the **activate** command to activate an ADSL2+ port and bind the port with an ADSL2+ line template.

     To activate a port, you must bind the port with a line template. If you do not specify the index of the line template, the system uses the template bound with the port last time to activate the port.
  3. Run the **alarm-config** command to bind an alarm template to the port.
- SHDSL access mode
  1. Run the **interface shl** command to enter the SHDSL mode.
  2. Run the **activate** command to activate an SHDSL port and bind the port with an SHDSL line profile.

     To activate a port, you must bind the port with a line profile. If you do not specify the index of the line profile, the system uses the profile bound with the port last time to activate the port.
  3. Run the **alarm-config** command to bind an alarm profile to the port.
- VDSL access mode
  1. Run the **interface vdsl** command to enter the VDSL mode.
  2. Activate a VDSL port and bind the port with a profile.
     - In the case of VDSL common mode, run the **activate** ***portid*** **template-index** ***template-index*** command to activate a VDSL2 port and bind the port with a VDSL2 line template.

NOTE

To activate a port, you must bind the port with a line template. If you do not specify the index of the line template, the system uses the template bound with the port last time to activate the port.

- In the case of VDSL TI mode, run the **activate** ***portid*** **spectrum-profile-index** ***spectrum-profile-index*** **dpbo-profile-index** ***dpbo-profile-index*** **upbo-profile-index** ***upbo-profile-index*** **service-profile-index** ***service-profile-index*** **noise-margin-profile-index** ***noise-margin-profile-index*** **delayinp-profile-index** ***delayinp-profile-index*** command to activate a VDSL2 port and bind the port with VDSL2 profiles.

3. Run the **alarm-config** command to bind an alarm template to the port.

----End

Example

To activate ADSL2+ port 0/2/0 and bind line template 2 and alarm template 2 to it, 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 profile-index 2
huawei(config-if-adsl-0/2)#alarm-config 0 2
```

To activate SHDSL port 0/4/0 and bind line profile 2 and alarm profile 2 to it, do as follows:

```
huawei(config)#interface shl 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 2
huawei(config-if-shl-0/4)#alarm-config 0 2
```

In the common VDSL mode, to activate VDSL2 port 0/1/0 and bind line template 2 and alarm template 2 to it, do as follows:

```
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 2
huawei(config-if-vdsl-0/1)#alarm-config 0 2
```

5.4 Creating an xDSL Service Port

A service port is a service channel connecting the user side to the network side. To provide 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 MA5616 supports the following modes of traffic classification:

- By user-side VLAN
- By user-side service encapsulation mode
- By VLAN+user-side packet priority
- By VLAN+user-side service encapsulation mode

Table 5-6 lists the default settings of a service port.

Table 5-6 Default settings of a service port

Parameter	Default Setting
Traffic profile ID	0-6
Administration status	Activated
Maximum number of learnable MAC addresses	255

Procedure

Step 1 Add a traffic profile.

Run the **traffic table ip** command to add 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 **3.14.1.1 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 applied to the triple play service scenario.
  - 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**: 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. The user-side VLAN is the 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 by this channel.
  - 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. 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 according to requirements.

- Run the **service-port desc** command to configure the description of the service port. Configure 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 set 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 provide 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 to restrict the maximum number of PCs that can access the Internet by using the same account. By default, the maximum number of the MAC addresses that can be learned by a service port is 255.

----End

Example

The MA5616 provides the Internet access service with the access rate 3072 kbit/s for 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 enable an account. Therefore, the MA5616 does not the service to the user currently. To plan data for a residential user who accesses the Internet in the ADSL2+ mode, 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 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
  Mapping 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
  Referenced Status    : not used
  ----------------------------------------------
huawei(config)#service-port 3 vlan 100 adsl 0/2/0 vpi 1 vci 39 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 residential user requests the Internet access service with the access rate 2048 kbit/s. To facilitate service expansion in the future, the MA5616 adopts the ADSL2+ mode to provide the Internet access service for the user and differentiates users by user-side VLAN (the S-VLAN is VLAN 50 and the C-VLAN is VLAN 10). Query result shows that the system has a proper traffic profile. Therefore, the system provides the Internet access service for the user immediately. To facilitate maintenance, configure description for the service port.

```
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)#service-port 4 vlan 50 adsl 0/2/0 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 residential user requests the Internet access service with the access rate 2048 kbit/s. To facilitate service expansion in the future, the MA5616 adopts the SHDSL mode to provide the Internet access service for the user. Query result shows that the system has a proper traffic profile. Therefore, the system provides the Internet access service for the user immediately. To facilitate maintenance, configure description for the service port.

```
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)#service-port 5 vlan 50 shdsl mode ptm 0/4/0 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 MA5616 adopts the VDSL mode to provide the Internet access service for the user and differentiates users by user-side VLAN (the S-VLAN is VLAN 50 and the C-VLAN is VLAN 10). Query result shows that the system does not have a proper traffic profile. The system needs to provide the Internet access service for the user immediately. To facilitate maintenance, configure description for the service port.

```
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
     8      3072     100304      6144     198608   4 -             local-pri
  ------------------------------------------------------------------------------
  Total Num : 8
huawei(config)#traffic table ip index 9 cir 8192 priority 4 priority-policy loca
l-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 9
  TD Name              : ip-traffic-table_9
  Priority             : 4
  Mapping 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
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 6 vlan 50 vdsl mode ptm 0/1/0 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
```

5.5 (Optional) Configuring the xPoA-xPoE Protocol Conversion

Configuring protocol conversion is required only when the encapsulation mode is IPoA or PPPoA; it is not required when the encapsulation mode is IPoE or PPPoE.

Context

In the xPoA access mode, data cannot be directly transmitted in the IP network, and protocol conversion is required. IPoA data and PPPoA data can be transmitted in the IP network only after the IPoA-IPoE and PPPoA-PPPoE conversions are performed.

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 need not 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 5-2 provides the configuration flow for the xPoA-xPoE protocol conversion.

Figure 5-2 Flowchart for configuring the xPoA-xPoE protocol conversion

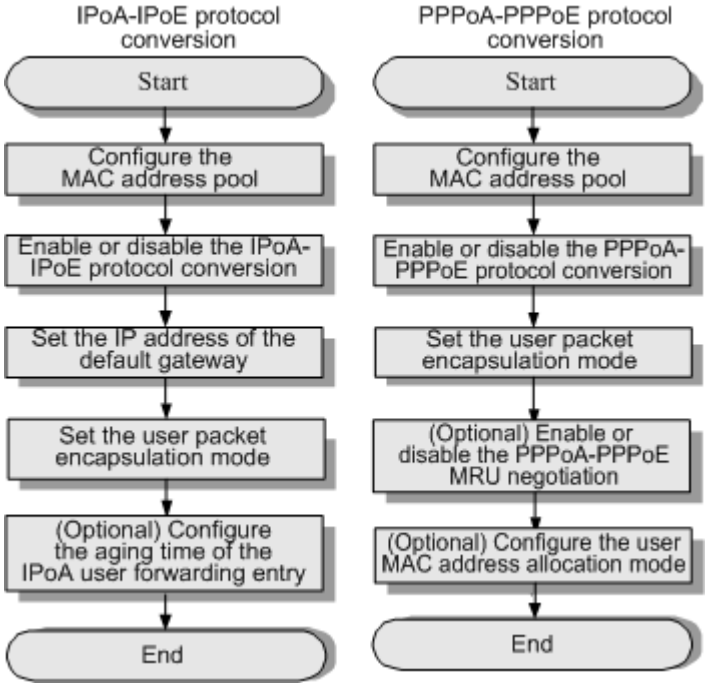


Table 5-7 lists the default settings of the xPoA-xPoE protocol conversion.

Table 5-7 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

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 MA5616 works in the L2 mode, set the IP address of the upper-layer router as the default gateway. If the MA5616 works in the L3 mode, set the IP address of the L3 interface corresponding to the MA5616 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. By default, the 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. 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 MA5616 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 need not be segmented or reassembled.

----End

Example

The MA5616 works in the L2 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 0/2/0 vpi 0 vci 35 type ipoa llc srcIP 10.1.1.20
```

The PPPoA service encapsulation mode is LLC. 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 0/2/0 vpi 0 vci 35 type pppoa llc
```

6 Configuring the Multicast Service (Multicast VLAN Mode)

About This Chapter

This topic describes how to configure the multicast service on the MA5616 in multicast VLAN mode.

6.1 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 6-1 lists the default settings of the multicast service of the MA5616.

Table 6-1 Default settings of the multicast service

Feature	Default Setting
Multicast protocol	Off
IGMP version	V3
Configuration mode of the multicast program	Configured statically
Multicast bandwidth management	Enabled
Multicast preview	Enabled
Multicast log function	Enabled

6.2 Configuring the Multicast Service on a Single-NE Network

This topic describes how to configure the multicast service on a standalone MA5616.

Service Requirements

The multicast function of the MA5616 is used for multicast video services, such as live TV and near-video on demand (NVOD). The MA5616 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 MA5616 is oriented to L2, and the MA5616 forwards data based on VLAN ID + multicast MAC address. A multicast program on the network is uniquely identified by VLAN ID + multicast IP address. The MA5616 differentiates multicast sources by VLAN ID. It allocates a unique VLAN ID to each multicast source, controls the multicast domain and user rights based on the multicast VLAN ID, and provides a platform for different ISPs to implement different multicast video services.

Prerequisite

The license for the multicast program or multicast user must be applied for and installed.

Data Plan

Before configuring the multicast video service, plan the data items as listed in **Table 6-2**.

Table 6-2 Data plan for configuring the multicast service on a standalone MA5616

Device	Item	Remarks
MA5616	Multicast VLAN	Generally, a multicast VLAN is allocated to each multicast ISP.
	L2 multicast protocol	IGMP proxy and IGMP snooping are supported.
	IGMP version	IGMP V3 and IGMP V2 are supported and IGMP V3 is compatible with IGMP V2.
	Configuration mode of the multicast program	The multicast program can be configured statically or generated dynamically.
	Multicast general query and group-specific query parameters	The default values are adopted.
	Program list	-
	User authentication policy	-
	Program bandwidth, uplink port bandwidth, and user bandwidth	-
	Multicast log policy	Multicast logs can be reported to the log server in syslog mode or in CDR mode.
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 MA5616.
Home gateway or modem	IGMP version	The IGMP version of the CPE cannot be earlier than the IGMP version used by the MA5616.

Procedure

----End

6.2.1 Configuring Global Multicast Parameters

The general parameters of L2 multicast protocols (including IGMP proxy and IGMP snooping) configured globally for a device are applicable to all the multicast VLANs of the device.

Context

Global multicast parameters include general query, group-specific query, and policy of processing multicast packets.

For the general query:

- Purpose: A general query packet is periodically sent by the MA5616 to check whether there is any multicast user who leaves the multicast group without sending the leave packet. Based on the query result, the MA5616 periodically updates the multicast forwarding table and releases the bandwidth of the multicast user who has left the multicast group in time.
- Principles: The MA5616 periodically sends the general query packet to all the online IGMP users. If the MA5616 does not receive the response packet from a multicast user within a specified time (robustness variable x interval of the general query + maximum response time of the general query), it regards the user as having left the multicast group and deletes the user from the multicast group.

For the group-specific query:

- Purpose: A group-specific query packet is sent by the MA5616 after a multicast user who 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.
- Principles: When a multicast user leaves a multicast group, for example, switches to another channel, the user sends a leave packet to the MA5616 in an unsolicited manner. If the multicast user is not configured with the quick leave attribute, the MA5616 sends a group-specific query packet to the multicast group. If the MA5616 does not receive the response packet from the multicast user within a specified time (robustness variable x interval of the group-specific query + maximum response time of the group-specific query), it deletes the multicast user from the multicast group.

Procedure

Step 1 In global config mode, run the **btv** command to enter BTV mode.

Step 2 Configure general query parameters.

1. Run the **igmp proxy router gen-query-interval** command to set the interval of the general query. By default, the 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 time is 10s.
3. Run the **igmp proxy router robustness** command to set the count of general queries. By default, the count is 2.

Step 3 Configure group-specific query parameters.

1. Run the **igmp proxy router sp-query-interval** command to set the interval of the group-specific query. By default, the interval is 1s.
2. Run the **igmp proxy router sp-response-time** command to set the maximum response time of the group-specific query. By default, the time is 0.8s.
3. Run the **igmp proxy router sp-query-number** command to set the count of group-specific queries. By default, the count is 2.

Step 4 Configure the policy of processing multicast packets.

The default processing mode is as follows: The normal mode is adopted for IGMP packets, that is, IGMP packets are processed under control. The discard mode is adopted for unknown multicast packets, that is, unknown multicast packets are discarded.

The default policy is adopted for multicast packets. That is, the policy need not be changed. When configuring other services, you can run the **igmp policy** command to configure the policy of processing multicast packets if you need to control the forwarding of multicast packets.

Step 5 Run the **display igmp config global** command to check whether the parameters are configured correctly.

----End

Example

To configure multicast general query parameters by setting the query interval to 150s, maximum response time to 20s, and query count to 3, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp proxy router gen-query-interval 150
huawei(config-btv)#igmp proxy router gen-response-time v3 200
huawei(config-btv)#igmp proxy router robustness 3
```

To configure multicast group-specific query parameters by setting the query interval to 20s, maximum response time to 10s, and query count to 3, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp proxy router sp-query-interval 200
huawei(config-btv)#igmp proxy router sp-response-time v3 100
huawei(config-btv)#igmp proxy router sp-query-number 3
```

Result

Check whether the multicast general query parameters and group-specific query parameters are configured correctly.

```
huawei(config)#btv
huawei(config-btv)#display igmp config global
  ------------------------------------------------------------------------
  Authorization                         : enable
  Robustness variable                   : 3        //The count of general queries
is 3.
  General query interval(s)             : 150      //The interval of the general
query is 150s.
  V2 General query response time(0.1s)  : 100
  V3 General query response time(0.1s)  : 200      //The maximum response time of
the general query is 20s.
  Specific query interval(0.1s)         : 200      //The interval of the group-
specific query is 10s.
  V2 Specific query response time(0.1s) : 8
  V3 Specific query response time(0.1s) : 100      //The maximum response time of
the group-specific query is 10s.
  Specific query number                 : 3        //The count of group-specific
queries is 3.
  V2 router present timeout(s)          : 400
  User action report switch             : disable
  Preview switch                        : enable
  Recognition time(s)                   : 30
  The time of reset preview-count       : 04:00:00
  Auto create log interval(h)           : 2
  Uplink port mode                      : default
  Bandwidth management switch           : enable
  CDR auto report interval(s)           : 600
  CDR auto report number                : 200
  CDR switch                            : disable
  IGMP Packet encapsulation             : all
  IGMP ECHO switch                      : disable
  Router IP                             : 192.168.1.1
  Initial unsolicited report interval(s): 1
  Query offline user switch             : -
  BTV Forward Mode                      : Mvlan
  ------------------------------------------------------------------------
```

6.2.2 Configuring the Multicast Program

A multicast program can be configured statically or generated dynamically. After the program is configured, the multicast user with the corresponding rights can watch or preview the program.

Prerequisites

The multicast VLAN to which the multicast program belongs must exist. For the details on configuring the VLAN, see **3.6 Configuring a VLAN**.

Context

In multicast services, multicast VLANs are used to identify different multicast Internet service providers (ISPs). Generally, a multicast VLAN is allocated to each multicast ISP for the VLAN-based management of multicast programs, multicast protocols, and IGMP versions, and for the control of multicast domain and user rights.

Create a common VLAN before creating a multicast VLAN.

- A multicast VLAN can be the same as a unicast VLAN. In this case, the multicast VLAN and the unicast VLAN share the same traffic channel.
- A multicast VLAN can be different from a unicast VLAN. In this case, the multicast VLAN and the unicast VLAN use different traffic channels.

Procedure

Step 1 Configure multicast programs.

A multicast program in a multicast VLAN can be configured statically or generated dynamically.

- Static configuration mode: Configure the program list for the multicast VLAN in advance and bind the rights profile to the program to manage the programs.

1. In multicast VLAN mode, run the **igmp match mode enable** command to set the static configuration mode. In this case, you need to configure the multicast program in advance. The program in the multicast VLAN is configured statically by default.
2. In multicast VLAN mode, 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 the multicast VLAN is V3, the source IP address of the program in the multicast VLAN must be configured. If the IGMP version of the multicast VLAN is V2, the source IP address of the program in the multicast VLAN cannot be configured.
3. Add a rights profile.

   In BTV mode, run the **igmp profile add** command to add a rights profile.
4. Bind the rights profile to the program.

   In BTV mode, run the **igmp profile** command to bind the rights profile to the program and set the rights to watch the program.

   NOTE

   If a user is bound with multiple rights profiles and the rights to a program are different in these profiles, the user uses the rights with the highest priority. 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 is generated according to the request of the user. In this mode, the program list is not required; 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 configure the dynamic generation mode.

CAUTION

When you run the **igmp match mode { enable | disable }** command to switch the program matching mode:

- This command can be executed only when the IGMP mode is disabled.
- The system will delete all the programs in this multicast VLAN. In this case, if a user is online, the system will force the user to go offline.

2. Run the **igmp match group** command to configure the IP address range of the program group that can be dynamically generated in the multicast VLAN. After the configuration, the user can request for only the programs whose IP addresses are within the specified range.

Step 2 Configure the multicast uplink port.

1. In multicast VLAN mode, run the **igmp uplink-port** command to configure the multicast uplink port. After the configuration, all the packets from the multicast VLAN are forwarded or received through this uplink port.
2. In BTV mode, run the **igmp uplink-port-mode** command to change the mode of the multicast uplink port. By default, the multicast uplink port is in default mode. On the MSTP network, the multicast uplink port adopts the MSTP mode.
   - Default mode: If a multicast VLAN contains only one uplink port, the IGMP packets that go upstream can be sent only through this port. If a multicast VLAN contains multiple uplink ports, the IGMP packets that go upstream are sent through all the uplink ports.
   - MSTP mode: This mode is applicable to the MSTP network.

Step 3 Select the multicast protocol.

Run the **igmp mode** { **proxy** | **snooping** } command to select the L2 multicast protocol. By default, the multicast function is disabled in the system.

In IGMP snooping mode, proxy can be enabled for the report packet and leave packet. When a multicast user joins or leaves a multicast program, the MA5616 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 for a program, after authenticating the user, the MA5616 sends the user report packet to the network side and obtains a corresponding multicast stream from the multicast router. The MA5616 does not send the report packets from the subsequent users for joining the same program to the network side any more.
- Run the **igmp leave-proxy enable** command to enable the proxy of the snooping leave packet. When the last user requests for leaving a program, the MA5616 sends the user leave packet to the network side and notifies the upper-layer device of stopping sending multicast

streams. The MA5616 does not send the leave packets from the users before the last user to the network side.

Step 4 Configure the IGMP version.

Run the **igmp version**{ **v2** | **v3** } command to configure the IGMP version. By default, IGMP V3 is enabled in the system. If the upper-layer and lower-layer devices on the network are of the IGMP V2 version and cannot recognize the IGMP V3 packets, run this command to switch the IGMP version.

IGMP V3 is compatible with IGMP V2 in packet processing. If IGMP V3 is enabled on the MA5616 and the upper-layer multicast router switches to IGMP V2, the MA5616 automatically switches to IGMP V2 when receiving the IGMP V2 packets. If the MA5616 does not receive any IGMP V2 packets within the preset IGMP V2 time to live (TTL) time, it automatically switches back to IGMP V3. In BTV mode, run the **igmp proxy router timeout** command to set the IGMP V2 TTL time. By default, the TTL time is 400s.

Step 5 Change the priority for forwarding IGMP packets.

Run the **igmp priority** command to change the priority for forwarding the IGMP packets on the uplink port. By default, the priority is 6 and it need not be changed.

- In IGMP proxy mode, the IGMP packets sent to the network side adopt the priority set through the **igmp priority** command in the multicast VLAN.
- In IGMP snooping mode, the IGMP packets forwarded to the network side adopt the priority of the user traffic stream. The priority of the traffic stream is set through the traffic profile.

Step 6 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 multicast program in the multicast VLAN.

----End

Example

Assume that the VLAN ID is 10, the program is configured statically, the IP address of the program is 224.1.1.1, the program bandwidth is 5000 kbit/s, the multicast uplink port is 0/0/1, the IGMP proxy is enabled, and the IGMP version is V3. To configure a program with these attributes, do as follows:

```
huawei(config)#vlan 10 smart
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp match mode enable
  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-mvlan10)#igmp program add name movie ip 224.1.1.1 sourceip
10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan10)#igmp uplink-port 0/0/1
huawei(config-mvlan10)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
  Command has been executed successfully
huawei(config-mvlan10)#igmp version v3
  This operation will delete all programs in current multicast vlan
  Are you sure to change current IGMP version? (y/n)[n]: y
```

Assume that the VLAN ID is 10, the program is generated dynamically, the IP address for the dynamic program group ranges from 224.1.1.1 to 224.1.1.100, the multicast uplink port is 0/0/1, the IGMP proxy is enabled, and the IGMP version is V3. To configure a program with these attributes, do as follows:

```
huawei(config)#vlan 10 smart
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#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-mvlan10)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
huawei(config-mvlan10)#igmp uplink-port 0/0/1
huawei(config-mvlan10)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
  Command has been executed successfully
huawei(config-mvlan10)#igmp version v3
  This operation will delete all programs in current multicast vlan
  Are you sure to change current IGMP version? (y/n)[n]: y
```

Result

Query the attributes and information of the program in the multicast VLAN in static configuration mode.

```
huawei(config)#display igmp config vlan 10
  ---------------------------------------------------------------------------
  IGMP mode                         : proxy     //IGMP proxy protocol
  IGMP version                      : IGMP V3   //IGMP V3
  Log switch                        : enable
  Default uplink port               : -
  Report proxy switch               : disable
  Leave proxy switch                : disable
  Unsolicited report interval(s)    : 10
  IGMP priority                     : 6
  Send global leave switch          : enable
  Program match mode              : enable    //The program matching mode is enabled
and the multicast program is configured statically.
  Program match group               : -
  ---------------------------------------------------------------------------
huawei(config)#display igmp program vlan 10 ip 224.1.1.1
{ <cr>||<K> }:

  Command:
          display igmp program vlan 10 ip 224.1.1.1
  ------------------------------------------
  Program index           : 0
  Create mode             : static
  Program name            : movie
  IP address              : 224.1.1.1     //IP address of the multicast program
  VLAN ID                 : 10
  Host attribute          : enable
  Log attribute           : enable
  Prejoin attribute       : disable
  Unsolicited attribute   : disable
  Priority                : 7
  Host IP                 : 0.0.0.0
  Bandwidth(kbps)         : 5000          //The bandwidth of the multicast program
is 5000 kbit/s.
  SourceIP                : 10.10.10.10
  Preview Profile         : 0
  Numbers of watching     : 0
  Program Grade           : -
  ------------------------------------------
```

Query the attributes and information of the program in the multicast VLAN in dynamic generation mode.

```
huawei(config-mvlan10)#display igmp config vlan 10
  ------------------------------------------------------------------------
  IGMP mode                         : proxy
  IGMP version                      : IGMP V3
  Log switch                        : enable
  Default uplink port               : -
  Report proxy switch               : disable
  Leave proxy switch                : disable
  Unsolicited report interval(s)    : 10
  IGMP priority                     : 6
  Send global leave switch          : enable
  Program match mode                : disable    //The program matching mode is
disabled and the multicast program is generated dynamically.
  Program match group               : 224.1.1.1 ~
224.1.1.100
  ------------------------------------------------------------------------
```

6.2.3 Configuring the Multicast User

When a user needs to watch the multicast program, you need to configure the user as a multicast user because only a multicast user can watch the multicast program.

Prerequisites

Before configuring a user as a multicast user, you must create a service channel and ensure that this channel is normal.

For an xDSL user, you must perform the following operations:

1. **3.6 Configuring a VLAN**
2. **5.2 Configuring an Upstream Port**
3. **5.3 Configuring an xDSL Port**
4. **5.4 Creating an xDSL Service Port**

Context

Add a multicast user and bind the multicast user with the multicast VLAN to create a multicast member. Bind the rights profile to the multicast user to implement multicast user authentication.

Procedure

Step 1 In global config mode, run the **btv** command to enter BTV mode.

Step 2 Configure the multicast user and the multicast user attributes.

1. Add a multicast user.

   Run the **igmp user add service-port** ***index*** command to add a multicast user.

   NOTE

   You can run the **display service-port** command to query the index of the traffic stream of the multicast user to be added.

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** command to configure the maximum number of programs that can be concurrently watched by the multicast user. The maximum number is 16.

Run the **igmp user watch-limit** command to configure the maximum number of programs of different priorities that can be watched by the multicast user.

3. Configure 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 leave mode of the multicast user. By default, the 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.
   - disable: The system sends the specific group query packet after receiving the leave packet of the multicast user. Within the set aging time, if the system does not receive the report packet of the multicast user, the user is considered as offline and the system deletes the multicast user from the multicast group.
   - mac-based: Indicates 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 and the user is the last one who watches the multicast program in the multicast group, 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.

Step 3 Configure the multicast user authentication.

To control the rights of a multicast user, you can enable the multicast user authentication function. Binding the rights profile to the multicast user implements multicast user authentication.

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 of multicast user is enabled. You can run the **igmp proxy authorization** command to change the configuration.

2. Bind the rights profile to the multicast user. Binding the rights profile to the multicast user implements user authentication.

   Run the **igmp user bind-profile** command to bind the rights profile to the multicast user. After the binding, the multicast user has the rights to the programs configured in the profile.

Step 4 Bind the multicast user to the multicast VLAN.

In 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 for the programs configured in the multicast VLAN.

Step 5 Run the **display igmp user** command to check whether the multicast user is configured correctly.

----End

Example

Assume that multicast user (port) 0/1/0 (with an index of the user traffic stream 100) is added to multicast VLAN 10, the user authentication and the log report function are enabled, the maximum number of programs that can be concurrently watched is 4, and rights profile **music** is bound to the user. To perform the configurations, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 100 auth log enable max-program 4
huawei(config-btv)#igmp user bind-profile service-port 100 profile-name music
huawei(config-btv)#quit
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
```

Result

Check whether the multicast user is configured correctly.

```
huawei(config)#display igmp user 0 //0 is the index of the multicast user. You can
run the display igmp user all command to query the index of the multicast user.
{ <cr>||<K> }:

  Command:
          display igmp user 0
  User                        : 0/1/0       //Port of the multicast user
  State                       : offline
  Authentication              : auth        //Authentication is
required.
  Quick leave                 : MAC-based
  IGMP flow ID                : 100
  Video flow ID               : 100
  Log switch                  : enable
  Bind profiles               : 1
  IGMP version                : IGMP v3
  Available programs          : 4           //The maximum number of programs that
can be concurrently watched is 4.
  Global Leave                : disable
  User MaxBandWidth           : no-limit
  Used bandwidth(kbps)        : 0
  Used bandwidth
  to max bandwidth(%)         : -
  Total video bandwidth       : -
  Mcast video bandwidth       : -
  Bind profile list
  ------------------------------------------
  index    Profile name          Program number
  ------------------------------------------
      0    music                        0    //The bound rights profile is
music.
  ------------------------------------------
  Total: 1
```

6.2.4 (Optional) Configuring the Multicast Bandwidth

To limit the multicast bandwidth of a user, you can enable the multicast bandwidth management function, namely, connection admission control (CAC), and then control the bandwidth of the 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 Access Node Control Protocol (ANCP) CAC function is enabled, and a user requests for 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. The system determines whether the user can watch the multicast program based on the result:

- 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. That is, the request of the user fails.

If the CAC function is not enabled, the system does not guarantee the bandwidth of the multicast program. In this case, the picture quality of the requested program is poor. For example, mosaic and delay occur.

Procedure

Step 1 In global config mode, run the **btv** command to enter BTV mode.

Step 2 Enable the CAC function globally.

- Run the **igmp bandwidthCAC enable** function to enable the CAC function globally.
- By default, the CAC function is enabled globally.

Step 3 Configure the bandwidth of the multicast program.

- Run the **igmp program add** command to configure the bandwidth of the multicast program.
- By default, the bandwidth of the multicast program is 5000 kbit/s.

Step 4 Configure the bandwidth of the multicast user.

- Run the **igmp user add service-port *index* max-bandwidth** command to configure the bandwidth of the multicast user.
- Before configuring the bandwidth of the multicast user, ensure that the service port of the multicast user exists. You can run the **display service-port** command to query the service port.
- By default, the bandwidth of the multicast user is not limited (**no-limit**).

Step 5 Check whether the multicast bandwidth is configured correctly.

- Run the **display igmp config global** command to check whether the CAC function is enabled globally.
- Run the **display igmp program** command to query the bandwidth of the multicast program.
- Run the **display igmp user** command to query the bandwidth of the multicast user.

----End

Example

Assume that the CAC function is enabled globally, the bandwidth of multicast user 0/1/0 is 10 Mbit/s, and the bandwidth of the multicast program with IP address 224.1.1.1 is 1 Mbit/s. To perform the configurations, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp bandwidthcAC enable
huawei(config-btv)#igmp user add service-port 0 max-bandwidth 10240 //0 is the
service port ID of the multicast user.
huawei(config-btv)#multicast-vlan 10
huawei(config-mvlan10)#igmp program add ip 224.1.1.1 bandwidth 1024
```

Result

Check whether the bandwidths of the multicast user and multicast program are configured correctly.

- Check whether the bandwidth of the multicast user is configured correctly.

```
huawei(config)#display igmp user all
{ <cr>||
<K> }:


Command:
          display igmp user
all
  Command is being executed, please
wait...

-------------------------------------------------------------------------------
  User Index  Bind     State   Auth   Quick     IGMP    Video   Log
Available
              profiles               leave     flow ID flow ID switch
programs

-------------------------------------------------------------------------------
  0              -    offline no-auth MAC-based 0       0       enable
8

-------------------------------------------------------------------------------
  Total: 1

huawei(config)#display igmp user
{ all<K>|extended-attributes<K>|user-index<U><0,191> }:0 //0 is the index of
the multicast user queried in the preceding part.
{ <cr>||
<K> }:


Command:
          display igmp user
0
  User                        :
0/1/0
  State                       :
offline
  Authentication              : no-
auth
  Quick leave                 : MAC-
based
  IGMP flow ID                :
0
  Video flow ID               :
0
  Log switch                  :
enable
  Bind profiles               :
-
  IGMP version                : IGMP
v3
  Available programs          :
8
  Global Leave                :
disable
  User MaxBandWidth           : 10240     //The bandwidth of the multicast user
is 10 Mbit/s.
  Used bandwidth(kbps)        :
0
  Used
bandwidth
  to max bandwidth(%)         :
```

```
0.00
  Total video bandwidth      :
-
  Mcast video bandwidth      : -
```

- Check whether the bandwidth of the multicast program is configured correctly.

```
huawei(config)#display igmp program all
{ <cr>||
<K> }:


Command:
          display igmp program
all

------------------------------------------------------------------------------
  Index| Create |      IP       |     Program      |User |VLAN |Prejoin|
Priority
       | Flag   |    Address    |       name       |num  | ID  |
|

------------------------------------------------------------------------------
   0       S     224.1.1.1        PROGRAM-0         0     10    disable
7

------------------------------------------------------------------------------
  Total: 1 program(s) (Static/Dynamic:
1/0)
  Note : # The program data is valid, but it is no
license.

huawei(config)#display igmp program index 0
 <cr>||
<K> }:


Command:
          display igmp program index 0

---------------------------------------------
  Program index           :
0
  Create mode             :
static
  Program name            :
PROGRAM-0
  IP address              :
224.1.1.1
  VLAN ID                 :
10
  Host attribute          :
enable
  Log attribute           :
enable
  Prejoin attribute       :
disable
  Unsolicited attribute   :
disable
  Priority                :
7
  Host IP                 :
0.0.0.0
  Bandwidth(kbps)         : 1024   //The bandwidth of the multicast program is
1 Mbit/s.
  SourceIP                :
-
  Preview Profile         :
0
  Numbers of watching     :
0
```

```
  Program Grade           :
-
  ------------------------------------------
```

6.2.5 (Optional) Configuring the 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 so that the user can determine whether to request for the program. The MA5616 can control the duration, interval, and count of user previews through the configuration of the multicast preview.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

Multicast preview is an advertising method provided by carriers for ISPs. The purpose is to allow users to have an overview of a program so that the user can determine whether to request for the program. To protect the legitimate interests of ISPs, the duration, interval, and count of user previews need to be controlled. The MA5616 controls the program preview of the user through the configuration of the multicast preview.

- Preview duration: After a user with the preview rights goes online, the user can watch the program that can be previewed but the user is restricted by the preview duration. When the preview time expires, the user will go offline.
- Preview interval: When the preview time expires, the user who is previewing a multicast program will go offline. The user can request for the program again only after the configured preview interval expires.
- Preview count: Refers to the count of program previews that a user can request for a multicast program in a period of 24 hours (the start time can be set). If the preview count reaches the configured preview count, the user cannot preview the program.

The multicast preview function is implemented through the binding of the preview profile to the multicast program.

NOTE

One multicast program can be bound with only one preview profile, but one preview profile can be referenced by multiple multicast programs.

Procedure

Step 1 In global config mode, run the **btv** command to enter BTV mode.

Step 2 Enable the multicast preview function globally.

NOTE

By default, the multicast preview function is enabled globally. You can run the **igmp preview { enable | disable }** command to change the configuration.

Step 3 Configure the preview profile.

Run the **igmp preview-profile add** command to configure the multicast preview profile.

The system has a default preview profile with index 0, which can only be modified and cannot be deleted.

Step 4 Bind the multicast program with the preview profile.

In multicast VLAN mode, run the **igmp program add ip***ip-addr***preview-profile***index* command to bind the preview profile to the multicast program so that the multicast program has the preview attributes defined in the preview profile.

By default, the multicast program is bound with the preview profile with index 0.

Step 5 Change the time for clearing the preview record.

Run the **igmp preview auto-reset-time** command to change the time for clearing the preview record. The system records only the preview of the multicast user on the current day.

By default, the system clears the preview record at 04:00:00.

Step 6 Modify the valid duration of the multicast preview.

Run the **igmp proxy recognition-time** command to modify the valid duration of the multicast preview. If the 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 the multicast preview is 30s.

----End

Example

Assume that the preview function of the multicast program is enabled, preview profile 1 is configured, the maximum preview duration is 150s, the maximum preview count is 10, this preview profile is used when program 224.1.1.1 is added, and other parameters use the default values. To perform the configurations, 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 10
huawei(config-mvlan10)#igmp program add ip 224.1.1.1 preview-profile 1
```

Result

Check whether the preview function of the multicast program is configured correctly.

- Check whether the preview function of the multicast program is enabled.

```
huawei(config)#display igmp config global

------------------------------------------------------------------------
  Authorization                         :
enable
  Robustness variable                   :
2
  General query interval(s)             :
125
  V2 General query response time(0.1s)  :
100
  V3 General query response time(0.1s)  :
100
  Specific query interval(0.1s)         :
10
  V2 Specific query response time(0.1s) :
8
  V3 Specific query response time(0.1s) :
8
  Specific query number                 :
```

```
2
  V2 router present timeout(s)          :
400
  User action report switch             :
disable
  Preview switch                        : enable  //The multicast preview
function is enabled.
  Recognition time(s)                   :
30
  The time of reset preview-count       :
04:00:00
  Auto create log interval(h)           :
2
  Uplink port mode                      :
default
  Bandwidth management switch           :
enable
  CDR auto report interval(s)           :
600
  CDR auto report number                :
200
  CDR switch                            :
disable
  IGMP Packet encapsulation             :
all
  IGMP ECHO switch                      :
disable
  Router IP                             :
192.168.1.1
  Initial unsolicited report interval(s):
1
  Query offline user switch             :
-
  BTV Forward Mode                      :
Mvlan
  ------------------------------------------------------------------------
```

- Check the configuration of the preview profile of the multicast program.

```
huawei(config)#display igmp preview-profile index 1
  Preview profile Index:           1
  Preview duration(s):           150  //The maximum preview duration is 150s.
  Preview interval(s):           120
  Preview times:                  10  //The maximum preview count is 10.
  Program reference number:        1
```

- Query the preview profile bound to the multicast program.

```
huawei(config)#display igmp program all
{ <cr>||
<K> }:


Command:
          display igmp program
all

--------------------------------------------------------------------------------
  Index| Create |      IP       |     Program      |User |VLAN |Prejoin|
Priority
       | Flag   |    Address    |       name       |num  | ID  |
|

--------------------------------------------------------------------------------
   0       S     224.1.1.1        PROGRAM-0         0     10    disable
7

--------------------------------------------------------------------------------
  Total: 1 program(s) (Static/Dynamic:
1/0)
  Note : # The program data is valid, but it is no
license.
```

```
The queried program index is 0.
huawei(config)#display igmp program index 0
{ <cr>||
<K> }:


Command:
          display igmp program index
0

-------------------------------------------
  Program index           :
0
  Create mode             :
static
  Program name            :
PROGRAM-0
  IP address              :
224.1.1.1
  VLAN ID                 :
10
  Host attribute          :
enable
  Log attribute           :
enable
  Prejoin attribute       :
disable
  Unsolicited attribute   :
disable
  Priority                :
7
  Host IP                 :
0.0.0.0
  Bandwidth(kbps)         :
5000
  SourceIP                :
-
  Preview Profile         : 1   //The index of the preview profile bound to the
multicast program is 1.
  Numbers of watching     :
0
  Program Grade           :
-
  -------------------------------------------
```

6.2.6 (Optional) Configuring the Program Prejoin

In program prejoin, the MA5616 receives the multicast stream of a program from the upper-layer multicast router to the uplink port before a user sends a request to join a program. In this manner, the multicast stream can be directly transmitted from the uplink port to the user port after the multicast user requests for a program, thus shortening the waiting time of the user for requesting for 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 MA5616 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 uplink port.

After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, you need to enable the unsolicited report function of IGMP packets so that the user can request for the program quickly. Generally, the upper-layer multicast router processes the user request by responding to the group-specific query and the general query.

Procedure

Step 1 Enable the program prejoin function.

Run the **igmp program add ip *ip-addr* prejoin enable** command to enable the program prejoin function.

By default, this function is disabled.

Step 2 After the program prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, you need to enable the unsolicited report function of IGMP packets.

- Run the **igmp program add ip ip-addr unsolicited enable** command to enable the unsolicited report function of IGMP packets. By default, this function is disabled.
- Run the **igmp unsolicited-report interval** command to change the interval of the unsolicited report of IGMP packets. By default, the time is 10s.

Step 3 Check whether the prejoin function is configured correctly.

- Run the **display igmp program** command to query the status of the program prejoin function and unsolicited report function.
- Run the **display igmp config vlan** command to query the interval of the unsolicited report of IGMP packets.

----End

Example

To enable the program prejoin function when adding a program whose IP address is 224.1.1.1, do as follows:

```
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp program add ip 224.1.1.1 prejoin enable
```

Result

Query the status of the program prejoin function and unsolicited report function.

```
huawei(config)#display igmp program all
{ <cr>||<K> }:

  Command:
          display igmp program all
  ------------------------------------------------------------------------------
  Index| Create |      IP       |     Program      |User |VLAN |Prejoin|Priority
       | Flag   |    Address    |       name       |num  | ID  |       |
  ------------------------------------------------------------------------------
   0       S     224.1.1.1        PROGRAM-0         0     10    disable    7
  ------------------------------------------------------------------------------
  Total: 1 program(s) (Static/Dynamic: 1/0)
  Note : # The program data is valid, but it is no license.

The queried program index is 0.
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#display igmp program index 0
{ <cr>||<K> }:
```

```
  Command:
          display igmp program index 0
  ------------------------------------------
  Program index           : 0
  Create mode             : static
  Program name            : PROGRAM-0
  IP address              : 224.1.1.1
  VLAN ID                 : 10
  Host attribute          : enable
  Log attribute           : enable
  Prejoin attribute       : enable   //The program prejoin function is enabled.
  Unsolicited attribute   : disable  //The unsolicited report function of IGMP
packets are disabled.
  Priority                : 7
  Host IP                 : 0.0.0.0
  Bandwidth(kbps)         : 5000
  SourceIP                : -
  Preview Profile         : 0
  Numbers of watching     : 0
  Program Grade           : -
  ------------------------------------------
```

6.2.7 (Optional) Configuring the Multicast Log

This topic describes how to configure the multicast log. Multicast log records the information about multicast programs watched by the multicast user, which provides a criterion for carriers to evaluate the viewership of multicast programs. The MA5616 can report the multicast log to the multicast server.

Prerequisites

The communication between the MA5616 and the multicast log server must be normal.

Context

The multicast log involves the multicast log of the multicast VLAN, multicast user, and multicast program. The system generates logs only when the log functions of all the multicast VLAN, multicast user, and multicast program are enabled.

If the online duration of the user is longer than the valid log generation time, the system generates logs in any of the following conditions:

- The user goes offline naturally, forcibly, or abnormally.
- The user is blocked or deleted.
- The program is deleted.
- The priority of the program is changed.
- The uplink port to which the program is bound is changed.
- The VLAN of the uplink port to which the program is bound is changed.
- The user preview times out.
- The rights mode is switched.
- The IGMP mode is switched.
- The bandwidth CAC fails.

The system supports a maximum of 32 k (1 k = 1024) 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 MA5616 can report the multicast log to the log server in syslog mode or in call detailed record (CDR) mode. By default, the MA5616 reports the log in 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.

Procedure

- Configure the parameters of the multicast log generation function of the MA5616.
  1. Enable the multicast log generation function.

     The multicast log involves the multicast log of the multicast VLAN, multicast user, and multicast program. The system generates logs only when the log functions of all the multicast VLAN, multicast user, and multicast program are enabled. By default, the log functions of all the multicast VLAN, multicast user, and multicast program are enabled.
     - In multicast VLAN mode, run the **igmp log { enable | disable }** command to configure the status of the log function of the multicast VLAN.
     - In BTV mode, run the **igmp user add service-port***index***log { enable | disable }** command to configure the status of the log function of the multicast user.
     - In multicast VLAN mode, run the **igmp program add ip***ip-addr***log { enable | disable }** command to configure the status of the log function of the multicast program.
  2. Change the interval of automatic log generation.

     In BTV mode, run the **igmp proxy log-interval** command to change the interval of automatic log generation.

     NOTE

     When the user stays online for a long time, the system generates logs at preset intervals. This prevents the problem that a log is not generated when the user leaves the multicast group without sending the leave packet, which can affect the accounting. By default, the interval is two hours.
  3. Change the minimum online duration for generating a valid log.

     In BTV mode, run the **igmp proxy recognition-time** command to change 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 duration is 30s.
- Configure the multicast log report function in CDR mode.
  1. Configure the multicast log server and the data transmission mode for the multicast log report in CDR mode.

     Run the **file-server auto-backup cdr** command to configure the active and standby multicast log servers.
  2. Enable the multicast log report function in CDR mode.

     In BTV mode, run the **igmp cdr { enable | disable }** command to configure the status of the multicast log report function in CDR mode.

- After the multicast log report function in CDR mode is enabled, the MA5616 reports local multicast logs to the multicast log server in the form of a file.
- After the multicast log report function in CDR mode is disabled, the MA5616 reports each single log to the syslog server in the default syslog mode.

3. Configure the parameters of the multicast log report in CDR mode.
   - In BTV mode, run the **igmp cdr-interval** command to configure the interval of the multicast log report in CDR mode. By default, the interval is 600s.
   - In BTV mode, run the **igmp cdr-number** command to configure the maximum number of logs that can be reported in CDR mode each time. When the number of multicast logs in the CDR file reaches the preset value, the MA5616 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 multicast log server for receiving the multicast log reported in CDR mode.
   - Run the **display igmp config global** command to query the status and other parameters of the multicast log report in CDR mode.

----End

Example

To configure the multicast log to be reported to log server 10.10.10.10 (active multicast log server) in CDR mode through TFTP transmission, do as follows:

```
huawei(config)#file-server auto-backup cdr primary 10.10.10.10 tftp
huawei(config)#btv
huawei(config-btv)#igmp cdr enable
```

Result

Query the configuration of the multicast log server for receiving the multicast log reported in CDR mode.

```
huawei(config)#display file-server auto-backup cdr
  --------------------------------------------------------------------------------
  Server type: Primary
  Trans mode : TFTP              //The transmission mode of the multicast log is
TFTP.
  IP address : 10.10.10.10       //The IP address of the multicast log server is
10.10.10.10.
  --------------------------------------------------------------------------------
  Current Server: Primary server
```

Query the status and other parameters of the multicast log report in CDR mode.

```
huawei(config)#display igmp config global
  ------------------------------------------------------------------------
  Authorization                         : enable
  Robustness variable                   : 2
  General query interval(s)             : 125
  V2 General query response time(0.1s)  : 100
  V3 General query response time(0.1s)  : 100
  Specific query interval(0.1s)         : 10
  V2 Specific query response time(0.1s) : 8
  V3 Specific query response time(0.1s) : 8
  Specific query number                 : 2
  V2 router present timeout(s)          : 400
  User action report switch             : disable
  Preview switch                        : enable
  Recognition time(s)                   : 30
  The time of reset preview-count       : 04:00:00
```

```
  Auto create log interval(h)           : 2
  Uplink port mode                      : default
  Bandwidth management switch           : enable
  CDR auto report interval(s)           : 600
  CDR auto report number                : 200
  CDR switch                           : enable  //The multicast log report in CDR
mode is enabled.
  IGMP Packet encapsulation             : all
  IGMP ECHO switch                      : disable
  Router IP                             : 192.168.1.1
  Initial unsolicited report interval(s): 1
  Query offline user switch             : -
  BTV Forward Mode                      : Mvlan
  ---------------------------------------------------------------------------
```

6.3 Configuring the Multicast Service on a Subtending Network

This topic describes how to configure the multicast service on the MA5616 on a subtending network.

Prerequisites

- Network devices and lines must be in the normal state.
- The multicast source must exist on the network and the IP address of the multicast source must be known.

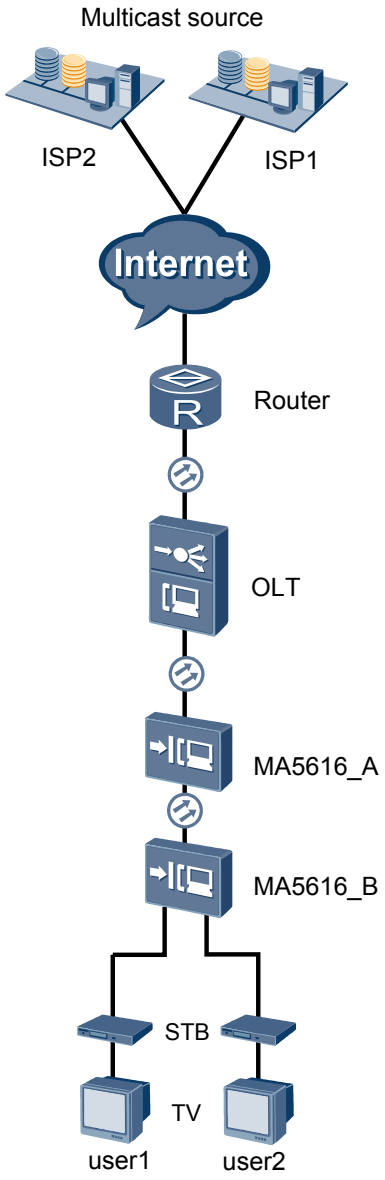
Context

When a subtended device needs to provide the multicast service, the subtending port on the subtending device needs to be configured as the multicast subtending port. In this manner, the subtended device regards the subtending device as an IGMP user.

Networking

Figure 6-1 shows the example network of the multicast service in subtending networking mode.

Figure 6-1 Example network of the multicast service in subtending networking mode



Data Plan

Table 6-3 provides the data plan for configuring the multicast service in subtending networking mode.

Table 6-3 Data plan for configuring the multicast service in subtending networking mode

Device	Item	Data
MA5616_A	Smart VLAN	● VLAN type: Smart VLAN ● VLAN ID: 4002-4003
	Uplink port	0/0/1

Device	Item	Data
	Subtending port	0/0/0
	IGMP version	IGMP V3 (default multicast version of the system in multicast VLAN mode)
	Multicast source	There are two multicast sources, namely, ISP 1 and ISP 2. ● ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ● ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
	Program library	Program in multicast VLAN 4002: Program 1: with IP address 224.1.1.1 and the IP address of the program source is the same as the IP address of ISP 1, namely, 10.10.10.10
		Program in multicast VLAN 4003: Program 2: with IP address 224.1.1.2 and the IP address of the program source is the same as the IP address of ISP 2, namely, 10.10.10.11
MA5616_B	Smart VLAN	● VLAN type: Smart VLAN ● VLAN ID: 4002-4005
	Uplink port	0/0/0
	IGMP version	IGMP V3 (default multicast version of the system in multicast VLAN mode)
	Multicast source	There are two multicast sources, namely, ISP 1 and ISP 2. ● ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ● ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
	Program library	Program in multicast VLAN 4002: Program 1: with IP address 224.1.1.1 and the IP address of the program source is the same as the IP address of ISP 1, namely, 10.10.10.10
		Program in multicast VLAN 4003: Program 2: with IP address 224.1.1.2 and the IP address of the program source is the same as the IP address of ISP 2, namely, 10.10.10.11
	Multicast user	Multicast user 1: ● VDSL2 port: 0/1/0 ● Multicast VLAN: 4002

Device	Item	Data
		Multicast user 2: ● VDSL2 port: 0/1/1 ● Multicast VLAN: 4003

Procedure

- **Configure the multicast service on MA5616_A.**

  1. Create VLANs.

     ```
     huawei(config)#vlan 4002-4003 smart
     ```

  2. Add the uplink port and the subtending port to the VLANs.

     ```
     huawei(config)#port vlan 4002-4003 0/0 1
     huawei(config)#port vlan 4002-4003 0/0 0
     ```

  3. Configure multicast VLANs and the IGMP mode.

     NOTE

     The IGMP mode can be configured to IGMP proxy or IGMP snooping according to the requirements. In this example, the IGMP mode is IGMP proxy. If the planned IGMP mode is IGMP snooping, you can configure the IGMP snooping mode by running the **igmp mode snooping** command in multicast VLAN mode.

     If configuring the IGMP mode fails, check whether the IGMP function is disabled. That is, the IGMP mode can be switched only when the IGMP function is disabled.

     ```
     huawei(config)#multicast-vlan 4002
     huawei(config-mvlan4002)#igmp mode proxy
       Are you sure to change IGMP mode?(y/n)[n]:y
     huawei(config-mvlan4002)#multicast-vlan 4003
     huawei(config-mvlan4003)#igmp mode proxy
       Are you sure to change IGMP mode?(y/n)[n]:y
     ```

  4. Configure the multicast uplink port.

     ```
     huawei(config-mvlan4003)#igmp uplink-port 0/0/1
     huawei(config-mvlan4003)#multicast-vlan 4002
     huawei(config-mvlan4002)#igmp uplink-port 0/0/1
     ```

  5. Configure multicast programs.

     NOTE

     - A multicast program can be configured statically or generated dynamically. In this example, the multicast program is configured statically.
     - In static configuration mode, you can run the **igmp program add** command to add multicast programs in batches. You cannot name a program, instead the system automatically names a program PROGRAM-M, in which M is the index of the added program.

     ```
     huawei(config-mvlan4002)#igmp program add name program1 ip 224.1.1.1
     sourceip 10.10.10.10
     huawei(config-mvlan4002)#multicast-vlan 4003
     huawei(config-mvlan4003)#igmp program add name program2 ip 224.1.1.2
     sourceip 10.10.10.11
     huawei(config-mvlan4003)#quit
     ```

  6. Configure the multicast subtending port.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp cascade-port 0/0/0
     ```

  7. Save the data.

```
huawei(config-btv)#quit
huawei(config)#save
```

- **Configure the multicast service on MA5616_B.**

  1. Create VLANs and add an uplink port to the VLANs.

     ```
     huawei(config)#vlan 4002-4005 smart
     huawei(config)#port vlan 4002-4005 0/0 0
     ```

  2. Configure service ports.

     ```
     huawei(config)#service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
     huawei(config)#service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
     ```

  3. Configure multicast VLANs and the IGMP mode.

     NOTE

     The IGMP mode can be configured to IGMP proxy or IGMP snooping according to the requirements. In this example, the IGMP mode is IGMP proxy. If the planned IGMP mode is IGMP snooping, you can configure the IGMP snooping mode by running the **igmp mode snooping** command in multicast VLAN mode.

     ```
     huawei(config)#multicast-vlan 4002
     huawei(config-mvlan4002)#igmp mode proxy
       Are you sure to change IGMP mode?(y/n)[n]:y
     huawei(config-mvlan4002)#multicast-vlan 4003
     huawei(config-mvlan4003)#igmp mode proxy
       Are you sure to change IGMP mode?(y/n)[n]:y
     ```

  4. Configure the multicast uplink port.

     ```
     huawei(config-mvlan4003)#igmp uplink-port 0/0/0
     huawei(config-mvlan4003)#multicast-vlan 4002
     huawei(config-mvlan4002)#igmp uplink-port 0/0/0
     ```

  5. Configure multicast programs.

     NOTE

     - A multicast program can be configured statically or generated dynamically. In this example, the multicast program is configured statically.
     - In static configuration mode, you can run the **igmp program add** command to add multicast programs in batches. You cannot name a program, instead the system automatically names a program PROGRAM-M, in which M is the index of the added program.

     ```
     huawei(config-mvlan4002)#igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
     huawei(config-mvlan4002)#multicast-vlan 4003
     huawei(config-mvlan4003)#igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
     ```

  6. Configure multicast users.

     ```
     huawei(config-mvlan4003)#igmp multicast-vlan member service-port 101
     huawei(config-mvlan4003)#multicast-vlan 4002
     huawei(config-mvlan4002)#igmp multicast-vlan member service-port 100
     huawei(config-mvlan4002)#btv
     huawei(config-btv)#igmp user add service-port 100
     huawei(config-btv)#igmp user add service-port 101
     huawei(config-btv)#quit
     ```

  7. Save the data.

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

----End

Result

- User 1 belongs to multicast VLAN 4002 and user 1 can watch the program with IP address 224.1.1.1 provided by ISP1.
- User 2 belongs to multicast VLAN 4003 and user 2 can watch the program with IP address 224.1.1.2 provided by ISP2.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps need to be performed manually and the configuration file cannot be imported directly.

MA5616_A

Create VLANs and add the uplink port and the subtending port to the VLANs. This step needs to be performed manually.

```
vlan 4002 to 4003 smart
port vlan 4002 to 4003 0/0 1
port vlan 4002-4003 0/0 0
```

Configure multicast VLANs and the IGMP mode. This step needs to be performed manually.

```
multicast-vlan 4002
igmp mode proxy
multicast-vlan 4003
igmp mode proxy
```

Configure the multicast uplink port, multicast programs, and multicast subtending port.

```
igmp uplink-port 0/0/1
multicast-vlan 4002
igmp uplink-port 0/0/1
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
multicast-vlan 4003
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp cascade-port 0/0/0
quit
save
```

MA5616_B

Create VLANs and add an uplink port to the VLANs. This step needs to be performed manually.

```
vlan 4002 to 4005 smart
 port vlan 4002 to 4005 0/0 0
```

Create service ports.

```
service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-
cttr 6 tx-cttr 6
 service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-vlan untagged rx-
cttr 6 tx-cttr 6
```

Configure multicast VLANs and the IGMP mode. This step needs to be performed manually.

```
multicast-vlan 4002
igmp mode proxy
multicast-vlan 4003
igmp mode proxy
```

Configure the multicast uplink port, multicast programs, and multicast users.

```
igmp uplink-port 0/0/0
multicast-vlan 4002
igmp uplink-port 0/0/0
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
multicast-vlan 4003
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
```

```
igmp user add service-port 100
igmp user add service-port 101
multicast-vlan 4002
igmp multicast-vlan member service-port 100
multicast-vlan 4003
igmp multicast-vlan member service-port 101
quit
save
```

7 Configuring the Voice Service

About This Chapter

The MA5616 supports user access through copper cables to provide the voice service.

Context

The MA5616 can provide the voice service through the H.248 or Session Initiation Protocol (SIP) protocol.

- The system communicates with the media gateway controller (MGC) through the H.248 protocol, and provides the voice service under the control of the MGC.
- The system communicates with the IP multimedia subsystem (IMS) core network device through the SIP protocol to provide the voice service.

The MA5616 supports the following services:

- Voice over IP (VoIP) service

  Supports the voice over IP service through the H.248 or SIP protocol.
- VoIP integrated services digital network (ISDN) basic rate access (BRA) service

  Supports the ISDN BRA over IP service through the H.248 protocol.
- Fax over IP (FoIP) service

  Supports the fax over IP service through the H.248 or SIP protocol.
- Modem over IP (MoIP) service

  Supports the modem over IP service through the H.248 or SIP protocol.

To ensure the normal voice service, the MA5616 supports the following security and reliability configurations:

- Device authentication

  Supports authentication of the MG interface through the H.248 protocol and authentication of the SIP interface through the SIP protocol.
- Emergency standalone

  Supports emergency standalone of the MG interface through the H.248 protocol.

- Dual homing

  Supports dual homing from the MG to the MGC through the H.248 protocol and authentication from the SIP AG to the SIP proxy server through the SIP protocol.

NOTE

In this document, the MG, AG, gateway, or SIP AG refers to the MA5616, unless otherwise stated.

The voice pre-configuraiton profile of the MA5616 supports the configuration of main voice parameters through a single command.

- Run the **voice-para-template** command to select the parameter profile for an area to quickly configure the voice service. Run the **display voice-para-template(sip)** and **display voice-para-template(H248)** commands to query the parameter configurations for different areas.
- When the parameter configurations defined in the system do not meet the requirements, run the **userdef-template-port-para** command to modify the parameter configurations in the user defined parameter profile.
- If you do not use the voice configuration profile, configure the voice parameters one by one by following the configuration steps in the next topics.

7.1 Configuring the VoIP PSTN Service (Based on the H.248 Protocol)
This topic describes how to configure the VoIP PSTN service on the MA5616 when the H.248 protocol is used.

7.2 Configuring the VoIP PSTN Service (Based on the SIP Protocol)
This topic describes how to configure the VoIP PSTN service on the MA5616 through the Session Initiation Protocol (SIP).

7.3 Configuring the VoIP ISDN BRA Service
This topic describes how to configure the VoIP ISDN BRA service on an IP network. When the MA5616 uses the H.248 protocol, the device supports the access of the ISDN BRA user. ISDN technology provides end-to-end (E2E) digital connection and supports multiple types of voice and non-voice telecom services.

7.4 Configuring the FoIP Service (Based on the H.248 Protocol)
This topic describes how to configure the FoIP service when the H.248 protocol is used to transmit the fax data service over the IP network.

7.5 Configuring the FoIP Service (Based on the SIP Protocol)
This topic describes how to configure the FoIP service based on the SIP protocol to transmit the fax data service over the IP network.

7.6 Configuring the MoIP Service (Based on the H.248 Protocol)
This topic describes how to configure the MoIP service when the H.248 protocol is used to transmit the modem data service over the IP network.

7.7 Configuring the MoIP Service (Based on the SIP Protocol)
This topic describes how to configure the MoIP service when the SIP protocol is used to transmit the modem data service over the IP network.

7.8 Configuring the Security and Reliability of the Voice Service
For the MA5616, the security configuration of the voice service includes the H.248-based, or SIP-based device authentication configuration. The reliability configuration of the voice service includes the dual-homing configuration and the emergency standalone configuration.

7.1 Configuring the VoIP PSTN Service (Based on the H.248 Protocol)

This topic describes how to configure the VoIP PSTN service on the MA5616 when the H.248 protocol is used.

Context

The voice over IP (VoIP) service uses the IP packet switching network for transmission after the traditional analog voice signals are compressed and packetized, to reduce the cost of the voice service.

For details about the VoIP service, see Voice in the *Feature Description*.

In the NGN network, the MA5616 functions as an access gateway (AG) and exchanges signaling with the media gateway controller (MGC) through the media gateway control protocol (the H.248 protocol). In this manner, 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 MA5616 (AG) and the MGC, plays a decisive role in the VoIP service based on the H.248 protocol. 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 the MGCP protocol by combining the features of other media gateway control protocols. Compared with the MGCP protocol, the H.248 protocol supports more types of access technologies and supports mobility of terminals. The configuration of the VoIP service based on the H.248 protocol is the same as the configuration of the VoIP service base on the MGCP protocol.

Prerequisite

According to the actual network, a route from the MA5616 to the MGC must be configured to ensure that the MA5616 and the MGC are reachable to each other.

Precaution

The media gateway control protocols 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 consistent with the corresponding data on the MGC. Before configuring the VoIP service, you must make the data plan by considering interconnection with the MGC.

Data preparation

Table 7-1 provides the data plan for configuring the VoIP PSTN service.

Table 7-1 Data plan for configuring the VoIP PSTN service based on the H.248 protocol

Item			Remarks
MG interface data (The data configuration must be consistent with the data configuration on the MGC.)	Parameters of the media stream and signaling stream	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 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 consist of all the IP addresses of the L3 interface of the media and signaling upstream VLAN.
		Default IP address of the MG	It is the IP address of the next hop from the MA5616 to the MGC.
	Attribute parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be started if these parameters are not configured.	MG interface ID	It is the MG interface ID used for the VoIP service to be configured. The MA5616 supports only one virtual access gateway (VAG).
		Signaling port ID of the MG interface	It is the transport layer protocol port ID used for the signaling exchange between the MA5616 (AG) and the MGC. Default signaling port ID specified in the H.248 protocol: 2944 (text) and 2945 (binary)
		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	
		Coding mode of the MG interface	Currently, only the **text** coding mode is supported.
		Transmission mode of the MG interface	The transmission mode is selected according to the requirements on the MGC side. Generally, UDP is adopted.

Item			Remarks
		Domain name of the MG interface	It corresponds to parameter **domainName** of the MG interface. When the H.248 protocol is used, this parameter must be configured if parameter **MIDType** of the H.248 message is configured as the domain name. Otherwise, the MG interface fails to be started. In other situations, this parameter is optional.
		Device name of the MG interface	It is supported only by the H.248 protocol, and corresponds to 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 parameter **MIDType** of the H.248 message is configured as the domain name. Otherwise, the MG interface fails to be started. In other situations, this parameter is optional.
		Start negotiation version of the H.248 protocol for the MG interface	It is recommended that you configure this parameter to 0, which indicates the negotiation is performed according to the profile. If the MGC interconnected with the MG is provided by another vendor, the profile must be configured.
	Digitmap of an 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 sent to the AG by the MGC, and therefore such digitmaps need not be configured on the AG. If the services such as emergency calls and emergency standalone are not required, the digitmaps need not be configured.
	Software Parameters of an 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 an MG Interface		According to the service requirements, the ringing modes of the MG interface need to be determined.

Item			Remarks
	TID Format of an MG Interface		The TID format determines the generation mode of various types of user terminals on an MG interface.
Voice service data (The data configuration must be consistent with the data configuration on the MGC.)	Slot that houses 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.
		User priority	According to the service requirements, the user priority needs to be specified. The user priorities are as follows: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: normal (common users, default priority in the system)
		User type	According to the service requirements, the user type needs to be specified. The user types are as follows: ● DEL: direct exchange lines (default type in the system) ● 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.

Item		Remarks
	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.
	Local Digitmap	Configure a proper local digitmap according to the local standards. If the MGC does not send the detailed digitmap to the MA5616, the MA5616 uses the local digitmap to match the phone number. **CAUTION** If the H.248 protocol is used, the local digitmap need not be configured by default. You can configure the local digitmap according to the requirements.
	Attributes of a PSTN Port	If the PSTN port needs to support the polarity reversal charging, the PSTN port needs to be configured to support the polarity reversal pulse. Other attributes need not be modified if there is no special requirement.
	Attributes of the Ringing Current	You can adjust the ringing tone volume by modifying the attributes of the ringing current. Generally, the attributes of the ringing current need not 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.

7.1.1 Configuring an MG Interface

This topic describes how to configure an MG interface for implementing the communication between the MA5616 (AG) and the MGC.

Context

- The MA5616 communicates with the MGC through the MG control protocol, that is, the H.248 protocol.
- One MA5616 supports up to one MG interface. The MG interface can be configured with the attributes such as authentication and ringing mapping.

7.1.1.1 Configuring the Upstream VLAN Interface

This topic describes how to specify the upstream VLAN interface for the media stream and signaling stream, and how to configure the IP addresses of the L3 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 L3 interface. Only one IP address functions as the primary address, and other IP addresses function as the secondary addresses.

Procedure

Step 1 Add an upstream VLAN.

Run the **vlan** command to add an upstream VLAN for the media stream and signaling stream.

Step 2 Add an upstream port to the VLAN.

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

Step 3 Configure the IP addresses of the VLAN L3 interface.

1. Run the **interface vlanif** command to enter the L3 interface of the upstream VLAN for the media stream and signaling stream.
2. Run the **ip address** command to configure the IP addresses of the L3 interface.

Step 4 Check whether the IP addresses of the L3 interface are the same as those in the data plan.

Run the **display interface vlanif** command to check whether the IP addresses of the L3 interface are the same as those in the data plan.

----End

Example

Assume that the media stream and signaling stream are transmitted upstream through upstream port 0/0/1. 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 L3 interfaces for the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/0 1
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
```

7.1.1.2 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 L3 interface of the media and signaling upstream VLAN must be configured. For details about how to configure the IP address, see **7.1.1.1 Configuring the Upstream VLAN Interface**.

Context

- The media IP address and the signaling IP address for the MG or SIP 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 or SIP 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.

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 L3 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 L3 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

Assume that the IP address of the gateway is 10.13.1.1. To add IP addresses 10.13.4.116 and 10.13.4.117 of L3 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 10.13.1.1
huawei(config-voip)#ip address media 10.13.4.117 10.13.1.1
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..............: 10.13.1.1
```

```
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.1.1
  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
```

7.1.1.3 Adding an MG Interface

This topic describes how to add an MG interface, through which the MA5616 can communicate with the MGC.

Context

One MA5616 supports up to one MG interface.

Procedure

Step 1 Add an MG interface.

Run the **interface h248** command to add an MG interface that supports H.248 protocol.

Step 2 Configure the attribute of the MG interface.

Run the **if-h248 attribute** command to configure the attribute of the MG interface according to the data plan.

An MG interface is reset successfully only when **mgip** (or **domainName** and **deviceName**), **mgport**, **primary-mgc-ip1** (or **mgc-domain-name1**), **primary-mgc-port**, **code**, **transfer**, and **mg-media-ip1** are configured successfully.

Table 7-2 lists the MG interface parameters you need to pay attention to when configuring the parameters for interconnection between the MG and the MGC.

Table 7-2 MG interface parameters

Parameter	Remarks
mgport	Indicates the transport layer protocol port ID used for the signaling exchange between the MA5616 (AG) and the MGC. The default signaling port ID defined in H.248 is 2944 (text) and 2945 (binary).
primary-mgc-ip1	When dual homing is not configured, you can configure the parameters of only one MGC. When dual homing is configured, you need to configure the IP address and port ID of the secondary MGC.
primary-mgc-port	

Parameter	Remarks
code	The coding modes of the MG interface and the MGC must be the same. Currently, only text coding mode is supported.
transfer	The transmission mode is selected according to the requirements of the MGC. Generally, UDP is used.
start-negotiate-version	If the MGC connecting to the MG is a Huawei device, the profile (parameter profile-index) does not need to be set; if the MGC connecting to the MG is a device of another vendor, the profile (parameter profile-index) must be set (the parameter value is prompted on the CLI). If the profile file in the system cannot meet requirements, contact Huawei for technical support.

Step 3 Check whether the attribute of the MG interface is the same as that in the data plan.

Run the **display if-h248 attribute** command to check whether the attribute of the MG interface is the same as that in the data plan.

----End

Example

Assume that the MG interface ID is 0, the H.248 protocol is used for interconnecting with the MGC, the signaling IP address is 10.13.4.116, the transport layer protocol port ID is 2944, IP address 1 of the primary MGC is 10.13.2.118, the transport layer protocol port ID of the primary MGC is 2944, media IP address 1 is 10.71.46.69, media IP address 2 is 10.13.4.117, the H.248 protocol version is started to be negotiated based on the profile, the transaction reliability is enabled. To add such an MG interface, do as follows:

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute  mgip 10.13.4.116 mgport 2944 code text
primary-mgc-ip1 10.13.2.118 primary-mgc-port 2944 mg-media-ip1 10.71.46.69
mg-media-ip2 10.13.4.117 start-negotiate-version 0 retrans enable
huawei(config-if-h248-0)#display if-h248 attribute
-------------------------------------------------
  MGID                                0
  MG Description                      -
  MG DomainName                       -
  Protocol                            H248
  Start Negotiate Version             0
  Profile Negotiation Parameter       Disable
  Profile index                       1:NoProfile("")
  2833Encrypt                         -
  Codetype                            Text
  Transfer Mode                       -
  HeartBeatGenTimer(s)                60
  HeartBeatRetransTimes               3
  HeartBeatRetransTimer(s)            60
  MG signalling IP                    10.13.4.116
```

```
  MG signalling Port                    2944
  MG media IP1                          10.71.46.69
  MG media IP2                          10.13.4.117
  MIDType                               IP4_ADDR
  DeviceName                            -
  Retrans                               Enable

  Active MGC       MGC Port       :2944            MGC IP1:10.13.2.118
  Active MGC       MGC Port       :2944            MGC IP2:-
  Active MGC       MGC Domain Name:-
  Standby MGC      MGC Port       :-               MGC
IP1:-
  Standby MGC      MGC Port       :-            MGC IP2:-
  Standby MGC      MGC Domain Name:-
  ------------------------------------------------
```

7.1.1.4 (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 need not be configured on the AG. If the services such as emergency calls and emergency standalone are not required, the digitmaps need not be configured.

Context

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) before configuring the digitmap.

- 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, it indicates that 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 call digitmap (due to call restriction in the case of an overload)
- Automatic redial digitmap of the card service

Table 7-3 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 7-3 Digitmap format in the H.248 protocol

Digit or Character	Description
0-9	Indicate dialed digits 0-9.
A-D	Indicate 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.
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. The short timer is applied when the collected number matches at least one dialing scheme, but more numbers may be received and these numbers match other dialing schemes.
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. The long timer is applied when the dialed number does not match any dialing scheme.
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.

Procedure

Step 1 Enter the MG interface mode.

In global config mode, run the **interface h248** command to enter the MG interface mode.

Step 2 Configure the digitmap.

Run the **digitmap set** command to configure the digitmap required in the data plan.

Step 3 (Optional) Configure the digitmap timer.

Run the **digitmap-timer** command to configure the digitmpa timer.

Generally, the digitmap 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.

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
  Urgent digitmap (for overload or bandwidth restrict)    : -
  Dualdial digitmap for card service                      : -
  ------------------------------------------------------------------------
```

7.1.1.5 (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 36 software parameters (numbered from 0 to 35) of an MG interface that supports H.248. **Table 7-4** lists the configurable parameters, and the other parameters are reserved in the system.

Table 7-4 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. This parameter can be configured only when the MG interface is in the local closed state. If the MG interface does not support dual homing, 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, even if the MG interface has registered with the secondary MGC, the MG interface can automatically switch back to the primary MGC if the primary MGC recovers. If the MG interface supports dual homing, you can run the **mgc_switch(h248)** command to perform the MGC switching.	Numeral type. Range: 0-2. ● 0: Indicates that dual homing is not supported. ● 1: Indicates that dual homing rather than auto-switching is supported. ● 2: Indicates that dual homing and auto-switching is supported. Default: 0

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. This parameter can be configured only when the MG interface is in the local closed state. When a wildcard is used for registration, all the terminals connecting to the MG interface register with the MGC through a message. This reduces 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".	Numeral type. Range: 0-1. ● 0: Indicates that a wildcard is used. ● 1: Indicates that a wildcard is not used. Default: 0
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 (h248)** command to configure the authentication parameters, and then run the **reset(h248)** 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. **CAUTION** Resetting the MG interface may interrupt the services.	Numeral type. Range: 0-1. ● 0: Indicates that device authentication is supported. ● 1: Indicates that device authentication is not supported. Default: 1

Parameter	Description	Default Setting
7	Indicates whether the MG interface supports security header. To configure an MG interface to or not to support security header, use this parameter. After configuring the security header, run the **auth(h248)** command to configure the authentication parameters, and then run the **reset(h248)** command to reset the MG interface. In this case, the MGC can manage the MG devices in a security manner, ensuring that the data is complete.	Numeral type. Range: 0-1. ● 0: Indicates that security header is supported. ● 1: Indicates that security header is not supported. Default: 1
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.	Numeral type. Range: 0-3. ● 0: Indicates that no call is permitted. ● 1: Indicates that only internal call is permitted. ● 2: Indicates that only emergency call is permitted. ● 3: indicates that internal call and emergency call are permitted. Default: 0

Parameter	Description	Default Setting
13	Indicates the maximum digitmap matching flag of the MG interface. To configure digitmap matching scheme of the MG interface, use this parameter. In the shortest matching, the collected phone number is reported immediately after it matches the digitmap. This is the quickest report mode. In certain cases, however, the phone number is reported before it is collected completely. In the longest matching, even if the collected phone number matches a dialing scheme, the phone number is not reported because more numbers may be received. If there is no dialing within the duration of the short timer (default: 5s), the phone number is reported after the short timer times out. Otherwise, the system matches other digitmap schemes. You can run the **digitmap-timer** command to configure the time length of the digitmap timer.	Numeral type. Range: 0-1. ● 0: Indicates that the match follows the protocol. ● 1: Indicates the longest match. ● 2: Indicates the shortest match. Default: 2
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.	Numeral type. Range: 0-1. ● 0: Indicates that media streams are not filtered by source port. ● 1: Indicates that media streams are filtered by source port. Default: 0

Parameter	Description	Default Setting
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 the function of filtering media streams by source port is disabled, the MG interface automatically filters the source port if the filtering timer times out.	Numeral type. Range: 0-30s. Default: 5s
22	Indicates the type of the prompt tone after the communication between the MG and the MGC is interrupted.	Numeral type. Range: 0-2. ● 0: Indicates the busy tone. ● 1: Indicates the device congestion tone. ● 2: Indicates the voice prompt. Default: 0
23	Indicates the length of the timer for synchronizing the port status.	Numeral type. Range: 0-120s. Default: 35s.
24	Indicates the maximum value of the Real-Time Transport Protocol (RTP) termination ID. The maximum values of RTP termination ID on the MG and the MGC must be the same.	Numeral type. Range: 0-65535.
25	Indicates the maximum random value for the protection against avalanche of the H.248 interface.	Numeral type. Range: 30000-300000ms.
26	Indicates the type of local blocking play tone.	Numeral type. Range: 0-4. ● 0: Indicates the busy tone. ● 1: Indicates the device congestion tone. ● 2: Indicates the mute. ● 3: Indicates the user-defined tone 1. ● 4: indicates the user-defined tone 2. Default: 0

Parameter	Description	Default Setting
27	Indicates the type of remote blocking play tone.	Numeral type. Range: 0-4. ● 0: Indicates the busy tone. ● 1: Indicates the device congestion tone. ● 2: Indicates the mute. ● 3: Indicates the user-defined tone 1. ● 4: Indicates the user-defined tone 2. Default: 0.
28	Indicates the duration of the howler tone.	Numeral type. Range: 1-65535s. Default: 60s
29	Indicates the duration of message waiting tone.	Numeral type. Range: 1-60000s. Default: 3s
30	Indicates the time limit of the alarm for extra long call.	Numeral type. Range: 1-65535 min. Default: 60 min.
31	Indicates whether to report the alarm for extra long call.	Numeral type. Range: 0-1. ● 0: Indicates that the alarm is reported. ● 1: Indicates that the alarm is not reported. Default: 1
32	Indicates the minimum interval for automatic registration of the remote block port. The MG interface is blocked because the MGC does not respond or responds incorrectly. After this parameter is configured, the MG interface can automatically register with the MGC.	Numeral type. Range: 0-60000s. 0 indicates that the port does not register automatically. Default: 1800s
33	Indicates whether the heartbeat message is disabled.	Numeral type: ● 0: Indicates that the heartbeat message is disabled. ● 1: Indicates that the heartbeat message is enabled. Default: 1

Parameter	Description	Default Setting
34	Indicates whether the MG actively establishes or releases the link for the BRA user after the MGC initiates the in-service or OOS request.	Numeral type. Range: 0-1. ● 0: Yes ● 1: No Default value: 0.
35	Indicates the out of service (OOS) and in-service mode of the ISDN port. ● When the OOS or in-service in wildcard mode is supported, the ISDN port reports the in-service or OOS, that is, reports only one in-service or OOS message in wildcard mode. This effectively reduces the messages between the MG interface and the MGC. ● When the in-service or OOS in single channel mode is supported, the ISDN port reports the in-service or OOS message over each channel. ● When both the in-service or OOS in single channel mode and the in-service or OOS in wildcard mode are supported, the in-service or OOS message is reported according to the actual requirement or reported in single channel mode.	Numeral type. Range: 0-2. ● 0: Indicates that both the OOS or in-service in single channel mode and the OOS or in-service in wildcard mode are supported. ● 1: Indicates that only the OOS and in-service in single channel mode is supported. ● 2: Indicates that only the OOS and in-service in wildcard mode is supported. Default value: 1.

Procedure

Step 1 Enter the MG interface mode.

In global config mode, run the **interface h248** command to enter the MG interface mode.

Step 2 Configure software parameters.

Run the **mg-software parameter** command the software parameters required in the data plan.

Step 3 Check whether the software parameters are the same as those in the data plan.

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
```

7.1.1.6 (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.

Context

Add the ringing mode mapping records of a specified MG interface. After the adding is successful, the MG interface can obtains the ringing mode according to the peer parameters issued by the MGC and then play the ringing to the user in this mode.

Procedure

Step 1 Check whether the ringing mode meets the requirements.

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**.

Step 2 Configure the user-defined ringing mode.

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

The system supports 16 user-defined ringing modes, which can be modified but cannot be added or deleted.

Step 3 Enter the MG interface mode.

Run the **interface h248** command to enter the MG interface mode.

Step 4 Add a ringing mapping.

Run the **mg-ringmode add** command to add a ringing mapping.

CAUTION

1. The peer parameter *mgcpara* that is on the MG and issued by the MGC 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.

Step 5 Check whether the ringing mapping is the same as that in the data plan.

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
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> }:
```

```
Command:
        display mg-ringmode attribute
------------------------------------------------------
 MGID       PeerPara   CadenceRing   InitialRing
------------------------------------------------------
 0          1          128           144
------------------------------------------------------
```

7.1.1.7 (Optional) Configuring the TID Format of an MG Interface

The TID format determines how various user terminal IDs on the MG interface are generated.

Context

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 before configuring the TID format.

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", it indicates that 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), it indicates that 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 shelf 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 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** 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.

Precaution

- 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

Step 1 To query the template information.

Run the **display tid-template** command to query the information about the default TID template of the system.

Step 2 Check whether the default TID template of the system meets the service requirements.

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**.

Step 3 Enter the MG interface mode.

Run the **interface h248** command to enter the MG interface mode.

Step 4 Configure the TID templates and the terminal prefix of various types of users on the current MG (VAG).

- In H248 mode, run the **tid-format rtp** command to configure the TID template and terminal prefix of the RTP ephemeral termination.
- In H248 mode, run the **tid-format pstn** command to configure the TID template and terminal prefix of the PSTN user.
- In H248 mode, run the **tid-format pstn** command to configure the TID template and the terminal prefix of the ISDN BRA user.
- In H248 mode, run the **tid-format pstn** command to configure the TID template and terminal prefix of the ISDN PRA user.

Step 5 Check whether the TID template and the terminal prefix are the same as those in the data plan.

Run the **display tid-format** 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 the TID
template 3.
  -------------------------------------------------
  Index      : 3
  Format     : %u/%u/%u
  Para-list  : F+1,S+1,P+1  // Keywords in the parameter list of the TID template
are "F", "S", and "P".
  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><Length
1-15> }:

  Command:
          display mgpstnuser 0/2/0
  ------------------------------------------------------------------------------
  F  /S /P    MGID     TelNo            Priority PotsLineType     TerminalID
  ------------------------------------------------------------------------------
  0  /2 /0    1        -                Cat3     DEL              aln/1/3/1
  ------------------------------------------------------------------------------
```

7.1.1.8 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.

Precaution

CAUTION

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

Step 1 Enter the H248 mode.

Run the **interface h248** command to enter the H248 mode.

Step 2 Enable the MG interface.

Run the **reset coldstart** command to enable the MG interface.

Step 3 Check the state of the MG interface.

You can query the status of the MG interface by using one of the following two methods.

- Run the **display if-h248 state** command to check whether the MG interface is in the normal state.
- Run the **quit** command to quit the global config mode, and then run the **display if-h248 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
-------------------------------------------------------------------------------
```

7.1.2 Configuring the VoIP PSTN User

After an MG interface is configured, you can add public switched telephone network (PSTN) users on the MG interface to implement the VoIP service.

7.1.2.1 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 so that the POTS terminal can access the network to implement the VoIP service.

Prerequisites

The POTS service board must be inserted into the planned slot.

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 7-5 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 7-5 Default settings of the attributes of the PSTN user

Parameter	Default Setting
Sequence of sending the phone number of the calling party	Ringing and then sending the phone number
Format of the phone number of the calling party	SDMF (FSK single data message format)

Parameter	Default Setting
Whether to support the detection of the ANSbar signal through monophony	Not support
Whether to support the bell ANS signal	Not support
Power-off interval	100 ms
FSK delay interval	800 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 dBm
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.)
FSK-mode	BELL_202
TAS-mode	NO-TAS

Procedure

Step 1 In global config mode, run the **board confirm** command to confirm the service board.

Step 2 Add a PSTN user.

1. In 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, **terminalid** must be configured and must be different from the TID 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 TID is not required because the system automatically allocates the TID 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 configured phone number, however, can be used only as the paging number for emergency standalone. It is recommended that you configure the phone number to be the same as the phone number allocated by the MGC. In addition, the phone number must be unique on the MG. This prevents number conflict when emergency standalone is enabled. If this parameter is not set, the phone number is null by default. Phone numbers for normal call services are allocated by the MGC, generally, no telephone number (namely, parameter telno) is configured on the MG.
- For details about the relation between the TID template and the terminal layering, see the Context in **7.1.1.7 (Optional) Configuring the TID Format of an MG Interface**.

3. Run the **display mgpstnuser** command to check whether the configured PSTN user data is the same as the planned data.

Step 3 (Optional) Configure the attributes of a PSTN user.

The attributes of a PSTN user need to be configured only when the default settings are inconsistent with the actual application.

1. Run the **mgpstnuser attribute set** or **mgpstnuser attribute batset** command to configure the attributes of a PSTN user.
2. Run the **display mgpstnuser attribute** command to check whether the attributes of the PSTN user are the same as the planned data.

----End

Example

Assume that the phone numbers of 32 PSTN users are 83110000-83110031, **terminalid** are 0-31 (the TID template with which the PSTN users on the MG interface are bound is not a layering template and **terminalid** needs to be allocated manually), and the default values are used for other attributes. To add the PSTN users in slot 0/3 on MG interface 0 in batches, do as follows:

```
huawei(config)#board confirm 0/3
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
83110000
huawei(config-esl-user)#display mgpstnuser 0 0 32
  ------------------------------------------------------------------------
  F  /S /P    MGID     TelNo            Priority PotsLineType TerminalID
  ------------------------------------------------------------------------
  0  /3 /0    0        83110000         Cat3     DEL          A0
  0  /3 /1    0        83110001         Cat3     DEL          A1
  ......
  0  /3 /30   0        83110030         Cat3     DEL          A30
```

```
0  /3 /31   0        83110031         Cat3     DEL          A31
------------------------------------------------------------------------
```

7.1.2.2 (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 7-6 lists the system parameters supported by the MA5616.

Table 7-6 System parameters supported by the MA5616

Parameter	Description	Default Setting
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 on the same device.	0: Indicates that the media stream is forwarded within the device.
6	Indicates whether to send power deny flag when softswitch indicates block.	1: Not send

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 the planned data.

----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,
14:Turkey,
20:Germany
  ------------------------------------------------------------------------------
```

7.1.2.3 (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 7-7 lists the overseas parameters supported by the MA5616.

Table 7-7 Overseas parameters supported by the MA5616

Parameter	Description	Default Setting
0	Indicates the upper threshold of the flash-hooking duration.	350 ms (in compliance with the Chinese mainland standards)
1	Indicates the lower threshold of the flash-hooking duration.	100 ms (in compliance with the Chinese mainland 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 type of ring DC offset.	Line B offset

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 the planned data.

----End

Example

To set the upper flash-hooking threshold (overseas parameter 0) to 800 ms (in compliance with the Hong Kong standards) and the lower flash-hooking threshold (overseas parameter 1) to 100 ms (in compliance with the Hong Kong standards), do as follows:

```
huawei(config)#oversea parameters 0 800
huawei(config)#oversea parameters 1 100
huawei(config)#display oversea parameters
{ <cr>|name<U><0,3> }:
  Command:
```

```
        display oversea parameters
 ------------------------------------------------------------------------------
 Parameter name index: 0     Parameter value: 800
 Mean: Hooking upper threshold(ms), reference: China:350, HongKong:800
 ------------------------------------------------------------------------------
 Parameter name index: 1     Parameter value: 100
 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: 1
 Mean: Type of ring DC offset, 0:Line A offset, 1:Line B offset
 ------------------------------------------------------------------------------
```

7.1.2.4 (Optional) Configuring the Local Digitmap

Local digitmap is also called local preconfigured digitmap. When the H.248 protocol is used, the MA5616 prefers to use the digitmap sent by the MGC to match the phone number. If the MGC does not send the detailed digitmap, the MA5616 uses the local digitmap to match the phone number. When the SIP protocol is used, the MA5616 has to use the local digitmap to match the phone number because the IMS network does not send the digitmap. When configuring services on the MA5616, configure a proper local digitmap according to the local standards.

Context

CAUTION

When the H.248 protocol is used, the local digitmap need not be configured by default. You can configure the local digitmap according to the requirements.

- When the H.248 protocol is used, the MA5616 is not configured with a default local digitmap. You can configure a local digitmap if required.
- When the SIP protocol is used, the MA5616 is configured with three default local digitmaps, namely, normal digitmap, emergency digitmap, and SCC digitmap. You can change the name and type of the default local digitmaps, and add or change the digitmap body in the default local digitmaps. In addition, you can add a local digitmap according to the requirements. **Table 7-8** lists the information about the default local digitmap.

Table 7-8 Information about the default local digitmap when the SIP protocol is used

Digitmap Name	Digitmap Type	Digitmap Body
DefaultNormalDmm	normal	x.S
DefaultSccDmm	scc	([EF]X[0-9E].F|[EF]X [0-9E].S|[EF][EF]X [0-9E].F|[EF][EF]X [0-9E].S)
DefaultEmergencyDmm	emergency	(11X|91X)

- The MA5616 supports a maximum of eight local digitmaps.
- For the meaning of each character in the digitmap body, see the Context in **7.1.1.4 (Optional) Configuring the Digitmap of an MG Interface**.

Precaution

- When the H.248 protocol is used, the type of the local digitmap can only be normal.
- When the SIP protocol is used, the type of the local digitmap can be normal, emergency, scc, direct-centrex, or second-centrex. For the meaning of the digitmap type, see the Parameter Description in the **local-digitmap add** command.

Procedure

Step 1 In privilege mode, run the **display protocol support** command to query the current protocol type used on the MA5616.

- When the H.248 protocol is used, go to **Step 5**.
- When the SIP protocol is used, go to **Step 2**.

Step 2 In privilege mode, run the **display local-digitmap** command to query the default local digitmap.

- If the default local digitmap can meet the requirements, the configuration is complete.
- If the default local digitmap cannot meet the requirements, perform one or more operations in **Step 3**, **Step 4**, and **Step 5** to configure a proper local digitmap.

Step 3 Run the **local-digitmap modify** command to change the name, type, or body of the local digitmap.

Step 4 Run the **local-digitmap append** command to add a digitmap body in the local digitmap.

Step 5 According to the data plan, run the **local-digitmap add** command to add a local digitmap.

Step 6 Run the **display local-digitmap** command to check whether the local digitmap is the same as the planned local digitmap.

----End

Example

Assume that the H.248 protocol is used on the MA5616. To add a local digitmap with the data listed in **Table 7-9**, do as follows:

Table 7-9 Local digitmap existing in the system

Digitmap Name	Digitmap Type	Digitmap Body
huawei	normal	([2-8]xxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)

```
huawei(config)#local-digitmap add huawei normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13
xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)
huawei(config)#display local-digitmap all
  ----------------------------------------
```

```
  Name: huawei
  Body: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|
x.F|[0-9].S)
  ----------------------------------------
```

Assume that the SIP protocol is used on the MA5616. The local digitmap exists in the system. **Table 7-10** lists the data of the local digitmap.

Table 7-10 Local digitmap existing in the system

Digitmap Name	Digitmap Type	Digitmap Body
huawei	normal	([2-8]xxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)

To change the existing local digitmap so that the name of the local digitmap is **huawei0**, add digitmap body 15xxxxxxxx, and add a local digitmap according to data plan listed in **Table 7-11**, do as follows:

Table 7-11 Local digitmap to be added

Digitmap Name	Digitmap Type	Digitmap Body
huawei1	emergency	(0E)

```
huawei(config)#display local-digitmap all
  ----------------------------------------
  Name: DefaultNormalDmm
  Type: normal
  Body: x.S
  ----------------------------------------
  Name: DefaultSccDmm
  Type: scc
  Body: (ExxFx.E|ExxFx.L|ExFx.E|ExFx.L|Exx.F|EFxx.F|Fxx.F|Ex.Ex.F)
  ----------------------------------------
  Name: DefaultEmergencyDmm
  Type: emergency
  Body: (11X|91X)
  ----------------------------------------
  Name: huawei
  Type: normal
  Body: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|
x.F|[0-9].S)
  ----------------------------------------
huawei(config)#local-digitmap modify huawei name huawei0
huawei(config)#local-digitmap append huawei0 15xxxxxxxxx
huawei(config)#local-digitmap add huawei1 emergency (11X|91X|0E)
huawei(config)#display local-digitmap all
  ----------------------------------------
  Name: DefaultNormalDmm
  Type: normal
  Body: x.S
  ----------------------------------------
  Name: DefaultSccDmm
  Type: scc
  Body: (ExxFx.E|ExxFx.L|ExFx.E|ExFx.L|Exx.F|EFxx.F|Fxx.F|Ex.Ex.F)
  ----------------------------------------
```

```
  Name: DefaultEmergencyDmm
  Type: emergency
  Body: (11X|91X)
  ----------------------------------------
  Name: huawei0
  Type: normal
  Body: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|
x.F|[0-9].S|15xxxxxxxxx)
  ----------------------------------------
  Name: huawei1
  Type: emergency
  Body: (11X|91X|0E)
  ----------------------------------------
```

7.1.2.5 (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 MA5616 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 charging 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 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 a PSTN port.

Step 3 Run the **pstnport electric batset** or **pstnport electric set** command to configure the electrical attributes of a PSTN port.

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 the planned data.

- 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 PSTN ports on the board in slot 0/3 to support the polarity reversal charging, do as follows:

NOTE

When a call starts 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 charging function, such as a charging phone set, implements the polarity reversal charging function based on the start time and the end time of a call.

7.1.2.6 (Optional) Configuring the Attributes of the Ringing Current

You can adjust the ringing tone volume by modifying the attributes of the ringing current. Generally, the attributes of the ringing current need not 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: The higher the frequency is, the sharper the ringing tones are.
- AC voltage amplitude: The greater the amplitude is, the louder the ringing tones are.

The default settings of the attributes of the ringing current are as follows:

- Ringing current frequency: 25 Hz
- AC voltage amplitude: 65 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 the planned data.

----End

Example

To set the ringing current frequency to 16 Hz (parameter value 0) and AC amplitude to 65 Vrms (parameter value 1), do as follows:

```
huawei(config)#voip
huawei(config-voip)#ring attribute set frequency 0 acamplitude 1
huawei(config-voip)#display ring attribute
  ringing current frequency  : 16Hz
  ringing current acamplitute: 65Vrms
```

7.2 Configuring the VoIP PSTN Service (Based on the SIP Protocol)

This topic describes how to configure the VoIP PSTN service on the MA5616 through the Session Initiation Protocol (SIP).

Context

The voice over IP (VoIP) service uses the IP packet switching network for transmission after the traditional analog voice signals are compressed and packetized, to reduce the cost of the voice service.

For details about the VoIP service, see Voice in the *Feature Description*.

The function and application of the SIP interface are similar to the function and application of the MG interface. The MA5616 can also function as a voice over IP gateway (VGW) component in the IMS architecture. In the downstream direction, it provides the access to PSTN users; in the upstream direction, it is connected to the IMS system through the SIP interface, providing the VoIP service by working with the IMS core.

Prerequisite

According to the actual network, a route from the MA5616 to the IMS core network device must be configured to ensure that the MA5616 and the IMS core network device are reachable to each other.

Data preparation

Table 7-12 provides the data plan for configuring the VoIP service.

Table 7-12 Data plan for configuring the VoIP service based on the SIP protocol

Item			Remarks
SIP interface data	Parameters of the media stream and signaling stream	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	It is used as the 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 consist of all the IP addresses of the L3 interface of the media and signaling upstream VLAN.

Item			Remarks
		Default IP address of the MG	It is the IP address of the next hop from the MA5616 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 fail.
	Attribute parameters of the SIP interface **NOTE** Parameters listed here are mandatory, which means that the SIP interface fails to be started if these parameters are not configured.	SIP interface ID	It is the SIP interface ID used for the VoIP service to be configured. The MA5616 supports only one virtual access gateway (VAG).
		Signaling port ID of the SIP interface	The value range is 5000-5999. The protocol specifies the port ID to be 5060.
		IP address of the primary IMS core network device to which the SIP interface belongs	When dual homing is not configured, parameters of only the primary IMS core network device are required. If dual homing is configured, the IP address and the port ID of the secondary IMS core network device must be configured.
		Port ID of the primary 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 IP mode, the IP address and the port ID of the primary proxy server must be configured. ● In DNS-A or DNS-SRV mode, the domain of the primary proxy server must be configured.
	Ringing Mode of the SIP Interface		The ringing mode of the SIP interface is determined by service requirements.

Item			Remarks
Voice service data (The data configuration must be consistent with the data configuration on the MGC.)	Slot that houses the voice service board		-
	User Data	Phone number	The phone number that the IMS core network device allocates to the user must be configured.
		User priority	According to the service requirements, the user priority needs to be specified. The user priorities are as follows: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: normal (common users, default priority in the system)
		User type	According to the service requirements, the user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default type in the system) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
	Centrex		According to the local standards, the out-centrex prefix and out-centrex attributes need to be configured.
	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.

Item		Remarks
	Local Digitmap	Configure a proper local digitmap according to the local standards. After the configuration, the local digitmap can be directly used to match the phone number after the user picks the phone off the hook.
	Attributes of a PSTN Port	If the PSTN port needs to support the polarity reversal charging, the PSTN port needs to be configured to support the polarity reversal pulse. Other attributes need not be modified if there is no special requirement.
	Attributes of the Ringing Current	You can adjust the ringing tone volume by modifying the attributes of the ringing current. Generally, the parameters of the ringing current attributes need not 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

7.2.1 Configuring the SIP Interface

This topic describes how to configure the SIP interface to implement the communication between the MA5616 (SIP AG) and the IMS core network device.

Context

- The MA5616 can communicate with the IMS core network device through the SIP protocol.
- One MA5616 supports only one SIP interface.

Procedure

7.2.1.1 Configuring the Upstream VLAN Interface

This topic describes how to specify the upstream VLAN interface for the media stream and signaling stream, and how to configure the IP addresses of the L3 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 L3 interface. Only one IP address functions as the primary address, and other IP addresses function as the secondary addresses.

Procedure

Step 1 Add an upstream VLAN.

Run the **vlan** command to add an upstream VLAN for the media stream and signaling stream.

Step 2 Add an upstream port to the VLAN.

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

Step 3 Configure the IP addresses of the VLAN L3 interface.

1. Run the **interface vlanif** command to enter the L3 interface of the upstream VLAN for the media stream and signaling stream.
2. Run the **ip address** command to configure the IP addresses of the L3 interface.

Step 4 Check whether the IP addresses of the L3 interface are the same as those in the data plan.

Run the **display interface vlanif** command to check whether the IP addresses of the L3 interface are the same as those in the data plan.

----End

Example

Assume that the media stream and signaling stream are transmitted upstream through upstream port 0/0/1. 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 L3 interfaces for the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/0 1
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
```

7.2.1.2 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 L3 interface of the media and signaling upstream VLAN must be configured. For details about how to configure the IP address, see **7.1.1.1 Configuring the Upstream VLAN Interface**.

Context

- The media IP address and the signaling IP address for the MG or SIP 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 or SIP 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.

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 L3 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 L3 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

Assume that the IP address of the gateway is 10.13.1.1. To add IP addresses 10.13.4.116 and 10.13.4.117 of L3 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 10.13.1.1
huawei(config-voip)#ip address media 10.13.4.117 10.13.1.1
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..............: 10.13.1.1
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.1.1
  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
```

7.2.1.3 Adding an SIP Interface

This topic describes how to add an SIP interface so that the MA5616 can communicate with the IMS through the SIP interface.

Prerequisites

The to-be-configured media and signaling IP addresses of the SIP interface must be added to the media and signaling IP address pools successfully.

Context

One MA5616 supports only one SIP interface.

Procedure

Step 1 Run the **display protocol support** command to query the current system protocol.

- If the system protocol is SIP, go to **Step 8**.
- If the system protocol is not SIP, go to **Step 2**.

Step 2 Run the **display if-h248 all** command to query whether an MG interface that supports the current protocol exists in the system.

Step 3 Run the **display mgpstnuser** command to check the user data, run the **esl user** command to enter ESL user mode, and then run the **mgpstnuser batdel** command to delete the voice service user.

Step 4 Run the **shutdown(h248)** command to shut down the MG interface.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation. Before performing this operation, be sure to check whether the operation is allowed.

Step 5 Run the **undo interface h248** command to delete the MG interface.

Step 6 Run the **protocol support sip** command to change the system protocol to SIP.

CAUTION

You must delete the default and user-defined local digitmaps before switching the protocol.

Step 7 After saving the configuration data by running the **save** command, run the **reboot system** command to reboot the system to make the new configuration take effect.

Step 8 Run the **interface sip** command to add an SIP interface.

Step 9 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 10 Run the **if-sip attribute optional** command to configure the optional attributes of the SIP interface.

Step 11 Run the **display if-sip attribute** command to query the SIP interface attributes.

Step 12 After the configuration, you need to run the **reset** command to reset the SIP interface to make the configuration take effect. Otherwise, the configuration is stored only in the database.

Step 13 After the configuration, run the **display if-sip attribute running** command to query the status of the SIP interface.

----End

Example

Assume that the media IP address is 10.13.4.116, signaling IP address is 10.13.4.117, transmission protocol is UDP, port ID is 5000, IP address 1 of the primary proxy server is 10.13.4.118, port ID of the primary proxy server is 5060, domain name of the primary proxy server is proxy.domain, IP address 1 of the secondary proxy server is 10.13.4.119, port ID of the secondary proxy server is 5060, home domain name is sip.huawei.com, and profile index is 1. To configure such attributes of SIP interface 0, do as follows:

```
huawei(config)#interface sip 0
huawei(config)#if-sip attribute basic media-ip 10.13.4.116 signal-ip
10.13.4.117 signal-port 5000 transfer udp primary-proxy-ip1 10.13.4.118
primary-proxy-port 5060 primary-proxy-domain proxy.domain
{ <cr>|home-domain<K>|primary-proxy-ip2<K>|proxy-addr-mode<K>|secondary-proxy-do
main<K>|secondary-proxy-ip1<K>|secondary-proxy-ip2<K>|secondary-proxy-port<K>|se
rver-dhcp-option<K>|sipprofile-index<K>|srvlogic-index<K> }:secondary-proxy-ip1
{ secondary-proxy-ip1-value<I><X.X.X.X> }:10.13.4.119
{ <cr>|home-domain<K>|primary-proxy-ip2<K>|proxy-addr-mode<K>|secondary-proxy-do
main<K>|secondary-proxy-ip2<K>|secondary-proxy-port<K>|server-dhcp-option<K>|sip
profile-index<K>|srvlogic-index<K> }:secondary-proxy-port 5060
{ <cr>|home-domain<K>|primary-proxy-ip2<K>|proxy-addr-mode<K>|secondary-proxy-do
main<K>|secondary-proxy-ip2<K>|server-dhcp-option<K>|sipprofile-index<K>|srvlogi
c-index<K> }:

  Command:
          if-sip attribute basic media-ip 10.13.4.116 signal-ip 10.13.4.117
signal-port 5000 transfer udp primary-proxy-ip1 10.13.4.118 primary-proxy-port
5060 primary-proxy-domain proxy.domain secondary-proxy-ip1 10.13.4.119
secondary-proxy-port 5060
huawei(config-if-sip-0)#if-sip attribute basic 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
  ------------------------------------------------------------
```

```
  MGID
0
  Signalling IP
10.13.4.117
  Signalling Port
5000
  Media IP
10.13.4.116
  Transfer Mode
UDP
  Primary Proxy IP 1
10.13.4.118
  Primary Proxy IP 2
-
  Primary Proxy Port
5060
  Secondary Proxy IP 1
10.13.4.119
  Secondary Proxy IP 2
-
  Secondary Proxy Port
5060
  Proxy Address Mode
IP
  SIPProfile Index
1:Default
  Service logic Index
0:Default
  Server Address DHCP Option
0:None
  Primary Proxy Domain Name
-
  Secondary Proxy Domain Name
-
  Home Domain Name
sip.huawei.com
  Description
-
  MG Domain Name
-
  Phone Context
-
  Register URI
-
  Conference Factory URI
-
  Primary Proxy State
up
  Secondary Proxy State
up
  Subscribe to UA-Profile              enable
  Subscribe to REG-STATE               disable
  Subscribe to MWI                     disable
  SDP negotiation mode                 remote
  Mode of supporting proxy dual-homing dualhome
  Proxy detection mode                 probe
  ------------------------------------------------------------
```

7.2.1.4 (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 preset ringing modes cannot meet the user requirements, you can use the user-defined ringing mode and configure the corresponding ringing mapping.
- You 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 a maximum of 16 records of the ringing mode mapping.

Precaution

- 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, go 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 0-15 ringing types.
- After configuring the user-defined ringing mode, you need to reset the corresponding service board to make the configuration take effect, so that the user of the service board can use the new 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 the ringing mapping.

Run this command to configure the ringing mode for the users on 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 ringmode** command to query ringing mapping records.

----End

Example

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

To add such a ringing mode mapping record on SIP interface 0, 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: 1: Special Ring 1:2
  InitialRing: 4: Normal Ring (FSK) 1:4
  ---------------------------------------------------------------
```

7.2.2 Configuring the VoIP PSTN User

After an SIP interface is configured, you can add public switched telephone network (PSTN) users on the SIP interface to implement the VoIP service.

7.2.2.1 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 so that the POTS terminal can access the network to implement the VoIP service.

Prerequisites

The POTS service board must be inserted into the planned slot.

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 7-13 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 7-13 Default settings of the attributes of the PSTN user

Parameter	Default Setting
Priority	cat3
PotsLineType	DEL
Sequence of sending the phone number of the calling party	Ringing and then sending the phone number

Parameter	Default Setting
Format of the phone number of the calling party	SDMF(FSK)
Power-off interval	100ms
FSK delay interval	800ms
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.)
Whether to support the detection of the ANSbar signal through monophony	Not support
Whether to support the bell ANS signal	Not support
Display mode of the FSK phone number of the calling party	BELL_202
TAS CID mode	NO-TAS

Procedure

Step 1 In global config mode, run the **board confirm** command to confirm the service board.

NOTE

You need not run this command if the board is integrated in the mother board.

Step 2 Add a PSTN user.

1. In 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 a PSTN user or add PSTN users in batches.

CAUTION

When adding a user, you can configure the phone number (parameter **telno**). When the public ID is generated by phone number, you must enter the phone number. It is recommended that you configure this phone number to be the same as the phone number configured on the IMS. In addition, ensure that the phone number is unique on the AG.

3. Run the **display sippstnuser** command to check whether the PSTN user data is the same as the planned data.

Step 3 (Optional) Configure the attributes of a PSTN user.

The attributes of a PSTN user need to be configured when the default settings are inconsistent with the actual application.

1. Run the **sippstnuser attribute set** or **sippstnuser attribute batset** command to configure the attributes of a PSTN user.
2. Run the **display sippstnuser attribute** command to check whether the attributes of the PSTN user are the same as the planned data.

----End

Example

Assume that the phone numbers of 32 PSTN users are 83120000-83120031 and the default values are used for other attributes. To add the PSTN users in slot 0/3 on SIP interface 0 in batches, do as follows:

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/3/0  0/3/31 0 telno 83120000 step 1
huawei(config-esl-user)#display sippstnuser 0/3
  ---------------------------------------
  F  /S /P    MGID     TelNo
  ---------------------------------------
  0  /3 /0    0        83120000
  ......
  0  /3 /30   0        83120030
  0  /3 /31   0        83120031
  ---------------------------------------
```

7.2.2.2 Configuring the Centrex

Centrex refers to a virtual user group. The MA5616 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.

Context

- The function that the members in a centrex can call each other by dialing short numbers need not be configured on the MA5616 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.
- In the actual configuration, configure whether the phone number reported by the MA5616 contains the centrex prefix according to the local standards. This function is controlled by the one hundred and fourty-eighth control point of the Sipprofile. The options of the parameter are 0 and 1, where 0 indicates that the phone number does not contain the centrex prefix and 1 indicates that the phone number contains the centrex prefix. By default, this parameter is configured to 1.

Precaution

The MA5616 supports the configuration of the centrex prefix through one of the following two methods:

- Method 1: Run the **sippstnuser servicedata parameters set** command to configure the centrex prefix and centrex attributes of a centrex.
- Method 2: Run the **local-digitmap add** command to add a direct centrex digitmap or a two-stage centrex digitmap.

CAUTION

The system does not support the adding of a direct centrex digitmap and a two-stage centrex digitmap at the same time. Add the corresponding digitmap according to the requirements.

When you add a direct centrex digitmap, the centrex attribute of the system is direct centrex. When you add a two-stage centrex digitmap, the centrex attribute of the system is two-stage centrex.

- If both the operations are carried out successfully through the preceding methods, the system adopts the configuration obtained through the **sippstnuser servicedata parameters set** command.
- If method 2 is adopted, the MA5616 uses the centrex digitmap to match the centrex prefix, and then uses the call digitmap, namely, the normal digitmap, to match the phone number dialed by the user.

Procedure

Step 1 Check whether the value of the control point of the Sipprofile needs to be changed. If the value needs to be changed, run the **interface sip** command to enter the SIP interface mode, and then run the **sipprofile modify** command to change the value to the required one.

Step 2 Configure the centrex call function of a centrex.

- Configure the centrex call function by using method 1 in Precaution:

1. In ESL user mode, run the **sippstnuser servicedata parameters set** command to configure the centrex prefix and centrex attributes of a centrex.
2. Run the **display sippstnuser servicedata** command to check whether the configuration of the centrex parameters of a centrex is the same the planned configuration.

- Configure the centrex call function by using method 2 in Precaution:

1. In global config mode, run the **local-digitmap add** command to configure a direct centrex digitmap or a two-stage centrex digitmap.
2. Run the **display local-digitmap** command to check whether the local digitmap is the same as the planned local digitmap.

----End

Example

Assume that the centrex prefix of the 0/3/ 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 0/3/0 telno
83120001
centrexprefix 8100 centrexflag dialsecondary
huawei(config-esl-user)#display sippstnuser servicedata 0/3/0 telno 83120001
  ----------------------------------------
  F /S /P           : 0  /3 /0
  telno             : 83120001
  centrexno         : -
  centrexprefix     : 8100
  centrexflag       : dialsecondary
  mwimode           : deferred
  hottime(s)        : 100
  hotlinenum        : -
  dialtone          : normal
  cfbnum            : -
  cfnrnum           : -
  cfunum            : -
  cfnrtime(s)       : 100
  ----------------------------------------
```

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: DefaultNormalDmm
  Type: normal
  Body: x.S
  ----------------------------------------
  Name: DefaultSccDmm
  Type: scc
  Body: (ExxFx.E|ExxFx.L|ExFx.E|ExFx.L|Exx.F|EFxx.F|Fxx.F|Ex.Ex.F)
  ----------------------------------------
  Name: DefaultEmergencyDmm
  Type: emergency
  Body: (11X|91X)
  ----------------------------------------
  Name: huawei1
  Type: second-centrex
  Body: (8100)
  ----------------------------------------
```

7.2.2.3 (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 7-14 lists the system parameters supported by the MA5616.

Table 7-14 System parameters supported by the MA5616

Parameter	Description	Default Setting
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 on the same device.	0: Indicates that the media stream is forwarded within the device.
6	Indicates whether to send power deny flag when softswitch indicates block.	1: Not send

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 the planned data.

----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,
14:Turkey,
20:Germany
  ---------------------------------------------------------------------------
```

7.2.2.4 (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 7-15 lists the overseas parameters supported by the MA5616.

Table 7-15 Overseas parameters supported by the MA5616

Parameter	Description	Default Setting
0	Indicates the upper threshold of the flash-hooking duration.	350 ms (in compliance with the Chinese mainland standards)
1	Indicates the lower threshold of the flash-hooking duration.	100 ms (in compliance with the Chinese mainland 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 type of ring DC offset.	Line B offset

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 the planned data.

----End

Example

To set the upper flash-hooking threshold (overseas parameter 0) to 800 ms (in compliance with the Hong Kong standards) and the lower flash-hooking threshold (overseas parameter 1) to 100 ms (in compliance with the Hong Kong standards), do as follows:

```
huawei(config)#oversea parameters 0 800
huawei(config)#oversea parameters 1 100
huawei(config)#display oversea parameters
{ <cr>|name<U><0,3> }:
  Command:
          display oversea parameters
  ---------------------------------------------------------------------------
  Parameter name index: 0     Parameter value: 800
```

```
 Mean: Hooking upper threshold(ms), reference: China:350, HongKong:800
 ----------------------------------------------------------------------------
 Parameter name index: 1     Parameter value: 100
 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: 1
 Mean: Type of ring DC offset, 0:Line A offset, 1:Line B offset
 ----------------------------------------------------------------------------
```

7.2.2.5 (Optional) Configuring the Local Digitmap

Local digitmap is also called local preconfigured digitmap. When the H.248 protocol is used, the MA5616 prefers to use the digitmap sent by the MGC to match the phone number. If the MGC does not send the detailed digitmap, the MA5616 uses the local digitmap to match the phone number. When the SIP protocol is used, the MA5616 has to use the local digitmap to match the phone number because the IMS network does not send the digitmap. When configuring services on the MA5616, configure a proper local digitmap according to the local standards.

Context

CAUTION

When the H.248 protocol is used, the local digitmap need not be configured by default. You can configure the local digitmap according to the requirements.

- When the H.248 protocol is used, the MA5616 is not configured with a default local digitmap. You can configure a local digitmap if required.
- When the SIP protocol is used, the MA5616 is configured with three default local digitmaps, namely, normal digitmap, emergency digitmap, and SCC digitmap. You can change the name and type of the default local digitmaps, and add or change the digitmap body in the default local digitmaps. In addition, you can add a local digitmap according to the requirements. **Table 7-16** lists the information about the default local digitmap.

Table 7-16 Information about the default local digitmap when the SIP protocol is used

Digitmap Name	Digitmap Type	Digitmap Body
DefaultNormalDmm	normal	x.S
DefaultSccDmm	scc	([EF]X[0-9E].F|[EF]X [0-9E].S|[EF][EF]X [0-9E].F|[EF][EF]X [0-9E].S)
DefaultEmergencyDmm	emergency	(11X|91X)

- The MA5616 supports a maximum of eight local digitmaps.

- For the meaning of each character in the digitmap body, see the Context in **7.1.1.4 (Optional) Configuring the Digitmap of an MG Interface**.

Precaution

- When the H.248 protocol is used, the type of the local digitmap can only be normal.
- When the SIP protocol is used, the type of the local digitmap can be normal, emergency, scc, direct-centrex, or second-centrex. For the meaning of the digitmap type, see the Parameter Description in the **local-digitmap add** command.

Procedure

Step 1 In privilege mode, run the **display protocol support** command to query the current protocol type used on the MA5616.

- When the H.248 protocol is used, go to **Step 5**.
- When the SIP protocol is used, go to **Step 2**.

Step 2 In privilege mode, run the **display local-digitmap** command to query the default local digitmap.

- If the default local digitmap can meet the requirements, the configuration is complete.
- If the default local digitmap cannot meet the requirements, perform one or more operations in **Step 3**, **Step 4**, and **Step 5** to configure a proper local digitmap.

Step 3 Run the **local-digitmap modify** command to change the name, type, or body of the local digitmap.

Step 4 Run the **local-digitmap append** command to add a digitmap body in the local digitmap.

Step 5 According to the data plan, run the **local-digitmap add** command to add a local digitmap.

Step 6 Run the **display local-digitmap** command to check whether the local digitmap is the same as the planned local digitmap.

----End

Example

Assume that the H.248 protocol is used on the MA5616. To add a local digitmap with the data listed in **Table 7-17**, do as follows:

Table 7-17 Local digitmap existing in the system

Digitmap Name	Digitmap Type	Digitmap Body
huawei	normal	([2-8]xxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)

```
huawei(config)#local-digitmap add huawei normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13
xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)
huawei(config)#display local-digitmap all
  ----------------------------------------
  Name: huawei
```

```
  Body: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|
x.F|[0-9].S)
  ------------------------------------------
```

Assume that the SIP protocol is used on the MA5616. The local digitmap exists in the system. Table 7-18 lists the data of the local digitmap.

Table 7-18 Local digitmap existing in the system

Digitmap Name	Digitmap Type	Digitmap Body
huawei	normal	([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)

To change the existing local digitmap so that the name of the local digitmap is **huawei0**, add digitmap body 15xxxxxxxxx, and add a local digitmap according to data plan listed in Table 7-19, do as follows:

Table 7-19 Local digitmap to be added

Digitmap Name	Digitmap Type	Digitmap Body
huawei1	emergency	(0E)

```
huawei(config)#display local-digitmap all
  ------------------------------------------
  Name: DefaultNormalDmm
  Type: normal
  Body: x.S
  ------------------------------------------
  Name: DefaultSccDmm
  Type: scc
  Body: (ExxFx.E|ExxFx.L|ExFx.E|ExFx.L|Exx.F|EFxx.F|Fxx.F|Ex.Ex.F)
  ------------------------------------------
  Name: DefaultEmergencyDmm
  Type: emergency
  Body: (11X|91X)
  ------------------------------------------
  Name: huawei
  Type: normal
  Body: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|
x.F|[0-9].S)
  ------------------------------------------
huawei(config)#local-digitmap modify huawei name huawei0
huawei(config)#local-digitmap append huawei0 15xxxxxxxxx
huawei(config)#local-digitmap add huawei1 emergency (11X|91X|0E)
huawei(config)#display local-digitmap all
  ------------------------------------------
  Name: DefaultNormalDmm
  Type: normal
  Body: x.S
  ------------------------------------------
  Name: DefaultSccDmm
  Type: scc
  Body: (ExxFx.E|ExxFx.L|ExFx.E|ExFx.L|Exx.F|EFxx.F|Fxx.F|Ex.Ex.F)
  ------------------------------------------
  Name: DefaultEmergencyDmm
```

```
  Type: emergency
  Body: (11X|91X)
  ----------------------------------------
  Name: huawei0
  Type: normal
  Body: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|
x.F|[0-9].S|15xxxxxxxxx)
  ----------------------------------------
  Name: huawei1
  Type: emergency
  Body: (11X|91X|0E)
  ----------------------------------------
```

7.2.2.6 (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 MA5616 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 charging 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 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 a PSTN port.

Step 3 Run the **pstnport electric batset** or **pstnport electric set** command to configure the electrical attributes of a PSTN port.

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 the planned data.

- 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 PSTN ports on the board in slot 0/3 to support the polarity reversal charging, do as follows:

NOTE

When a call starts 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 charging function, such as a charging phone set, implements the polarity reversal charging function based on the start time and the end time of a call.

7.2.2.7 (Optional) Configuring the Attributes of the Ringing Current

You can adjust the ringing tone volume by modifying the attributes of the ringing current. Generally, the attributes of the ringing current need not 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: The higher the frequency is, the sharper the ringing tones are.
- AC voltage amplitude: The greater the amplitude is, the louder the ringing tones are.

The default settings of the attributes of the ringing current are as follows:

- Ringing current frequency: 25 Hz
- AC voltage amplitude: 65 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 the planned data.

----End

Example

To set the ringing current frequency to 16 Hz (parameter value 0) and AC amplitude to 65 Vrms (parameter value 1), do as follows:

```
huawei(config)#voip
huawei(config-voip)#ring attribute set frequency 0 acamplitude 1
huawei(config-voip)#display ring attribute
  ringing current frequency  : 16Hz
  ringing current acamplitute: 65Vrms
```

7.3 Configuring the VoIP ISDN BRA Service

This topic describes how to configure the VoIP ISDN BRA service on an IP network. When the MA5616 uses the H.248 protocol, the device supports the access of the ISDN BRA user. ISDN technology provides end-to-end (E2E) digital connection and supports multiple types of voice and non-voice telecom services.

Prerequisites

According to the actual network, a route from the MA5616 to the MGC must be configured to ensure that the MA5616 communicates with the MGC normally.

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. This service lowers the cost of the voice service. For the detailed description of the VoIP service, see Voice Feature in the *Feature Description*.
- Defined by the International Telegraph and Telephone Consultative Committee (CCITT), the ISDN is a communication network evolved from the Integrated Digital Network (IDN). The ISDN service provides the E2E digital connection and supports multiple types of voice and non-voice telecom services. On the ISDN network, users can access the network through the following two interfaces: (The ISDN technology provides two types of user-network interfaces based on the user-network interface reference model.)
  - ISDN basic rate interface (BRI), which supports a rate of 144 kbit/s and provides two B channels (for carrying services) and one D channel (for transmitting call control signaling and maintenance and management signaling). The rate of B channels is 64 kbit/s and the rate of D channel is 16 kbit/s. The service carried on the ISDN BRI is the ISDN basic rate access (BRA) service.
  - ISDN primary rate interface (PRI), which supports a rate of 2.048 Mbit/s and provides 30 B channels and one D channel. The rates of the B channel and D channel are both 64 kbit/s. The service carried on the ISDN PRI is the ISDN primary rate access (PRA) service.
- The MA5616 supports only the VoIP ISDN BRA service.
- The MA5616 provides the ISDN BRA service through the DSL port on the DSLD board. For detailed description of the DSLD board, see DSLD - Eight-Channel ISDN Service Board in the *Hardware Description*.

Precaution

The media gateway control protocol (MGCP) is a master/slave protocol. under which the MGC controls the AG to implement call connection and disconnection. The data on the AG for the interconnection with the MGC, such as the attributes of the MG interface and the attributes of the VoIP user, must be the same as the corresponding data on the MGC. Therefore, before configuring the VoIP service, you must contact MGC engineers to check and ensure that the interconnection data plan for the AG is consistent with the corresponding plan for the MGC.

Data preparation

Table 7-20 provides the data plan for configuring the H.248-based VoIP ISDN BRA service.

Table 7-20 Data plan for configuring the H.248-based VoIP ISDN BRA service

Item			Remarks
MG interface data (The data must be consistent with the data on the MGC.)	Parameters of the media stream and signaling stream	Upstream VLAN for media and signaling streams	It is used as the upstream VLAN of the VoIP service to be configured. Standard VLAN is recommended.
		Uplink port for media and signaling streams	It is used as the uplink port for the VoIP service to be configured.
		Media IP address and signaling IP address	These IP addresses must be contained in the media and signaling IP address pools. The media and signaling IP address pools consist of all the IP addresses of the L3 interface of the upstream VLAN for media and signaling streams.
		Default IP address of the MG	It is the next hop IP address from the MA5616 to the MGC.
	Attribute parameters of the MG interface **NOTE** There are many MG interface parameters. Only mandatory parameters are listed here. If the mandatory parameters are not configured, the MG interface cannot be started.	MG interface ID	It is the ID of the MG interface used by the VoIP service to be configured. The MA5616 supports only one VAG.
		Signaling port ID of the MG interface	It is the transport layer protocol port ID used for the signaling exchange between the MA5616 (AG) and the MGC. The default signaling port ID defined in H.248 is 2944 (text) and 2945 (binary).
		IP address of the primary MGC to which the MG interface belongs	When dual homing is not configured, you can configure the parameters of only the primary MGC. When dual homing is configured, you also need to configure the IP address and port ID of the secondary MGC.
		Port ID of the primary MGC to which the MG interface belongs	

Item			Remarks
		Coding mode of the MG interface	Currently, only the **text** mode is supported.
		Transmission mode of the MG interface	The transmission mode is selected according to the requirements of the MGC. Generally, UDP is used.
		Domain name of the MG interface	It corresponds to the **domainName** parameter of the MG interface. When the H.248 protocol is used, this parameter must be configured if the **MIDType** parameter of the H.248 message is configured to **domainName**. Otherwise, the MG interface cannot be started. In other situations, this parameter is optional.
		Device name of the MG interface	It is supported by only the H.248 protocol, and it corresponds to the **deviceName** parameter of the MG interface that uses the H.248 protocol. This parameter must be configured if the **MIDType** parameter of the H.248 message is configured to **domainName**. Otherwise, the MG interface cannot be started. In other situations, this parameter is optional.
	Digitmap of the MG interface		The digitmaps 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 need not be configured on the AG. If the services such as emergency calls and emergency standalone are not required, this parameter need not be configured.

Item			Remarks
	Software parameters of the MG interface		Whether the MG interface supports the functions such as dual homing and emergency standalone is determined by the service requirements.
	Ringing mode of the MG interface		Which ringing mode is used by the MG interface is determined by the service requirements.
	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.
IUA link	**IUA link set**		The IUA link can be configured only after the IUA link set is configured.
	IUA link **NOTE** The local port ID, local IP address, remote port ID, and remote IP address of different links must not be completely same; otherwise, the service cannot be configured.	IUA link ID	It indicates the link for transmitting the signaling.
		IUA link set ID	-
		Local port ID	To activate the link normally, it must be the same as the remote port ID configured on the MGC.
		Local IP address	It must be the same as the remote IP address of the link configured on the MGC. In addition, the local IP addresses of the links that are in the same link set must be the same. (The IP address must exist in the media IP address pool.)
		Remote port ID	To activate the link normally, it must be the same as the local port ID configured on the MGC.

Item			Remarks
		Remote IP address	It must be the same as the local IP address of the link configured on the MGC. The SCTP protocol supports the multi-homing function. That is, one link can be configured with the IP addresses of multiple MGCs as the remote IP addresses. When one MGC is faulty, the link can be switched to other MGCs automatically. This ensures that the service is not affected. The MA5616 supports the configuration of the active remote IP address and standby remote IP address.
ISDN BRA user data (The data must be consistent with the data on the MGC.)	Slot that houses the DSLD service board		1-4
	User data	Termination ID	If the TID format bound to the BRA user does not support terminal layering function, this parameter needs to be configured, and the configuration must be consistent with the configuration on the MGC.
		User priority	The user priority must be specified according to the service requirements. There are three categories of user priorities, which are as follows: ● cat1: government1 (category 1 government user) ● cat2: government2 (category 2 government user) ● cat3: normal (common user, default) The priorities of cat1, cat2, and cat3 are in descending order.
		Interface ID	It indicates the interface for the BRA user data to pass through the MG and MGC. The configuration of this parameter must be consistent with the corresponding configuration on the MGC.

Item		Remarks
	System parameters	The system parameters including the oversea 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.
	Attributes of an ISDN BRA Port	The attributes such as the working mode, remote power supply status, and auto-deactivation status of the port can be configured. Modify such attributes only if there is a special requirement.

7.3.1 Configuring an MG Interface

This topic describes how to configure an MG interface for implementing the communication between the MA5616 (AG) and the MGC.

Context

- The MA5616 communicates with the MGC through the MG control protocol, that is, the H.248 protocol.
- One MA5616 supports up to one MG interface. The MG interface can be configured with the attributes such as authentication and ringing mapping.

7.3.1.1 Configuring the Upstream VLAN Interface

This topic describes how to specify the upstream VLAN interface for the media stream and signaling stream, and how to configure the IP addresses of the L3 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 L3 interface. Only one IP address functions as the primary address, and other IP addresses function as the secondary addresses.

Procedure

Step 1 Add an upstream VLAN.

Run the **vlan** command to add an upstream VLAN for the media stream and signaling stream.

Step 2 Add an upstream port to the VLAN.

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

Step 3 Configure the IP addresses of the VLAN L3 interface.

1. Run the **interface vlanif** command to enter the L3 interface of the upstream VLAN for the media stream and signaling stream.
2. Run the **ip address** command to configure the IP addresses of the L3 interface.

Step 4 Check whether the IP addresses of the L3 interface are the same as those in the data plan.

Run the **display interface vlanif** command to check whether the IP addresses of the L3 interface are the same as those in the data plan.

----End

Example

Assume that the media stream and signaling stream are transmitted upstream through upstream port 0/0/1. 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 L3 interfaces for the media IP address pool and the signaling IP address pool respectively, do as follows:

```
huawei(config)#vlan 3 smart
huawei(config)#port vlan 3 0/0 1
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
```

7.3.1.2 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 L3 interface of the media and signaling upstream VLAN must be configured. For details about how to configure the IP address, see **7.1.1.1 Configuring the Upstream VLAN Interface**.

Context

- The media IP address and the signaling IP address for the MG or SIP 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 or SIP 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.

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 L3 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 L3 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

Assume that the IP address of the gateway is 10.13.1.1. To add IP addresses 10.13.4.116 and 10.13.4.117 of L3 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 10.13.1.1
huawei(config-voip)#ip address media 10.13.4.117 10.13.1.1
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..............: 10.13.1.1
  MAC Address..........: 00-E0-FC-AF-91-33

  IP Address...........: 10.13.4.117
  Subnet Mask..........: 255.255.0.0
  Gateway..............: 10.13.1.1
  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
```

7.3.1.3 Adding an MG Interface

This topic describes how to add an MG interface, through which the MA5616 can communicate with the MGC.

Context

One MA5616 supports up to one MG interface.

Procedure

Step 1 Add an MG interface.

Run the **interface h248** command to add an MG interface that supports H.248 protocol.

Step 2 Configure the attribute of the MG interface.

Run the **if-h248 attribute** command to configure the attribute of the MG interface according to the data plan.

An MG interface is reset successfully only when **mgip** (or **domainName** and **deviceName**), **mgport**, **primary-mgc-ip1** (or **mgc-domain-name1**), **primary-mgc-port**, **code**, **transfer**, and **mg-media-ip1** are configured successfully.

Table 7-21 lists the MG interface parameters you need to pay attention to when configuring the parameters for interconnection between the MG and the MGC.

Table 7-21 MG interface parameters

Parameter	Remarks
mgport	Indicates the transport layer protocol port ID used for the signaling exchange between the MA5616 (AG) and the MGC. The default signaling port ID defined in H.248 is 2944 (text) and 2945 (binary).
primary-mgc-ip1	When dual homing is not configured, you can configure the parameters of only one MGC. When dual homing is configured, you need to configure the IP address and port ID of the secondary MGC.
primary-mgc-port	
code	The coding modes of the MG interface and the MGC must be the same. Currently, only text coding mode is supported.

Parameter	Remarks
transfer	The transmission mode is selected according to the requirements of the MGC. Generally, UDP is used.
start-negotiate-version	If the MGC connecting to the MG is a Huawei device, the profile (parameter profile-index) does not need to be set; if the MGC connecting to the MG is a device of another vendor, the profile (parameter profile-index) must be set (the parameter value is prompted on the CLI). If the profile file in the system cannot meet requirements, contact Huawei for technical support.

Step 3 Check whether the attribute of the MG interface is the same as that in the data plan.

Run the **display if-h248 attribute** command to check whether the attribute of the MG interface is the same as that in the data plan.

----End

Example

Assume that the MG interface ID is 0, the H.248 protocol is used for interconnecting with the MGC, the signaling IP address is 10.13.4.116, the transport layer protocol port ID is 2944, IP address 1 of the primary MGC is 10.13.2.118, the transport layer protocol port ID of the primary MGC is 2944, media IP address 1 is 10.71.46.69, media IP address 2 is 10.13.4.117, the H.248 protocol version is started to be negotiated based on the profile, the transaction reliability is enabled. To add such an MG interface, do as follows:

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute  mgip 10.13.4.116 mgport 2944 code text
primary-mgc-ip1 10.13.2.118 primary-mgc-port 2944 mg-media-ip1 10.71.46.69
mg-media-ip2 10.13.4.117 start-negotiate-version 0 retrans enable
huawei(config-if-h248-0)#display if-h248 attribute
-------------------------------------------------
  MGID                                  0
  MG Description                        -
  MG DomainName                         -
  Protocol                              H248
  Start Negotiate Version               0
  Profile Negotiation Parameter         Disable
  Profile index                         1:NoProfile("")
  2833Encrypt                           -
  Codetype                              Text
  Transfer Mode                         -
  HeartBeatGenTimer(s)                  60
  HeartBeatRetransTimes                 3
  HeartBeatRetransTimer(s)              60
  MG signalling IP                      10.13.4.116
  MG signalling Port                    2944
  MG media IP1                          10.71.46.69
  MG media IP2                          10.13.4.117
  MIDType                               IP4_ADDR
  DeviceName                            -
```

```
  Retrans                                Enable

  Active MGC       MGC Port       :2944            MGC IP1:10.13.2.118
  Active MGC       MGC Port       :2944            MGC IP2:-
  Active MGC       MGC Domain Name:-
  Standby MGC      MGC Port       :-               MGC
IP1:-
  Standby MGC      MGC Port       :-            MGC IP2:-
  Standby MGC      MGC Domain Name:-
  ------------------------------------------------
```

7.3.1.4 (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 need not be configured on the AG. If the services such as emergency calls and emergency standalone are not required, the digitmaps need not be configured.

Context

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) before configuring the digitmap.

- 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, it indicates that 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 call digitmap (due to call restriction in the case of an overload)
- Automatic redial digitmap of the card service

Table 7-22 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 7-22 Digitmap format in the H.248 protocol

Digit or Character	Description
0-9	Indicate dialed digits 0-9.
A-D	Indicate 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.
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. The short timer is applied when the collected number matches at least one dialing scheme, but more numbers may be received and these numbers match other dialing schemes.
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. The long timer is applied when the dialed number does not match any dialing scheme.
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.

Procedure

Step 1 Enter the MG interface mode.

In global config mode, run the **interface h248** command to enter the MG interface mode.

Step 2 Configure the digitmap.

Run the **digitmap set** command to configure the digitmap required in the data plan.

Step 3 (Optional) Configure the digitmap timer.

Run the **digitmap-timer** command to configure the digitmpa timer.

Generally, the digitmap 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.

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
  Urgent digitmap (for overload or bandwidth restrict)    : -
  Dualdial digitmap for card service                      : -
  ------------------------------------------------------------------------
```

7.3.1.5 (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 36 software parameters (numbered from 0 to 35) of an MG interface that supports H.248. **Table 7-23** lists the configurable parameters, and the other parameters are reserved in the system.

Table 7-23 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. This parameter can be configured only when the MG interface is in the local closed state. If the MG interface does not support dual homing, 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, even if the MG interface has registered with the secondary MGC, the MG interface can automatically switch back to the primary MGC if the primary MGC recovers. If the MG interface supports dual homing, you can run the **mgc_switch(h248)** command to perform the MGC switching.	Numeral type. Range: 0-2. ● 0: Indicates that dual homing is not supported. ● 1: Indicates that dual homing rather than auto-switching is supported. ● 2: Indicates that dual homing and auto-switching is supported. Default: 0

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. This parameter can be configured only when the MG interface is in the local closed state. When a wildcard is used for registration, all the terminals connecting to the MG interface register with the MGC through a message. This reduces 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".	Numeral type. Range: 0-1. ● 0: Indicates that a wildcard is used. ● 1: Indicates that a wildcard is not used. Default: 0
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 (h248)** command to configure the authentication parameters, and then run the **reset(h248)** 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. **CAUTION** Resetting the MG interface may interrupt the services.	Numeral type. Range: 0-1. ● 0: Indicates that device authentication is supported. ● 1: Indicates that device authentication is not supported. Default: 1

Parameter	Description	Default Setting
7	Indicates whether the MG interface supports security header. To configure an MG interface to or not to support security header, use this parameter. After configuring the security header, run the **auth(h248)** command to configure the authentication parameters, and then run the **reset(h248)** command to reset the MG interface. In this case, the MGC can manage the MG devices in a security manner, ensuring that the data is complete.	Numeral type. Range: 0-1. ● 0: Indicates that security header is supported. ● 1: Indicates that security header is not supported. Default: 1
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.	Numeral type. Range: 0-3. ● 0: Indicates that no call is permitted. ● 1: Indicates that only internal call is permitted. ● 2: Indicates that only emergency call is permitted. ● 3: indicates that internal call and emergency call are permitted. Default: 0

Parameter	Description	Default Setting
13	Indicates the maximum digitmap matching flag of the MG interface. To configure digitmap matching scheme of the MG interface, use this parameter. In the shortest matching, the collected phone number is reported immediately after it matches the digitmap. This is the quickest report mode. In certain cases, however, the phone number is reported before it is collected completely. In the longest matching, even if the collected phone number matches a dialing scheme, the phone number is not reported because more numbers may be received. If there is no dialing within the duration of the short timer (default: 5s), the phone number is reported after the short timer times out. Otherwise, the system matches other digitmap schemes. You can run the **digitmap-timer** command to configure the time length of the digitmap timer.	Numeral type. Range: 0-1. ● 0: Indicates that the match follows the protocol. ● 1: Indicates the longest match. ● 2: Indicates the shortest match. Default: 2
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.	Numeral type. Range: 0-1. ● 0: Indicates that media streams are not filtered by source port. ● 1: Indicates that media streams are filtered by source port. Default: 0

Parameter	Description	Default Setting
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 the function of filtering media streams by source port is disabled, the MG interface automatically filters the source port if the filtering timer times out.	Numeral type. Range: 0-30s. Default: 5s
22	Indicates the type of the prompt tone after the communication between the MG and the MGC is interrupted.	Numeral type. Range: 0-2. ● 0: Indicates the busy tone. ● 1: Indicates the device congestion tone. ● 2: Indicates the voice prompt. Default: 0
23	Indicates the length of the timer for synchronizing the port status.	Numeral type. Range: 0-120s. Default: 35s.
24	Indicates the maximum value of the Real-Time Transport Protocol (RTP) termination ID. The maximum values of RTP termination ID on the MG and the MGC must be the same.	Numeral type. Range: 0-65535.
25	Indicates the maximum random value for the protection against avalanche of the H.248 interface.	Numeral type. Range: 30000-300000ms.
26	Indicates the type of local blocking play tone.	Numeral type. Range: 0-4. ● 0: Indicates the busy tone. ● 1: Indicates the device congestion tone. ● 2: Indicates the mute. ● 3: Indicates the user-defined tone 1. ● 4: indicates the user-defined tone 2. Default: 0

Parameter	Description	Default Setting
27	Indicates the type of remote blocking play tone.	Numeral type. Range: 0-4. ● 0: Indicates the busy tone. ● 1: Indicates the device congestion tone. ● 2: Indicates the mute. ● 3: Indicates the user-defined tone 1. ● 4: Indicates the user-defined tone 2. Default: 0.
28	Indicates the duration of the howler tone.	Numeral type. Range: 1-65535s. Default: 60s
29	Indicates the duration of message waiting tone.	Numeral type. Range: 1-60000s. Default: 3s
30	Indicates the time limit of the alarm for extra long call.	Numeral type. Range: 1-65535 min. Default: 60 min.
31	Indicates whether to report the alarm for extra long call.	Numeral type. Range: 0-1. ● 0: Indicates that the alarm is reported. ● 1: Indicates that the alarm is not reported. Default: 1
32	Indicates the minimum interval for automatic registration of the remote block port. The MG interface is blocked because the MGC does not respond or responds incorrectly. After this parameter is configured, the MG interface can automatically register with the MGC.	Numeral type. Range: 0-60000s. 0 indicates that the port does not register automatically. Default: 1800s
33	Indicates whether the heartbeat message is disabled.	Numeral type: ● 0: Indicates that the heartbeat message is disabled. ● 1: Indicates that the heartbeat message is enabled. Default: 1

Parameter	Description	Default Setting
34	Indicates whether the MG actively establishes or releases the link for the BRA user after the MGC initiates the in-service or OOS request.	Numeral type. Range: 0-1. ● 0: Yes ● 1: No Default value: 0.
35	Indicates the out of service (OOS) and in-service mode of the ISDN port. ● When the OOS or in-service in wildcard mode is supported, the ISDN port reports the in-service or OOS, that is, reports only one in-service or OOS message in wildcard mode. This effectively reduces the messages between the MG interface and the MGC. ● When the in-service or OOS in single channel mode is supported, the ISDN port reports the in-service or OOS message over each channel. ● When both the in-service or OOS in single channel mode and the in-service or OOS in wildcard mode are supported, the in-service or OOS message is reported according to the actual requirement or reported in single channel mode.	Numeral type. Range: 0-2. ● 0: Indicates that both the OOS or in-service in single channel mode and the OOS or in-service in wildcard mode are supported. ● 1: Indicates that only the OOS and in-service in single channel mode is supported. ● 2: Indicates that only the OOS and in-service in wildcard mode is supported. Default value: 1.

Procedure

Step 1 Enter the MG interface mode.

In global config mode, run the **interface h248** command to enter the MG interface mode.

Step 2 Configure software parameters.

Run the **mg-software parameter** command the software parameters required in the data plan.

Step 3 Check whether the software parameters are the same as those in the data plan.

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
```

7.3.1.6 (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.

Context

Add the ringing mode mapping records of a specified MG interface. After the adding is successful, the MG interface can obtains the ringing mode according to the peer parameters issued by the MGC and then play the ringing to the user in this mode.

Procedure

Step 1 Check whether the ringing mode meets the requirements.

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**.

Step 2 Configure the user-defined ringing mode.

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

The system supports 16 user-defined ringing modes, which can be modified but cannot be added or deleted.

Step 3 Enter the MG interface mode.

Run the **interface h248** command to enter the MG interface mode.

Step 4 Add a ringing mapping.

Run the **mg-ringmode add** command to add a ringing mapping.

CAUTION

1. The peer parameter *mgcpara* that is on the MG and issued by the MGC 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.

Step 5 Check whether the ringing mapping is the same as that in the data plan.

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
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> }:
```

```
Command:
        display mg-ringmode attribute
------------------------------------------------------
 MGID       PeerPara   CadenceRing   InitialRing
------------------------------------------------------
 0          1          128           144
------------------------------------------------------
```

7.3.1.7 (Optional) Configuring the TID Format of an MG Interface

The TID format determines how various user terminal IDs on the MG interface are generated.

Context

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 before configuring the TID format.

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", it indicates that 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), it indicates that 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 shelf 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 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** 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.

Precaution

- 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

Step 1 To query the template information.

Run the **display tid-template** command to query the information about the default TID template of the system.

Step 2 Check whether the default TID template of the system meets the service requirements.

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**.

Step 3 Enter the MG interface mode.

Run the **interface h248** command to enter the MG interface mode.

Step 4 Configure the TID templates and the terminal prefix of various types of users on the current MG (VAG).

- In H248 mode, run the **tid-format rtp** command to configure the TID template and terminal prefix of the RTP ephemeral termination.
- In H248 mode, run the **tid-format pstn** command to configure the TID template and terminal prefix of the PSTN user.
- In H248 mode, run the **tid-format pstn** command to configure the TID template and the terminal prefix of the ISDN BRA user.
- In H248 mode, run the **tid-format pstn** command to configure the TID template and terminal prefix of the ISDN PRA user.

Step 5 Check whether the TID template and the terminal prefix are the same as those in the data plan.

Run the **display tid-format** 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 the TID
template 3.
  -------------------------------------------------
  Index      : 3
  Format     : %u/%u/%u
  Para-list  : F+1,S+1,P+1  // Keywords in the parameter list of the TID template
are "F", "S", and "P".
  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><Length
1-15> }:

  Command:
          display mgpstnuser 0/2/0
  ------------------------------------------------------------------------------
  F  /S /P    MGID     TelNo            Priority PotsLineType     TerminalID
  ------------------------------------------------------------------------------
  0  /2 /0    1        -                Cat3     DEL              aln/1/3/1
  ------------------------------------------------------------------------------
```

7.3.1.8 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.

Precaution

CAUTION

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

Step 1 Enter the H248 mode.

Run the **interface h248** command to enter the H248 mode.

Step 2 Enable the MG interface.

Run the **reset coldstart** command to enable the MG interface.

Step 3 Check the state of the MG interface.

You can query the status of the MG interface by using one of the following two methods.

- Run the **display if-h248 state** command to check whether the MG interface is in the normal state.
- Run the **quit** command to quit the global config mode, and then run the **display if-h248 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
--------------------------------------------------------------------------------
```

7.3.2 Configuring the IUA Link

This topic describes how to configure the IUA link for signaling transmission between the MA5616 and MGC in the VoIP ISDN BRA service.

Context

- Simple Control Transmission Protocol (SCTP) is a connection-oriented protocol. Its most fundamental function is to provide reliable transmission for interaction messages between the MA5616 and MGC. The SCTP protocol implements services based on the association between two SCTP endpoints. SCTP can be regarded as a transmission layer. Its upper layer is called SCTP subscriber, and its lower layer is the IP network.
- The IUA link is the carrier of the interaction signaling between the MA5616 and MGC.

7.3.2.1 Adding an IUA Link Set

This topic describes how to add an IUA link set. When configuring the VoIP ISDN service, you need to configure the IUA link to carry the Q.931 call signaling. Before adding an IUA link, you must add a corresponding link set. Otherwise, the link cannot be added.

Context

- The system supports the configuration of a maximum of two IUA link sets.
- After a link set is configured successfully, the system is in the deactivated state by default.

Procedure

Step 1 In global config mode, run the **sigtran** command to enter the Sigtran mode.

Step 2 Run the **iua-linkset add** command to add an IUA link set.

Step 3 You can run the **display iua-linkset attribute** command to check whether the configured IUA link set information is the same as the data plan.

----End

Example

Assume that the link set ID is 0, working mode of the link set is active/standby mode, pending duration is 20s, prefix of the IID is b/, IID generation mode is using the binary value that is automatically generated in ffsspp mode, namely, parameter 2. To add such an IUA link set, do as follows:

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 0 trafficmode override pendingtime 20 iid-
map 2
braprefix b/
huawei(config-sigtran)#display iua-linkset attribute
{ <cr>|linksetno<L> }:

  Command:
          display iua-linkset attribute
------------------------------------------------------------
  LinksetNo             :0
  MGID                  :-
  PendingTime           :20
  TrafficMode           :override
  C/S-Mode              :server
  IID-Type              :integer
  IID-Map               :2
  BRA IID-Prefix        :b/
  BRA IID-Suffix        :-
  PRA IID-Prefix        :-
  PRA IID-Suffix        :-
  Jointly-Work          :disable
------------------------------------------------------------
```

7.3.2.2 Adding an IUA Link

This topic describes how to add an IUA link. After the link set is added, you can add an IUA link to carry the Q.931 call signaling for the ISDN user.

Prerequisites

The IUA link set must be added.

Context

- Make sure that a minimum of one item in the local port ID, local IP address, remote port ID, and remote IP address of a link is different from the corresponding item of other links.
- Only two links can be configured in the same link set. In addition, the local IP addresses of the two links must be the same.

Procedure

Step 1 (This step is not required if the command line interface is already in the Sigtran mode.) In global config mode, run the **sigtran** command to enter the Sigtran mode.

Step 2 Run the **iua-link add** command to add an IUA link.

Step 3 You can run the **display iua-link attribute** command to check whether the configured IUA link information is the same as the data plan.

----End

Example

Assume that the link ID is 0, link set ID is 0, local port ID is 1402, local IP address is 10.10.10.10, remote port ID is 1404, and remote IP address 1 is 10.10.10.20. To add such a link, do as follows:

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-link add 0 0 1402 10.10.10.10 1404 10.10.10.20
huawei(config-sigtran)#display iua-link attribute
{ <cr>|linkno<L> }:

  Command:
          display iua-link attribute
  ------------------------------------------------------------------------
  LinkNo                :  0
  LinksetNo             :  0
  Local port            :  1402
  Local IP address      :  10.10.10.10
  Remote port           :  1404
  Remote IP address     :  10.10.10.20
  Remote IP address 2   :  -
  Bound MGC             :  -
  Priority              :  0
  ------------------------------------------------------------------------
```

7.3.3 Configuring the VoIP ISDN BRA User

This topic describes how to configure the VoIP ISDN BRA user. After the MG interface is configured, you can add the VoIP ISDN BRA user on this interface to implement the VoIP ISDN BRA service.

7.3.3.1 Configuring the ISDN BRA User Data

This topic describes how to configure the ISDN BRA user data based on H.248 (the data must be the same as the corresponding data on the MGC) so that the ISDN BRA user can access the network to use the ISDN BRA service.

Prerequisites

The H832DSLD service board must be inserted into the planned slot correctly and the board must be in the normal state.

NOTE

You can run the **display board** command to query the board status.

- If the query result is **Normal**, it indicates that the board is in the normal state.
- If the query result is **Auto_find**, you need to run the **board confirm** command to confirm the board.
- If the query result is **Failed**, handle the fault according to Service Board Is in the Failed State described in the *Maintenance Guide*.

The working mode of the BRA port must be configured according to the requirements. For details about how to configure the working mode of the BRA port, see **7.3.3.4 (Optional) Configuring the Attributes of an ISDN BRA Port**.

Context

One H832DSLD board can be configured with a maximum of eight ISDN BRA users.

Default Configuration

Table 7-24 lists the default settings of the attributes of the ISDN BRA user. When configuring these attributes, you can modify the values according to the service requirements.

Table 7-24 Default settings of the attributes of the ISDN BRA user

Parameter	Default Settings
Priority of the ISDN BRA user	cat3: (common user)
Flag of reporting the UNI fault of the ISDN BRA user	Disable
Threshold for the number of auto recoveries from deterioration faults	20

Procedure

Step 1 In global config mode, run the **esl user** command to enter the ESL user mode.

Step 2 Run the **mgbrauser add** command to add an ISDN BRA.

- When **iid-map** in the **iua-linkset add** command is configured to 1, interfaceid must be configured and be different from the interfaceid of other users in the same link set.
- The terminal ID of an ISDN BRA user must be different from the terminal IDs of other users.
- If the MG interface does not support the terminal layering function, the terminal ID must be configured when an ISDN BRA user is added. In addition, the terminal ID must differ from the terminal ID of the existing ISDN BRA user by an integer multiple of 2. For example, to add the first ISDN BRA user, the terminal ID is 2; to add the second ISDN BRA user, the terminal ID is 4; to add the third ISDN BRA user, the terminal ID is 6; the rest may be deduced by analogy.
- If the MG interface supports the terminal layering function, the terminal ID cannot be configured when an ISDN BRA user is added on the MG interface. The system automatically allocates a terminal ID for the user.

Step 3 Run the **display mgbrauser attribute** command to check whether the ISDN PSTN user data is the same as the data plan.

Step 4 (Perform this step only when you need to modify the attributes of the ISDN BRA user.) Run the **mgbrauser attribute set** command to configure the attributes of the ISDN BRA user.

Step 5 (Perform this step only after you modify the attributes of the ISDN BRA user.) Run the **display mgbrauser attribute** command to query whether the configured attributes of the ISDN BRA user are the same as the data plan.

----End

Example

Assume the following configurations:

- Link set ID: 0

- IUA interface ID: 0 (value of **iid-map**: 1)
- Terminal ID: 2 (not supporting the terminal layering function)
- User priority: cat3
- Telephone number: 83110001 (Before configuring a emergency standalone number, ensure that the emergency standalone function has been enabled on the MG interface. For details, see **7.3.1.5 (Optional) Configuring the Software Parameters of an MG Interface**.)
- UNI alarm report function: enable
- Threshold for the number of auto recoveries from L1 deterioration faults: 30

To add an ISDN BRA user with such configurations on port 0/4/0 of MG interface 0, do as follows:

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/4/0 0 0 interfaceid 0 terminalid 2 prior
ity cat3 telno 83110001
 Are you sure to configure the working mode of the DSL board to normal and reset
 the board automatically? (y/n)
[n]:y
huawei(config-esl-user)#display mgbrauser 0/4
  ------------------------------------------------------------------------------
  F  /S /P /B  MGID     LinkSetNo UserIFID TelNo            Priority TerminalID
  ------------------------------------------------------------------------------
  0  /4 /0 /0  0        0         0        83110001         Cat3     A2
  ------------------------------------------------------------------------------
huawei(config-esl-user)#mgbrauser attribute set 0/4/0 priority cat3 unireport
enable auto-resume-limit 30
huawei(config-esl-user)#display mgbrauser attribute 0/4/0
{ <cr>|endframeid/slotid/portid<S><Length 1-15> }:

  Command:
          display mgbrauser attribute 0/4/0
  ------------------------------------------------------
  F  /S /P  UNIreport  Prior  Auto-reservice-times/limit
  ------------------------------------------------------
  0  /4 /0  enable     Cat3   0/30
  ------------------------------------------------------
```

7.3.3.2 (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 7-25 lists the system parameters supported by the MA5616.

Table 7-25 System parameters supported by the MA5616

Parameter	Description	Default Setting
0	Indicates the howler tone sending flag.	1: Indicates that the howler tone is sent.
1	Indicates the overseas version flag.	0: Indicates China.

Parameter	Description	Default Setting
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 on the same device.	0: Indicates that the media stream is forwarded within the device.
6	Indicates whether to send power deny flag when softswitch indicates block.	1: Not send

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 the planned data.

----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,
14:Turkey,
20:Germany
  ---------------------------------------------------------------------------
```

7.3.3.3 (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 7-26 lists the overseas parameters supported by the MA5616.

Table 7-26 Overseas parameters supported by the MA5616

Parameter	Description	Default Setting
0	Indicates the upper threshold of the flash-hooking duration.	350 ms (in compliance with the Chinese mainland standards)
1	Indicates the lower threshold of the flash-hooking duration.	100 ms (in compliance with the Chinese mainland 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 type of ring DC offset.	Line B offset

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 the planned data.

----End

Example

To set the upper flash-hooking threshold (overseas parameter 0) to 800 ms (in compliance with the Hong Kong standards) and the lower flash-hooking threshold (overseas parameter 1) to 100 ms (in compliance with the Hong Kong standards), do as follows:

```
huawei(config)#oversea parameters 0 800
huawei(config)#oversea parameters 1 100
huawei(config)#display oversea parameters
{ <cr>|name<U><0,3> }:
  Command:
          display oversea parameters
  ------------------------------------------------------------------------------
  Parameter name index: 0     Parameter value: 800
  Mean: Hooking upper threshold(ms), reference: China:350, HongKong:800
  ------------------------------------------------------------------------------
  Parameter name index: 1     Parameter value: 100
  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: 1
  Mean: Type of ring DC offset, 0:Line A offset, 1:Line B offset
  ------------------------------------------------------------------------------
```

7.3.3.4 (Optional) Configuring the Attributes of an ISDN BRA Port

This topic describes how to configure the attributes of an ISDN BRA port to ensure that the ISDN BRA port can meet the actual application requirements. You can configure the auto-deactivation status, remote power supply status, UNI fault alarming function, and working mode of the port.

Default Configuration

Table 7-27 lists the default values of the attributes of an ISDN BRA port. When configuring the attributes, you can change the values according to the service requirements.

Table 7-27 Default values of the attributes of an ISDN BRA port

Parameter	Default Setting
Autodeactive	Disable
Autodeactive-delay	30
Activemode	unstable-active
Remotepower	Disable
Unialarm	Disable
Workmode	p2mp

Procedure

Step 1 In global config mode, run the **braport** command to enter braport mode.

Step 2 Run the **braport attribute set** command to configure the attributes such as the working mode, auto-deactivation status, and remote power supply status of the port.

If an ISDN BRA port needs to be connected to multiple terminal users, configure the working mode of the port to p2mp. If an ISDN BRA port needs to be connected to only one terminal user, configure the working mode of the port to p2p.

For detailed description of the **braport attribute set** command, see the parameter description in **braport attribute set**.

----End

Example

Assume that the working mode is p2mp, the activation mode is stable, and the auto-deactivation function is disabled. To configure such attributes of ISDN BRA port 0/4/0, do as follows:

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/4/0 workmode p2mp activemode stable-
active
huawei(config-braport)#display braport attribute
{ frameid/slotid/portid<S><Length 1-15>|frameid/slotid<S><Length 1-15> }:0/4/0

  Command:
          display braport attribute 0/4/0
------------------------------------------------------------------------------
F  /S /P  Remotepower Workmode Autodeactive Deactivedelay Activemode Unialarm
------------------------------------------------------------------------------
0  /4 /0  disable     p2mp     disable      30            stable     disable
------------------------------------------------------------------------------
```

7.4 Configuring the FoIP Service (Based on the H.248 Protocol)

This topic describes how to configure the FoIP service when the H.248 protocol is used to transmit the fax data service over the IP network.

Prerequisites

- The communication between the MG and the MGC must be in the normal state, and the fax mode on the MGC side must be consistent with the fax mode on the MG side.
- The voice service port used by the FoIP service and the voice service on that port must be in the normal state.

Context

The FoIP service can be classified according to the following modes:

- According to the coding/decoding mode: In this mode, the FoIP service is classified into T.30 transparent transmission fax (using the G.711 coding) and T.38 fax (using the T.38 coding).
- According to the role of the MGC: In this mode, the FoIP service is classified into the SoftSwitch-controlled fax and the self-switch fax (the fax flow is controlled by the MGC itself).

The MA5616 supports the self-switch mode and the auto-negotiation mode:

- Self-switch: If the self-switch mode is configured, the fax working mode of the MA5616 is not controlled by the MGC. Therefore, manual configuration is required.
- Auto-negotiation: If the auto-negotiation mode is configured, the fax working mode of the MA5616 is automatically configured during the negotiation with the MGC. Therefore, manual configuration is not required.

The MA5616 supports the V2 and V3 fax flows.

- In the V2 negotiation flow, the MG determines the transmission mode to be used (transparent transmission mode or T.38-based transmission mode), and determines whether the fax port ID is increased by 2. No signaling negotiation is performed when the port ID is increased by 2. Therefore, when the V2 T.38 is configured, the IDs of the local and peer ports must be configured consistently. That is, the port IDs are both increased by 2 or neither of the port IDs is increased by 2.
- In the V3 negotiation flow, the softswitch determines the transmission mode to be used (transparent transmission mode or T.38-based transmission mode). To be specific, if the softswitch requires the T.38-based transmission mode, this transmission mode is used; otherwise, the transparent transmission mode is used. In addition, the softswitch determines whether the fax port ID is increased by 2 through signaling negotiation.

The MA5616 supports the 10 ms packing function and the RFC 2198 function.

- 10 ms packing function: In addition to the 20 ms G.711 transparent transmission, the fax transparent transmission function is added with the 10 ms G.711 transparent transmission. This reduces delay, improves the performance of transparent transmission, and decreases the impact of packet loss on the transmission of the fax service data.

- RFC 2198 function: Through the redundant transmission, the RFC 2198 function improves the reliability of data transmission. When the network packet loss occurs, the RFC 2198 can ensure the service quality.

Default Configuration

Table 7-28 lists the default configuration of the flows of the FoIP service:

Table 7-28 Default configuration of the flows of the FoIP service

Item	Default
FAX transfers mode	Thoroughly
FAX flow	V3 Flow
Packet-interval-10ms	Disable
Negomode	Negotiation
Rfc2198-start-mode	Disable Rfc2198SmartStartup
TransEvent	ControlledByMGC
Vbd-codec	G.711A
Vbd-payload-type	Static

Procedure

Step 1 Configure public fax and modem parameters.

1. Run the **fax-modem parameters negomode** command to configure the negotiation mode.
2. (Optional) Run the **fax-modem parameters packet-interval-10ms** command to enable or disable the 10ms packing function.
3. (Optional) Run the **fax-modem parameters rfc2198-start-mode** command to configure the RFC2198 function.
4. (Optional) Run the **fax-modem parameters transevent** command to configure the transmission mode of the modem event.
5. (Optional) Run the **fax-modem parameters vbd-codec** command to configure the codec mode of the voice-band data (VBD).
6. (Optional) Run the **fax-modem parameters vbd-pt-type** command to configure the payload type of the VBD.

Step 2 Configure the fax working mode.

- If the auto-negotiation mode is configured in **Step 1.1**, go to **Step 2.1**.
- If the self-switch mode is configured in **Step 1.1**, run the **fax parameters workmode** command to configure fax working mode.

1. Run the **fax parameters flow** command to configure the fax flow.
2. (Optional) Run the **fax parameters is-port+2** command to configure the T.38 port ID.

NOTE

If the fax machines are not configured on the same MG interface, the configurations for whether the T.38 fax port ID is added by 2 for the two sides must be consistent. That is, the T.38 fax port ID of the two sides are both added by 2 or not added by 2.

Step 3 Query public fax and modem parameters and the codec mode of the fax.

Run the **display fax-modem parameters** and **display fax parameters** commands to query the fax transmission parameters.

----End

Example

Assume that:

- The negotiation mode of the MA5616 is self-switch.
- The 10 ms packing function and the RFC2198 intelligent startup function are enabled.
- The transmission mode of the modem event is ControlledByMGC (default).
- The codec mode of the VBD is G.711A (default).
- The payload type of the VBD is static payload (default).
- The working mode of the fax is transparent transmission (thoroughly).
- The fax working flow is V3 flow.

To configure the MA5616, do as follows:

```
huawei(config)#fax-modem parameters negomode selfswitch packet-interval-10ms
enable
rfc2198-start-mode enableRfc2198SmartStartup transevent controlledByMGC
vbd-codec G.711A vbd-pt-type static
huawei(config)#fax parameters workmode thoroughly flow v3
huawei(config)#display fax-modem parameters
  ---------------------------------------------------------------------------
  Negomode               : Self switch
  Packet-interval-10ms   : Enable
  Rfc2198-start-mode     : Enable Rfc2198SmartStartup
  TransEvent             : ControlledByMGC
  Vbd-codec              : G.711A
  Vbd-payload-type       : Static
  ---------------------------------------------------------------------------
huawei(config)#display fax parameters
  ---------------------------------------------------------------------------
  FAX transfers mode                  :Thoroughly
  T38 Fax Port                        :RTP port
  FAX flow                            :V3 Flow
  ---------------------------------------------------------------------------
```

7.5 Configuring the FoIP Service (Based on the SIP Protocol)

This topic describes how to configure the FoIP service based on the SIP protocol to transmit the fax data service over the IP network.

Prerequisites

- The communication between the MA5616 and the IMS must be in the normal state.
- The voice service port used by the FoIP service and the voice service on that port must be in the normal state.

Context

During the application of the fax service, the FoIP service can be classified into two modes according to the participation of the SIP signaling in the transmission control process:

- Self-switch: If the self-switch mode is configured, the fax working mode of the MA5616 needs to be configured manually.
- Auto-negotiation: If the auto-negotiation mode is configured, the fax working mode of the MA5616 needs to be configured manually.

The FoIP service can be classified into two modes according to the fax coding:

- Transparent transmission fax: The voice encoding (G.7xx encoding) is adopted.
- T.38 fax: The T.38 encoding is adopted.

The MA5616 supports the 10 ms packing function and the RFC 2198 function.

- 10 ms packing function: In addition to the 20 ms G.711 transparent transmission, the fax transparent transmission function is added with the 10 ms G.711 transparent transmission. This reduces delay, improves the performance of transparent transmission, and decreases the impact of packet loss on the transmission of the modem service data.
- RFC 2198 function: Through the redundant transmission, the RFC 2198 improves the reliability of data transmission. When the network packet loss occurs, the RFC 2198 can ensure the service quality.

Data preparation

It is recommended that you plan the working mode of the fax on the entire IP multimedia subsystem (IMS) before configuring the data so that the working mode on the entire network is consistent.

Table 7-29 Items involved in the FoIP service

Item	Option	Remarks
Codec negotiation mode	Negotiation	The codec mode needs to be negotiated through the SIP signaling.
	Self-switch	The MG determines what codec mode is used.
Codec mode	Transparent transmission fax	The G.711 encoding is adopted.
	T.38 flow	The T.38 encoding is adopted.

Default Configuration

Table 7-30 lists the default configuration of the flows of the FoIP service.

Table 7-30 Default configuration of the flows of the FoIP service

Item	Default
Codec negotiation mode	Negotiation
Codec mode	Transparent transmission fax

Procedure

Step 1 Configure public fax and modem parameters.

1. Run the **interface sip** command to enter the SIP mode.
2. Run the **fax-modem parameters negomode** command to configure the negotiation mode.
3. (Optional) Run the **fax-modem parameters rtp-interval** command to enable or disable the 10 ms packing function.
4. (Optional) Run the command to configure the RFC2198 function.
5. (Optional) Run the **fax-modem parameters vbd-codec** command to configure the codec mode of the voice-band data (VBD).
6. (Optional) Run the **fax-modem parameters vbd-pt-type** command to configure the payload type of the VBD.
7. (Optional) Run the **rfc2833 set rfc2833-fax-modem** command to configure the mode for reporting fax or modem events.

Step 2 Configure the codec mode of the fax.

Run the **fax parameters** command to configure the fax working mode of the SIP interface.

Step 3 Check whether the fax transmission parameters are the same as the data plan.

Run the **display fax-modem parameters** and **display fax parameters** commands to check the fax transmission parameters.

----End

Example

Assume that:

- The negotiation mode of the MA5616 is self-switch.
- The 10 ms packing function and the RFC2198 intelligent startup function are enabled.
- The RFC2198 negotiation mode is fixedstart.
- The codec mode of the VBD is G.711A.
- The payload type of the VBD is static payload.
- The transmission mode of the fax is transparent transmission (thoroughly).

To configure the MA5616, do as follows:

```
huawei(config)#interface sip 0
huawei(config-if-sip-0)#fax-modem parameters negomode self-switch rtp-interval 1
vbd-pt-type static
huawei(config-if-sip-0)#rfc2198 set rfc2198-negomode fixedstart rfc2198-startmode
smart2198
huawei(config-if-sip-0)#display fax-modem parameters
 --------------------------------------------------------------------------------
```

```
 MGID                  :0
 Nego-mode             :self-switch
 Rtp-interval          :10ms
 Vbd-codec             :G.711A
 Vbd-pt-type           :static
 Vbd-attribute-type    :v.152
 ------------------------------------------------------------------------------
huawei(config-if-sip-0)#fax parameters transmode 0
huawei(config-if-sip-0)#quit
huawei(config)#display fax parameters
{ <cr>|mgid<U><0,16777215> }:0

  Command:
          display fax parameters 0
 ---------------------------------------
 MGID      Transmode
 ---------------------------------------
 0         Thoroughly
 ---------------------------------------
```

7.6 Configuring the MoIP Service (Based on the H.248 Protocol)

This topic describes how to configure the MoIP service when the H.248 protocol is used to transmit the modem data service over the IP network.

Prerequisites

- The communication between the MG and the MGC must be in the normal state.
- The voice service port used by the MoIP service and the voice service on that port must be in the normal state.

Context

The MA5616 supports the self-switch mode and the auto-negotiation mode:

- Self-switch: If the self-switch mode is configured, the modem working mode of the MA5616 is not controlled by the MGC. Therefore, manual configuration is required.
- Auto-negotiation: If the auto-negotiation mode is configured, the modem working mode of the MA5616 is automatically configured during the negotiation with the MGC. Therefore, manual configuration is not required.

The MA5616 supports the 10 ms packing function and the RFC 2198 function.

- 10 ms packing function: In addition to the 20 ms G.711 transparent transmission, the modem transparent transmission function is added with the 10 ms G.711 transparent transmission. This reduces delay, improves the performance of transparent transmission, and decreases the impact of packet loss on the transmission of the modem service data.
- RFC 2198 function: Through the redundant transmission, the RFC 2198 improves the reliability of data transmission. When the network packet loss occurs, the RFC 2198 can ensure the service quality.

The MoIP service supports two transmission modes: the transparent transmission mode and the relay (redundancy) mode. The MA5616 supports only the modem service in the transparent transmission mode. In the transparent transmission mode, the MG uses the G.711 mode to encode and decode the modem signal, and processes the signal like processing the common RTP data. The transparent transmission mode depends on the bearer network to a great extent.

The report mode of the modem event:

- Direct: In direct mode, the host reports the modem event to the MGC immediately when the host receives a modem event.
- Delay: In delay mode, the host does not report the modem event immediately after an event is received, but waits for a period of time until the event times out and the fax signal is detected. In this way, when the high-speed modem machine fails in the high-speed transmission negotiation, it can transmit data in low-speed transmission mode.
- Direct for high-speed signals: In the mode of the direct for high-speed signals, the host reports the modem event with low speed signals to the MGC 5.5s after the host receives a modem event; the host reports the modem event with high speed signals to the MGC immediately when the host receives a modem event.

Procedure

Step 1 Configure public fax and modem parameters.

1. Run the **fax-modem parameters negomode** command to configure the negotiation mode.
2. (Optional) Run the **fax-modem parameters packet-interval-10** command to enable or disable the 10 ms packing function.
3. (Optional) Run the **fax-modem parameters RFC2198-start-mode** command to configure the RFC2198 function.
4. (Optional) Run the **fax-modem parameters transevent** command to configure the transmission mode of the modem event.
5. (Optional) Run the **fax-modem parameters vbd-codec** command to configure the codec mode of the voice-band data (VBD).
6. (Optional) Run the **fax-modem parameters vbd-pt-type** command to configure the payload type of the VBD.

Step 2 Configure the event report mode of fax codec.

1. Run the **modem parameters tranmode** command to configure the transmission mode of the modem.
2. (Optional) Run the **modem parameters eventmode** command to configure the report mode of the modem event.

   NOTE

   - To enable the MGC to quickly respond to a modem event, you need to configure the report mode of the modem event as the direct report mode.
   - By default, the transmission mode of the modem is the transparent transmission mode, and the modem event is reported in the direct mode.

Step 3 Query public fax and modem parameters and the codec mode of the fax.

Run the **display fax-modem parameters** and **display modem parameters** commands to query modem parameters.

----End

Example

Assume that:

- The negotiation mode of the MA5616 is self-switch.

- The 10 ms packing function and the RFC2198 intelligent startup function are enabled.
- The transmission mode of the modem event is ControlledByMGC (default).
- The codec mode of the VBD is G.711A (default).
- The payload type of the VBD is static payload (default).
- The working mode of modem is transparent transmission (thoroughly).
- The report mode of the modem event is direct.

To configure the MA5616, do as follows:

```
huawei(config)#fax-modem parameters negomode selfswitch packet-interval-10ms
enable
rfc2198-start-mode enableRfc2198SmartStartup transevent controlledByMGC
vbd-codec G.711A vbd-pt-type static
huawei(config)#modem parameters tranmode 0 eventmode 1
huawei(config)#display fax-modem parameters
  ---------------------------------------------------------------------------
  Negomode               : Self switch
  Packet-interval-10ms   : Enable
  Rfc2198-start-mode     : Enable Rfc2198SmartStartup
  TransEvent             : ControlledByMGC
  Vbd-codec              : G.711A
  Vbd-payload-type       : Static
  ---------------------------------------------------------------------------
huawei(config)#display modem parameters
  ---------------------------------------------------------------------------
  MODEM transfers mode                  :Thoroughly
  MODEM event mode                      :Direct
  ---------------------------------------------------------------------------
```

7.7 Configuring the MoIP Service (Based on the SIP Protocol)

This topic describes how to configure the MoIP service when the SIP protocol is used to transmit the modem data service over the IP network.

Prerequisites

- The communication between the MA5616 and the IMS must be in the normal state.
- The VoIP service must be configured, see **7.2.2 Configuring the VoIP PSTN User**.
- The voice service port used by the MoIP service and the voice service on that port must be in the normal state.

Context

The MA5616 supports the self-switch mode and the auto-negotiation mode:

- Self-switch: If the self-switch mode is configured, you need to configure the fax working mode of the MA5616 manually.
- Auto-negotiation: If the auto-negotiation mode is configured, you need to configure the fax working mode of the MA5616 manually.

The MA5616 supports the 10 ms packing function and the RFC 2198 function.

- 10 ms packing function: In addition to the 20 ms G.711 transparent transmission, the modem transparent transmission function is added with the 10 ms G.711 transparent transmission.

This reduces delay, improves the performance of transparent transmission, and decreases the impact of packet loss on the transmission of the modem service data.

- RFC 2198 function: Through the redundant transmission, the RFC 2198 improves the reliability of data transmission. When the network packet loss occurs, the RFC 2198 can ensure the service quality.

The MoIP service supports two transmission modes: the transparent transmission mode and the relay (redundancy) mode. The MA5616 supports only the modem service in the transparent transmission mode. In the transparent transmission mode, the MG uses the G.711 mode to encode and decode the modem signal, and processes the signal like processing the common RTP data. The transparent transmission mode depends on the bearer network to a great extent.

Procedure

Step 1 Configure public fax and modem parameters.

1. Run the **interface sip** command to enter the SIP interface mode.
2. Run the **fax-modem parameters negomode** command to configure the negotiation mode.
3. (Optional) Run the **fax-modem parameters packet-interval-10ms** to enable or disable the 10 ms packing function.
4. (Optional) Run the command to configure the RFC 2198 function.
5. (Optional) Run the command to configure the startup mode of the RFC 2198 function.
6. (Optional) Run the **fax-modem parameters vbd-codec** command to configure the codec mode of the voice-band data (VBD).
7. (Optional) Run the **fax-modem parameters vbd-pt-type** command to configure the payload type of the VBD.
8. (Optional) Run the **rfc2833 set rfc2833-fax-modem** command to configure the mode for reporting fax or modem events.

Step 2 Configure the transmission mode of the modem.

Run the **modem parameters tranmode** command to configure the transmission mode of the modem. Currently, only the modem service in the transparent transmission mode is supported.

Step 3 Check whether the modem parameters are the same as those in the data plan.

Run the **display fax-modem parameters** and **display modem parameters** commands to query modem parameters.

----End

Example

Assume that:

- The negotiation mode of the MA5616 is self-switch.
- The 10 ms packing function and the RFC2198 intelligent startup function are enabled.
- The RFC2198 negotiation mode is fixedstart.
- The codec mode of the VBD is G.711A.
- The payload type of the VBD is static payload.
- The transmission mode of the modem is transparent transmission (thoroughly).

To configure the MA5616, do as follows:

```
huawei(config)#interface sip 0
huawei(config-if-sip-0)#fax-modem parameters negomode self-switch vbd-codec g.711a
vbd-pt-type
 static rtp-interval 1
huawei(config-if-sip-0)#rfc2198 set rfc2198-negomode fixedstart rfc2198-startmode
smart2198
huawei(config-if-sip-0)#modem parameters transmode 0
huawei(config-if-sip-0)#display fax-modem parameters
 ---------------------------------------------------------------------------
 MGID                   :0
 Nego-mode              :self-switch
 Rtp-interval           :10ms
 Vbd-codec              :G.711A
 Vbd-pt-type            :static
 Vbd-attribute-type     :v.152
 ---------------------------------------------------------------------------

huawei(config-if-sip-0)#display modem parameters
 ---------------------------------------
 MGID      Transmode
 ---------------------------------------
 0         Thoroughly
 ---------------------------------------
```

7.8 Configuring the Security and Reliability of the Voice Service

For the MA5616, the security configuration of the voice service includes the H.248-based, or SIP-based device authentication configuration. The reliability configuration of the voice service includes the dual-homing configuration and the emergency standalone configuration.

7.8.1 Configuring the Device Authentication

The purpose of authentication is to verify the validity of users and networks. The same authentication algorithm is used on the MG and the MGC separately. Then, the calculation results on the MG and the MGC are compared on either side. If the calculation results are the same, it indicates that the authentication is successful. If the calculation results are different, it indicates that the authentication fails.

7.8.1.1 Configuring the Device Authentication (Based on the H.248 Protocol)

This topic describes how to configure the device authentication parameters of the MA5616 to prevent illegal devices from registering with the MGC when the H.248 protocol is used.

Prerequisites

- The MG interface must be added successfully on the MA5616.
- The parameters, including the encryption type, the initial key, and the DH authentication MG ID, must be configured on the MGC. These parameters must be the same as the parameters configured on the MA5616.

Precautions

When the MGC is Huawei SoftX3000, the authentication MG ID must be a string of more than eight characters.

Procedure

Step 1 In 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 MG interface to support the device authentication.

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 device authentication parameters.

Step 6 Run the **reset coldstart** command to reset the MG interface.

----End

Example

To configure the device authentication parameters shown in the **Table 7-31** for the MA5616, do as follows:

Table 7-31 Data plan for configuring the authentication parameters (H.248)

Configuration Item	Value
MGID	0
Whether to use the wildcard in registration	Yes
Whether to support the device authentication.	Yes
Authentication MG ID	MA5616 It must be the same as the configuration on the MGC. Otherwise, the MG cannot register with the MGC.
Initial key	Default: 0123456789ABCDEF. It must be the same as the initial key configured on the MGC.

```
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 uses wildcard in registration
      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 supports authentication
      0: Yes
      1: No
huawei(config-if-h248-0)#auth auth_mgid MA5616 initial_key 0123456789ABCDEF
huawei(config-if-h248-0)#display auth
 [AUTH_PARA config]
  Initial Key    : 0123456789ABCDEF
  Auth MGid      : MA5616
  Algorithm      : MD5
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

7.8.1.2 Configuring the Device Authentication (Based on the SIP Protocol)

This topic describes how to configure the authentication information for the SIP interface or a single user of the MA5616 when the SIP protocol is used.

Prerequisites

- The SIP interface must be added successfully on the MA5616.
- The authentication user name and password must be configured on the IMS. Such parameters must be the same as the authentication user name and password configured on the MA5616.

Context

- The authentication information can be configured for the SIP interface. The configuration takes effect only after you run the **reset** command on the SIP interface.
- The authentication information can be configured for a single user. The configuration takes effect immediately after the configuration is complete.
- In the actual application, whether the user uses the authentication information configured for the SIP interface or a single user can be controlled through system parameter 81 in the **sipprofile modify** command.

Procedure

- Configure the authentication information for the 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 an SIP interface.
  3. Run the **display sip-auth** command to query the authentication information of an SIP interface.
  4. Run the **reset** command to reset the SIP interface.
- Configure the authentication information for a single user.
  1. Run the **esl user** command to enter the ESL user mode.
  2. Run the **sippstnuser auth set** command to configure the authentication user name and password for a single user.

3. Run the **display sippstnuser authinfo** command to query the authentication information of a specified user.

----End

Example

- To configure the authentication information for SIP interface 0 with the user name of huawei.com and the password of 123456789, do as follows:

```
huawi(config)#interface sip 0
huawei(config-if-sip-0)#sip-auth-parameter
{ <cr>|auth-mode<K>|password-mode<K> }:password-mode
{ password-mode-value<E><password,ha1> }:password
{ <cr>|auth-mode<K> }:

  Command:
          sip-auth-parameter password-mode password
  User Name(<=64 chars, "-" indicates deletion):huawei.com
  User Password(<=64 chars, "-" indicates deletion):
  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
  The configuration will take effect after resetting the interface
```

- To configure the authentication information for a single user on port0/3/0 with the user name of user1.com and the password of 987654321, do as follows:

```
huawi(config)#esl user
huawei(config-esl-user)#sippstnuser auth set 0/3/0 telno 88442200 password-
mode
password
  User Name(<=64 chars, "-" indicates deletion):user1.com
  User Password(<=64 chars, "-" indicates deletion):
```

7.8.2 Configuring the Dual Homing

Dual-homing is a disaster recovery mechanism of emergency communication against softswitch failure or unexpected disaster (such as fire in the equipment room, disconnection of the cable connected to the equipment room, and abnormal power supply).

7.8.2.1 Configuring the Dual Homing (Based on the H.248 Protocol)

Based on the H.248 protocol, configuring the dual homing means registering one MA5616 with two MGCs. When one MGC is faulty and cannot support the communication, the MA5616 automatically switches to the other MGC.

Prerequisites

- The MGC1 and MGC2 must be configured on the attributes of the MG interface.
- On the MGCs, the data for interconnecting with the MG interface must be configured.

Context

The MA5616 supports registering the MG interface with two MGCs (MGC1 and MGC2). MGC1 functions as the active MGC and MGC2 functions as the standby MGC. When MGC1 is down, the MG automatically registers with MGC2 and works under the control of MGC2.

Procedure

Step 1 In global config mode, run the **interface h248** command to enter the MG interface mode.

Step 2 Run the **mg-software parameter 2** command to configure the MG interface to support the dual homing.

----End

Example

To configure MG interface 0 to support the dual homing, and not to automatically switch over to the active MGC when the active MGC recovers, do as follows:

```
huawei(config)#interface h248 0
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 dual-home function
      0: Do not support the dual-homing
      1: Support the dual-homing, but do not support the auto switchover
      2: Support the dual-homing and auto switchover
```

Related Operation

Table 7-32 lists the related operation for configuring the dual homing when the H.248 protocol is used.

Table 7-32 Related operation for configuring the dual homing (H.248)

To...	Run the Command...
Forcibly switch the MG to register with the other MGC	**mgc switch**

7.8.2.2 Configuring the Dual Homing (Based on the SIP Protocol)

The SIP dual-homing means that the MA5616 supports the 1+1 mutual assistance mode of the upstream P-CSCF/PROXY, namely, the deployment in the active/standby mode. When one of the upstream active/standby devices is faulty, the MA5616 service automatically switches to another device, thus implementing the disaster recovery for the access reliability of the device when the SIP protocol is used.

Prerequisites

On the IMS, the data for interconnecting with the SIP interface must be configured.

Context

The MA5616 supports configuring the SIP interface on two proxy servers (Proxy 1 and Proxy 2), where, Proxy 1 functions as the active proxy server. After Proxy 1 fails, the MG can switch to Proxy 2 to continue working.

Procedure

Step 1 In global config mode, run the **interface sip** command to enter the MG interface mode.

Step 2 Run the **if-sip attribute basic** command to configure the IP address of the active/standby proxy server of the SIP interface and other mandatory attributes, including the media IP address, signaling IP address, transfer protocol, port ID, domain name and port ID of the proxy server, homing domain name, and profile index. The dual homing is implemented through the configuration of the active/standby proxy server.

Step 3 Run the **reset** command to reset the SIP interface to validate the configuration data.

----End

Example

Assume that:

- The media IP address is 10.10.10.13, signaling IP address is 10.10.10.13, transfer protocol is UDP, and port ID is 5000.
- The obtaining mode of the IP address of the proxy server is the IP mode, IP address 1 of the active proxy server is 10.10.10.14, port ID of the active proxy server is 5060, IP address 1 of the standby proxy server is, 10.10.10.15, and the port ID of the standby proxy server is 5060.
- The profile index is 1.

To configure the dual homing of SIP interface 0, do as follows:

```
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

{ <cr>|home-domain<K>|primary-proxy-ip2<K>|proxy-addr-mode<K>|secondary-proxy-do
main<K>|secondary-proxy-ip2<K>|server-dhcp-option<K>|sipprofile-index<K>|srvlogi
c-index<K> }:

  Command:
          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
{ <cr>|media-ip<K>|primary-proxy-domain<K>|primary-proxy-ip1<K>|primary-proxy-ip
2<K>|primary-proxy-port<K>|proxy-addr-mode<K>|secondary-proxy-domain<K>|secondar
y-proxy-ip1<K>|secondary-proxy-ip2<K>|secondary-proxy-port<K>|server-dhcp-option
<K>|signal-ip<K>|signal-port<K>|srvlogic-index<K>|transfer<K> }:

  Command:
          if-sip attribute basic home-domain huawei.com sipprofile-index 1

huawei(config-if-sip-0)#reset
```

Related Operation

Table 7-33 lists the related operation for configuring the dual homing.

Table 7-33 Related operation for configuring the dual homing

To...	Run the Command...
Query the configuration of the SIP interface	**display if-sip attribute**

7.8.3 Configuring the Emergency Standalone

This topic describes how to configure the emergency standalone function on the MA5616. When the MA5616 and the MGC device fail to communicate with each other, the MA5616 independently processes the internal users connecting to the same MG interface; therefore, the internal users can make calls normally without the control of MGC.

Prerequisites

- The H.248 protocol must be used in the system.
- The media IP address must exist in the IP address pool.
- The voice users must be configured on the MG interface and the users can call each other successfully.
- If the device cannot communicate with the MG, run the **system parametres 5** command to configure the media stream forwarding mode as the mode in which the media stream is forwarded within the device.
- The phone number of the MG user is configured to be the same as the phone number on the MGC.

Context

- When the MG interface works in the emergency standalone state, only the internal users on the MG interface can communicate with each other properly.
- To keep the user phone number in the emergency standalone state consistent with the phone number in the normal condition, configure the phone number on the MG to be the same as the phone number on the MGC.

Procedure

Step 1 Run the **mg-software parameter 11 1** command to configure the MG interface to support the emergency standalone function.

Step 2 Run the **digitmap set inner** command to configure the digitmap for the internal calls.

Step 3 (Optional) Run the **standalone parameters** command to configure the parameters of the emergency standalone timers.

NOTE

In general, the default parameters of the emergency standalone timers are used, and you need not configure them.

----End

Example

To configure MG0 to support the emergency standalone function and configure the digitmap for internal calls as 8764XXXX, 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 flag
       0: None
       1: Inner
       2: Emergency
       3: Both
huawei(config-if-h248-0)#digitmap set inner 8764XXXX
huawei(config-if-h248-0)#display digitmap
  ------------------------------------------------------------------------------
  Inner digitmap                                        : 8764XXXX
  Urgent digitmap (for overload or bandwidth restrict)  : -
  Dualdial digitmap for card service                    : -
  ------------------------------------------------------------------------------
```

NOTE

The configured digitmap corresponds to the user phone number.

8 Configuration Example of Services on the MA5616 Through GPON Upstream Transmission

About This Chapter

This topic describes how to configure Internet access service, multicast service, voice service, and triple play service on the MA5616 on different networks.

8.1 Configuration Example of the xDSL Internet Access Service
This topic describes how to configure the xDSL Internet access service in the PPPoE, IPoE, PPPoA and IPoA modes.

8.2 Configuration Example of the Multicast Service (Multicast VLAN Mode)
This topic describes how to configure the multicast service on the MA5616 in multicast VLAN mode.

8.3 Configuration Example of the VoIP Service
This topic describes how to configure the VoIP service based on the H.248 or SIP protocol.

8.4 Configuration Example of the VLAN Stacking Wholesale Service
This topic describes the VLAN stacking wholesale service and how to configure the VLAN stacking wholesale service on the MA5616.

8.5 Configuring the Triple Play Service
This topic describes the triple play service and how to configure the triple play service on the MA5616 that is used on the GPON upstream transmission network.

8.1 Configuration Example of the xDSL Internet Access Service

This topic describes how to configure the xDSL Internet access service in the PPPoE, IPoE, PPPoA and IPoA modes.

8.1.1 Configuration Example of the xDSL Internet Access Service Through PPPoE Dialup

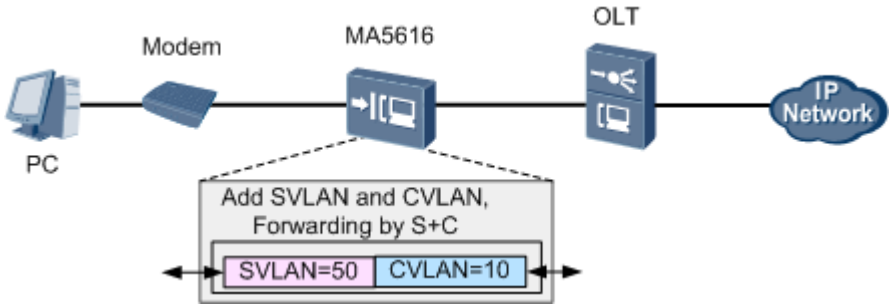
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode through the PPPoE dialup and at a rate of 2048 kbit/s, and the user packet goes upstream carrying two VLAN tags through the MA5616.

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.
- PITP is enabled to protect the user account against theft and roaming.
- A traffic profile is adopted for rate limitation. The user access rate is 2048 kbit/s.

Figure 8-1 shows an example network of the xDSL Internet access service through the PPPoA dialup.

Figure 8-1 Example network of the xDSL Internet access service through the PPPoA dialup



Prerequisite

- The number of xDSL ports is limited by the licenses. Make sure that sufficient licenses are already applied for.
- Configure the AAA function.
  - To enable the AAA function on the device, see **3.12 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

MA5616 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 service-profile profile-id 1
huawei(config-vlan-srvprof-1)#forwarding vlan-connect
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 50 profile-id 1
```

Step 2 Configure upstream ports.

Add upstream ports 0/0/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/0 0
```

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **3.7.1 Configuring the ADSL2+ Profile**. Here, 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 template-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(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
```

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 MA5616, 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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

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 MA5616, 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 0/4/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/1/0 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. Here, the **cntel** is considered as an example.

```
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 **3.10.1 Configuring Anti-Theft and Roaming of User Account Through PITP**.

Step 7 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, 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.

Configuration File

Configuration File in the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan service-profile profile-id 1
forwarding vlan-connect
commit
quit
vlan bind service-profile 50 profile-id 1
port vlan 50 0/0 0
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
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 0/0 0
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/4
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 0/0 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 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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/1/0 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
```

8.1.2 Configuration Example of the xDSL IPoE Internet Access Service

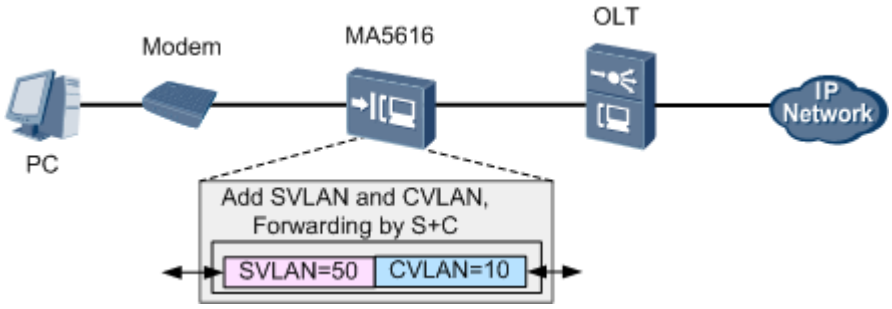
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode, and then access the Internet in the IPoE mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the IPoE mode. The account authentication is implemented through the DHCP option 82 field.
- 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.
- A traffic profile is adopted for rate limitation. The user access rate is 2048 kbit/s.

Figure 8-2 shows an example network of the xDSL IPoE Internet access service.

Figure 8-2 Example network of the xDSL IPoE Internet access service



Prerequisite

The number of xDSL ports is under the control of licenses. Make sure that sufficient licenses are already requested.

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 service-profile profile-id 1
huawei(config-vlan-srvprof-1)#forwarding vlan-connect
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 50 profile-id 1
```

Step 2 Configure upstream ports.

Add upstream ports 0/0/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/0 0
```

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **3.7.1 Configuring the ADSL2+ Profile**. Here, 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 template-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(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
   ```

   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 MA5616, 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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

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 MA5616, 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 0/4/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
```

```
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/1/0 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.

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
```

NOTE

- For the details about the security of DHCP accounts, see **3.10.2 Configuring Anti-Theft and Roaming of User Accounts Through DHCP**.

Step 7 Save the data.

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

----End

Verification

- 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.

Configuration File

Configuration File for the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan service-profile profile-id 1
forwarding vlan-connect
commit
quit
vlan bind service-profile 50 profile-id 1
port vlan 50 0/0 0
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 0/0 0
shdsl line-profile quickadd 3 ptm rate 512 2048
```

```
interface shl 0/4
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 0/0 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 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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/1/0 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
```

8.1.3 Configuration Example of the xDSL PPPoA Internet Access Service

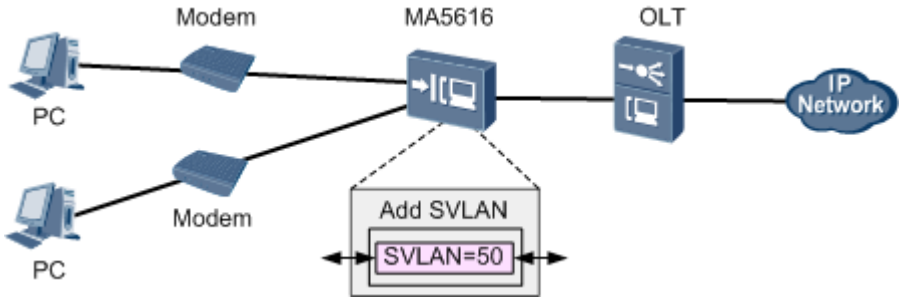
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode, and then access the Internet in the PPPoA mode at a rate of 2048 kbit/s.

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.

Figure 8-3 shows an example network of the xDSL PPPoA Internet access service.

Figure 8-3 Example network of the xDSL PPPoA Internet access service



Prerequisite

- The number of xDSL ports is under the control of licenses. Make sure that sufficient licenses are already requested.
- Configure the AAA function.
  - To enable the AAA function on the device, see **3.12 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 MA5616 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 0/0/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/0 0
```

Step 3 In the case of the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **3.7.1 Configuring the ADSL2+ Profile**. 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(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
```

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 MA5616, 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 MA5616HW/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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
   huawei(config-if-shl-0/4)#deactivate 0
   huawei(config-if-shl-0/4)#activate 0 3
   huawei(config-if-shl-0/4)#alarm-config 0 1
   huawei(config-if-shl-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(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
   ```

   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 MA5616, 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 0/4/0, 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 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 2 description MA5616HW/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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0, 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 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5616HW/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 0/4/0 vpi 1 vci 39 type pppoa llc
huawei(config)#encapsulation 0/1/0 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. Here, the **cntel** is considered as an example.

```
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 **3.10.1 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 0/0 0
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 MA5616HW/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 0/0 0
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/4
deactivate 0
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5616HW/Vlanid:50/shdsl/smart
mac-address max-mac-count service-port 2 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
```

```
encapsulation 0/4/0 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 0/0 0
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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5616HW/Vlanid:50/vdsl/smart
mac-address max-mac-count service-port 3 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/1/0 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

8.1.4 Configuration Example of the xDSL IPoA Internet Access Service

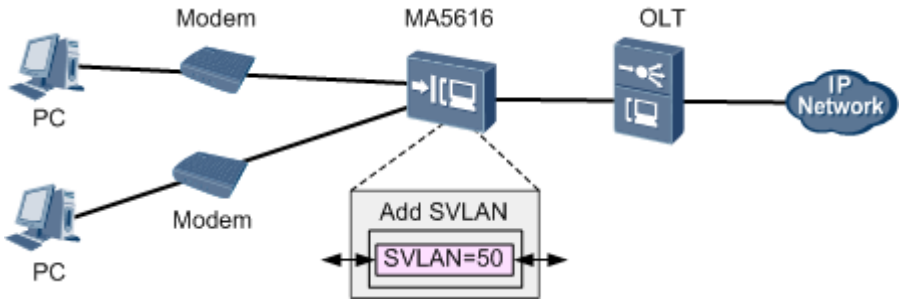
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode, and then access the Internet in the IPoA mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the IPoA mode. The MA5616 works in the L2 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.
- The user access rate is 2048 kbit/s, which is restricted by the traffic profile.

Figure 8-4 shows an example network of the xDSL IPoA Internet access service.

Figure 8-4 Example network of the xDSL IPoA Internet access service



Prerequisite

The number of xDSL ports is under the control of licenses. Make sure that sufficient licenses are already requested.

Procedure

Step 1 Create a VLAN.

Create smart VLAN 50.

```
huawei(config)#vlan 50 smart
```

Step 2 Configure upstream ports.

Add upstream ports 0/0/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/0 0
```

Step 3 In the case of the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **3.7.1 Configuring the ADSL2+ Profile**. 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(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
```

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 MA5616, 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 MA5616HW/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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

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 MA5616, 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 0/4/0, 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 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 2 description MA5616HW/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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

   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 MA5616, 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 0/1/0, 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 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5616HW/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.

NOTE

Run the **encapsulation** command to configure the target IP address for IPoA encapsulation. If you do not configure the target IP address, the IP address of the default gateway of the IPoA encapsulation is used. This example uses the IP address of the default gateway of the IPoA encapsulation as the user target IP address.

```
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 0/4/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
huawei(config)#encapsulation 0/1/0 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 0/0 0
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 MA5616HW/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 0/0 0
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/4
deactivate 0
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5616HW/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 0/4/0 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 0/0 0
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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5616HW/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 0/1/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

8.2 Configuration Example of the Multicast Service (Multicast VLAN Mode)

This topic describes how to configure the multicast service on the MA5616 in multicast VLAN mode.

8.2.1 Configuration Example of the Multicast Video Service (Static Configuration Mode)

This topic describes how to configure the multicast video service if the program in the multicast VLAN is configured statically.

Prerequisites

- Network devices and lines must be in the normal state.
- The multicast source must exist on the network and the IP address of the multicast source must be known.

Context

The program in the multicast VLAN can be configured statically or generated dynamically.

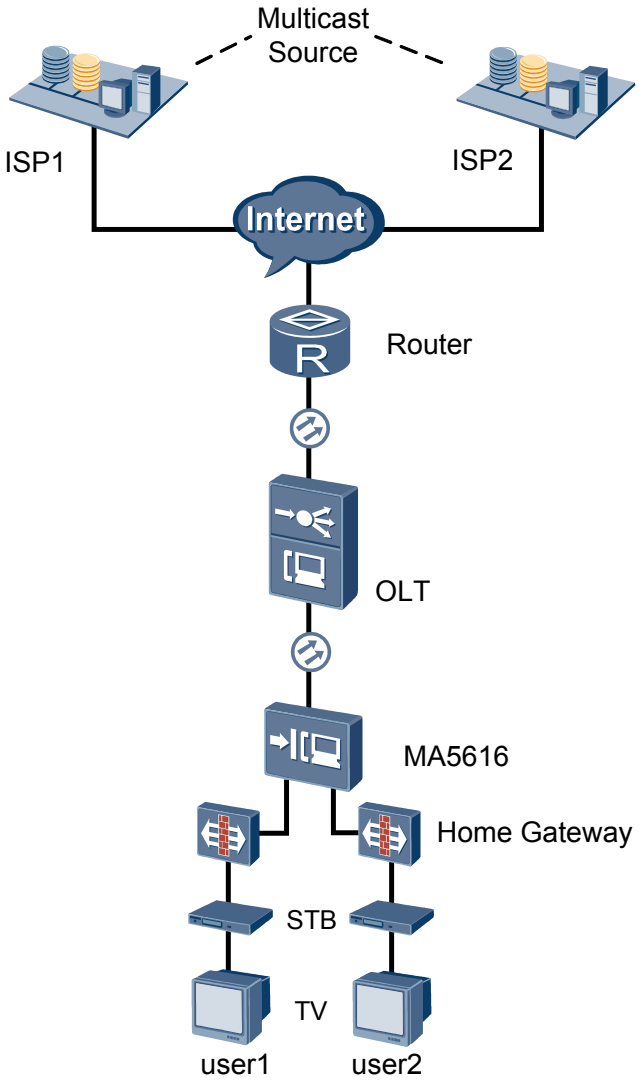
For the static configuration mode:

- The program list needs to be configured for the multicast VLAN. Then, the user can request for the program in this program list.
- The following functions are supported: bandwidth management of the multicast program, user bandwidth management, program preview, and program prejoin.
- The program in the multicast VLAN is configured statically by default.

Networking

Figure 8-5 shows the example network of the multicast service.

Figure 8-5 Example network of the multicast service



Data Plan

Table 8-1 provides the data plan for configuring the multicast service.

Table 8-1 Data plan for configuring the multicast service

Device	Item	Data
ONU: MA5616	Smart VLAN	● VLAN type: Smart VLAN ● VLAN ID: 4002-4003
	Uplink port	0/0/1
	IGMP version	IGMP V3 (default multicast version of the system in multicast VLAN mode)

Device	Item	Data
	Multicast source	There are two multicast sources, namely, ISP 1 and ISP 2. ● ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ● ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
	Program library	Program in multicast VLAN 4002: Program 1: with IP address 224.1.1.1 and the IP address of the program source is the same as the IP address of ISP 1, namely, 10.10.10.10
		Program in multicast VLAN 4003: Program 2: with IP address 224.1.1.2 and the IP address of the program source is the same as the IP address of ISP 2, namely, 10.10.10.11
	Multicast user	Multicast user 1: ● VDSL2 port: 0/1/0 ● Multicast VLAN: 4002
		Multicast user 2: ● VDSL2 port: 0/1/1 ● Multicast VLAN: 4003

Procedure

Step 1 Create VLANs and add an uplink port to the VLANs.

```
huawei(config)#vlan 4002-4003 smart
huawei(config)#port vlan 4002-4003 0/0 1
```

Step 2 Configure service ports.

```
huawei(config)#service-port 100 vlan 4002 vdsl mode ptm 0/1/0 multi-service user-vlan untagged
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 101 vlan 4003 vdsl mode ptm 0/1/1 multi-service user-vlan untagged
rx-cttr 6 tx-cttr 6
```

Step 3 Configure multicast VLANs and the IGMP mode.

NOTE

The IGMP mode can be configured to IGMP proxy or IGMP snooping according to the requirements. In this example, the IGMP mode is IGMP proxy. If the planned IGMP mode is IGMP snooping, you can configure the IGMP snooping mode by running the **igmp mode snooping** command in multicast VLAN mode.

The IGMP mode can be switched only when the IGMP mode is off.

```
huawei(config)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4002)#multicast-vlan 4003
```

```
huawei(config-mvlan4003)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

Step 4 Configure the multicast uplink port.

```
huawei(config-mvlan4003)#igmp uplink-port 0/0/1
huawei(config-mvlan4003)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp uplink-port 0/0/1
```

Step 5 Configure multicast programs.

NOTE

- In static configuration mode, you can run the **igmp program add** command to add multicast programs. You cannot name a program, instead the system automatically names a program PROGRAM-M, in which M is the index of the added program.
- If the IGMP version of the multicast VLAN is V3, the source IP address of the program in the multicast VLAN must be configured. If the IGMP version of the multicast VLAN is V2, the source IP address of the program in the multicast VLAN cannot be configured.

```
huawei(config-mvlan4002)#igmp program add name program1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp program add name program2 ip 224.1.1.2 sourceip
10.10.10.11
```

Step 6 Configure multicast users.

```
huawei(config-mvlan4003)#btv
huawei(config-btv)#igmp user add service-port 100
huawei(config-btv)#igmp user add service-port 101
huawei(config-btv)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4003)#quit
```

Step 7 Save the data.

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

----End

Result

- User 1 belongs to multicast VLAN 4002 and user 1 can watch the program with IP address 224.1.1.1 provided by ISP1.
- User 2 belongs to multicast VLAN 4003 and user 2 can watch the program with IP address 224.1.1.2 provided by ISP2.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps need to be performed manually and the configuration file cannot be imported directly.

Create VLANs and add an uplink port to the VLANs. This step needs to be performed manually.

```
vlan 4002 to 4003 smart
port vlan 4002 to 4003 0/0 1
```

Create service ports.

```
service-port 100 vlan 4002 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-
cttr 6 tx-cttr 6
service-port 101 vlan 4003 vdsl mode ptm 0/1/1 multi-service user-vlan untagged rx-
cttr 6 tx-cttr 6
```

Configure multicast VLANs and the IGMP mode. This step needs to be performed manually.

```
multicast-vlan 4002
igmp mode proxy
multicast-vlan 4003
igmp mode proxy
```

Configure the multicast uplink port, multicast programs, and multicast users.

```
igmp uplink-port 0/0/1
multicast-vlan 4002
igmp uplink-port 0/0/1
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
multicast-vlan 4003
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp user add service-port 100
igmp user add service-port 101
multicast-vlan 4002
igmp multicast-vlan member service-port 100
multicast-vlan 4003
igmp multicast-vlan member service-port 101
quit
save
```

8.2.2 Configuration Example of the Multicast Video Service (Dynamic Generation Mode)

This topic describes how to configure the multicast video service if the program matching mode of the multicast VLAN is the dynamic generation mode.

Prerequisites

- Network devices and lines must be in the normal state.
- The multicast source must exist on the network and the IP address range of the multicast program must be known.
- The multicast program must be configured in dynamic generation mode.

Context

The program in the multicast VLAN can be configured statically or generated dynamically.

Dynamic generation mode: A program is dynamically generated according to the program requested by the user.

- In this mode, the program list is not required. You need to configure the IP address range of the program group that can be dynamically generated. The user can request for only the program whose IP address is within this IP address range.
- The following functions are not supported: bandwidth management of the multicast program, user bandwidth management, program preview, and program prejoin.

The program in the multicast VLAN is configured statically by default. Run the **igmp match mode disable** command to configure the dynamic generation mode.

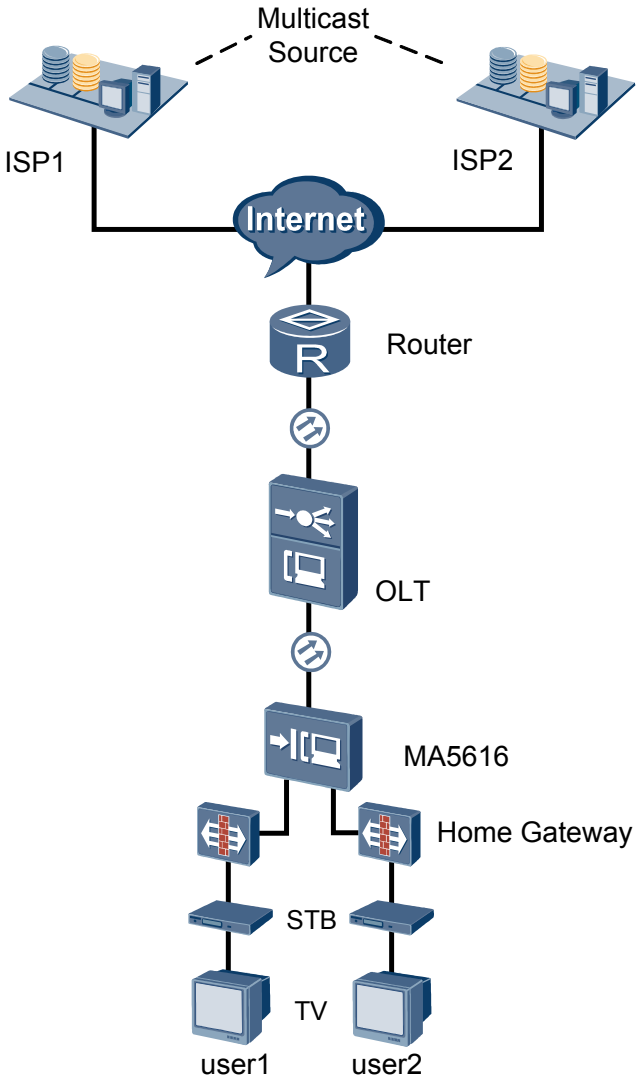
NOTE

The **igmp match mode** command for configuring the mode of the multicast program can be executed only when the IGMP mode is off.

Networking

Figure 8-6 shows the example network of the multicast service.

Figure 8-6 Example network of the multicast service



Data Plan

Table 8-2 provides the data plan for configuring the multicast service.

Table 8-2 Data plan for configuring the multicast service

Device	Item	Data
ONU: MA5616	Smart VLAN	● VLAN type: Smart VLAN ● VLAN ID: 4002-4005
	Uplink port	0/0/1
	IGMP version	IGMP V3 (default multicast version of the system in multicast VLAN mode)

Device	Item	Data
	Multicast source	There are two multicast sources, namely, ISP 1 and ISP 2. ● ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ● ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
	Program library	Program in multicast VLAN 4002: Program 1: with IP address 224.1.1.1 and the IP address of the program source is the same as the IP address of ISP 1, namely, 10.10.10.10
		Program in multicast VLAN 4003: Program 2: with IP address 224.1.1.2 and the IP address of the program source is the same as the IP address of ISP 2, namely, 10.10.10.11
	Multicast user	Multicast user 1: ● VDSL2 port: 0/1/0 ● Multicast VLAN: 4002
		Multicast user 2: ● VDSL2 port: 0/1/1 ● Multicast VLAN: 4003

Procedure

Step 1 Create VLANs and add an uplink port to the VLANs.

```
huawei(config)#vlan 4002-4005 smart
huawei(config)#port vlan 4002-4005 0/0 1
```

Step 2 Configure service ports.

```
huawei(config)#service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-vlan untagged
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-vlan untagged
rx-cttr 6 tx-cttr 6
```

Step 3 Configure multicast VLANs and the multicast mode.

NOTE

The IGMP mode can be configured to IGMP proxy or IGMP snooping according to the requirements. In this example, the IGMP mode is IGMP proxy. If the planned IGMP mode is IGMP snooping, you can configure the IGMP snooping mode by running the **igmp mode snooping** command in multicast VLAN mode.

The IGMP mode can be switched only when the IGMP mode is off.

```
huawei(config)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp match mode disable
huawei(config-mvlan4002)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp match mode disable
```

```
huawei(config-mvlan4003)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

Step 4 Configure the multicast uplink port.

```
huawei(config-mvlan4003)#igmp uplink-port 0/0/1
huawei(config-mvlan4003)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp uplink-port 0/0/1
```

Step 5 Configure multicast programs.

Configure the program in the multicast VLAN in dynamic generation mode, and specify the IP address range of the program that can be requested by the user to 224.1.1.1-224.1.1.2.

NOTE

The execution of the **igmp match mode** command for configuring the mode of the multicast program will cause the user to go offline. Therefore, plan the multicast program mode before configuring the multicast program. This command can be executed only when the IGMP function is disabled.

```
huawei(config-mvlan4002)#igmp match group ip 224.1.1.1 to-ip 224.1.1.2
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp match group ip 224.1.1.1 to-ip 224.1.1.2
```

Step 6 Configure multicast users.

```
huawei(config-mvlan4002)#btv
huawei(config-btv)#igmp user add service-port 100
huawei(config-btv)#igmp user add service-port 101
huawei(config-btv)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4003)#quit
```

Step 7 Save the data.

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

----End

Result

- User 1 belongs to multicast VLAN 4002 and user 1 can watch the program with IP address 224.1.1.1 provided by ISP1.
- User 2 belongs to multicast VLAN 4003 and user 2 can watch the program with IP address 224.1.1.2 provided by ISP2.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps need to be performed manually and the configuration file cannot be imported directly.

Create VLANs and add an uplink port to the VLANs. This step needs to be performed manually.

```
vlan 4002 to 4005 smart
port vlan 4002 to 4005 0/0 1
```

Create service ports.

```
service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
```

Configure multicast VLANs and the IGMP mode. This step needs to be performed manually.

```
multicast-vlan 4002
igmp match mode disable
igmp mode proxy
multicast-vlan 4003
igmp match mode disable
igmp mode proxy
```

Configure the multicast uplink port, multicast programs, and multicast users.

```
igmp uplink-port 0/0/1
multicast-vlan 4002
igmp uplink-port 0/0/1
igmp match group ip 224.1.1.1 to-ip 224.1.1.2
multicast-vlan 4003
igmp match group ip 224.1.1.1 to-ip 224.1.1.2
btv
igmp user add service-port 100
igmp user add service-port 101
multicast-vlan 4002
igmp multicast-vlan member service-port 100
multicast-vlan 4003
igmp multicast-vlan member service-port 101
quit
save
```

8.3 Configuration Example of the VoIP Service

This topic describes how to configure the VoIP service based on the H.248 or SIP protocol.

8.3.1 Configuration Example of the VoIP PSTN Service (Based on the H.248 Protocol)

This topic describes how to configure the VoIP service based on the H.248 protocol.

Service Requirements

In an office, the MA5616 that adopts the H.248 protocol is newly deployed. Data plan and configuration, however, are not performed on the MGC (softswitch) connected to the MA5616. The following voice services are required:

- POTS service needs to be provided for phone 0-phone 31 for 32 users.
- Polarity reversal charging is adopted.

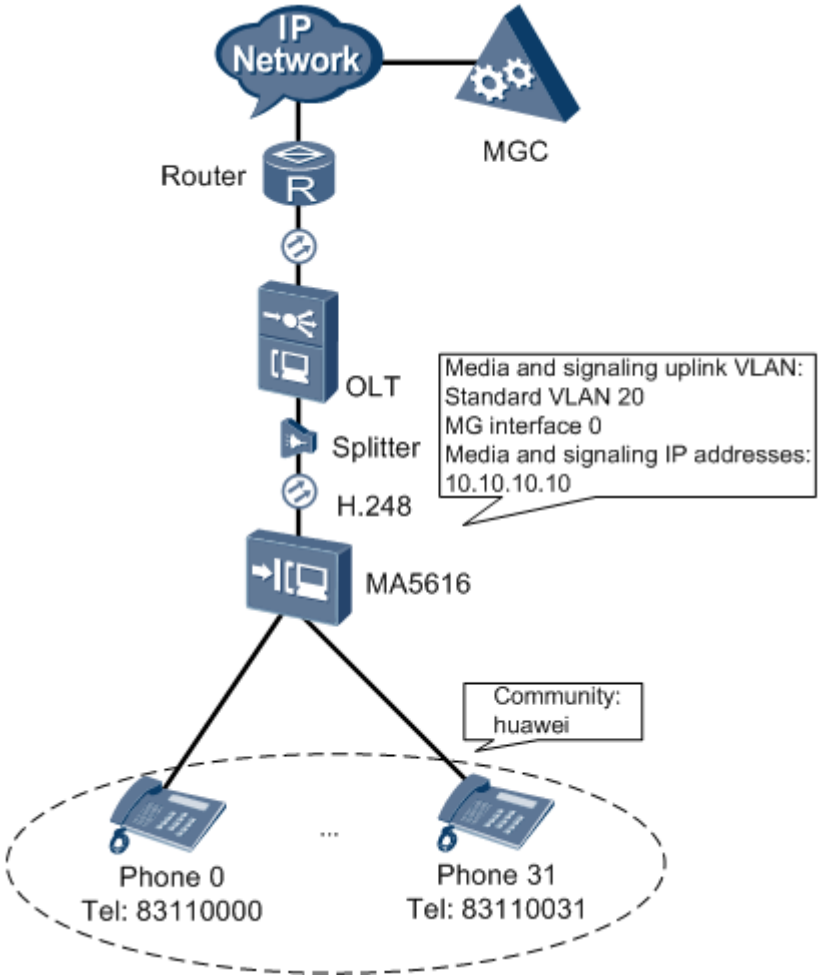
Prerequisite

- According to the actual network, a route from the MA5616 to the MGC must be configured to ensure that the MA5616 and the MGC are reachable to each other.
- POTS service board ASRB must be inserted into the planned slot, and the RUN ALM indicator on the board must be green and must be on for 1s and off for 1s repeatedly.

Networking

Figure 8-7 shows the example network of the VoIP service based on the H.248 protocol.

Figure 8-7 Example network of the VoIP service based on the H.248 protocol



Data Plan

After the service requirements are further confirmed and analyzed with engineers of the office, the data plan is made by considering the interconnection with the MGC and according to the data plan described in **7.1 Configuring the VoIP PSTN Service (Based on the H.248 Protocol)**. **Table 8-3** provides the data plan for configuring the VoIP service based on the H.248 protocol.

Table 8-3 Data plan for configuring the VoIP service based on the H.248 protocol

Item			Data
MG interface data (The data configuration must be consistent with the data	Parameters of the media stream and signaling stream	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the voice service. In this section, standard VLAN 20 is adopted.

Item			Data
configuration on the MGC.)		Media and signaling upstream port	0/0/1
		Media IP address and signaling IP address	These two IP addresses are both 10.10.10.10.
		Default IP address of the MG	Confirmed with the engineers of this office, the IP address of the next hop from the MA5616 to the MGC is 10.10.10.1.
	Attribute parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be started if these parameters are not configured.	MG interface ID	0, indicating that the negotiation is based on the profile
		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 network of the office does not support dual homing. 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 MA5616.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	The **text** coding mode is adopted.
		Transmission mode of the MG interface	UDP
		Domain name of the MG interface	The message ID (MID) adopts the IP address (default), and may not be configured with a domain name.
		Device name of the MG interface	The MID adopts the IP address (default), and may not be configured with a device name.
		Start negotiation version of the H.248 protocol for the MG interface	0
	Digitmap of an MG Interface		Special applications such as emergency calls and emergency standalone are not configured. Therefore, the digitmap is not configured.

Item			Data
	Software Parameters of an MG Interface		According to the Context in **Software Parameters of an MG Interface** and confirmed with the engineers of the office, the default configuration can meet the service requirements. Therefore, the software parameters are not configured.
	Ringing Mode of an MG Interface		Confirmed with the engineers of the office, the value of the ringing parameter (corresponding to the users) specified 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.
	TID Format of an MG Interface		To differentiate users by terminal ID (TID), the engineers of the office require that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the slot ID/shelf 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.
Voice service data (The data configuration must be consistent with the data configuration on the MGC.)	Slot that houses the voice service board		The user is accessed through the 0/3 port on the ASRB board.
	User Data	Phone number	The emergency standalone is not supported. Therefore, you need not configure the phone number when adding a user. Phone numbers allocated by the MGC for phone 0-phone 31 are 83110000-83110031. **NOTE** Generally, No telephone number (namely, parameter telno) is configured on the MG, because telephone numbers are specified by the MGC.
		TID	The terminal layering is supported. Therefore, the TID need not be allocated manually.

Item			Data
		User priority	Users are common users, and the user priority uses the default priority, namely, cat3.
		User type	Users are common users, and the user type uses the default user type, namely, DEL.
	System Parameters		According to the Context in **7.1.2.2 (Optional) Configuring the System Parameters** and confirmed with the engineers of the office, the default configuration can meet the service requirements. Therefore, the system parameters are not configured.
	Overseas Parameters		According to the Context in **7.1.2.3 (Optional) Configuring the Overseas Parameters** and confirmed with the engineers of the office, the default configuration can meet the service requirements. Therefore, the overseas parameters are not configured.
	Local Digitmap **CAUTION** By default, these parameters need not be configured if the H.248 protocol is used. You can configure these parameters according to the requirements.	Digitmap name	huawei
		Digitmap type	Only the normal digitmap is supported if the H.248 protocol is used.
		Digitmap body	Plan this parameter according to the prefix of the local phone number. In this example, the ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx) digitmap body is used.
	Attributes of a PSTN Port		The polarity reversal charging is required for the service. Therefore, you need to configure the PSTN port to which the user belongs so that the PSTN port supports the polarity reversal impulse. The other attributes of the PSTN port need not be modified.

Item		Data
	Attributes of the Ringing Current	The ringing attribute need not be configured unless otherwise specified.

Procedure

Step 1 Configure the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/0/1 to the VLAN, and configure the IP address of the L3 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 0/0 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
```

Step 2 Configure the media and signaling IP address pools.

Add the IP address of the VLAN L3 interface configured in the previous step to the media and signaling IP address pools respectively. Thus, 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-if-vlanif20)#quit
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
```

Step 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-voip)#quit
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
start-negotiate-version 0
```

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 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 template of the PSTN user on MG interface 0.

Configure the TID generation mode. According to the data plan, the terminal prefix of the PSTN user needs to be configured to **huawei**, and the TID template adopts layering template 6.

CAUTION

The MA5616 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 Start 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 manners (see Parameter Description of the **reset** command). For a newly configured MG interface, start the MG interface in a cold start manner.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

Step 7 Query the running status of the MG interface.

After the MG interface is interconnected with the MGC successfully, the MG interface needs to be in the normal state, indicating that the MG interface works in the normal state.

```
huawei(config-if-h248-0)#quit
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
  ------------------------------------------------------------------------------
```

Step 8 Configure the PSTN user data.

Add POTS users phone 0-phone 31 so that the users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0
```

Step 9 Configure the local digitmap.

After the configuration, the MA5616 matches the phone number according to the local digitmap if the MGC does not send the detailed digitmap to the MA5616.

```
huawei(config-esl-user)#quit
huawei(config)#local-digitmap add huawei normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|
13xxxxxxxxx|0xxxxxxxxx)
```

Step 10 Configure the polarity reversal charging function.

Configure the physical attributes of the PSTN port to which the user belongs to support the polarity reversal pulse, so that the user can support the polarity reversal charging.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
```

Step 11 Save the data.

```
huawei(config-pstnport)#quit
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 service can be provided normally. In normal cases, phone 0-phone 31 can call each other.

- The calling party can hear the dial tone after picking up the phone off the hook.
- 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 ringback tone.

  NOTE

  When the calling party calls the number of a specified user, if the phone of the specified user does not ring but the phone of another user connected to the MA562X rings, and the calling party hears the ringback tone, check whether the MGC is configured with the call forwarding service, causing the line cross.

  - If the MGC is configured with the call forwarding service, cancel the call forwarding service on the MGC.
  - If the MGC is not configured with the call forwarding service, contact Huawei technical support engineer to handle the fault.
- The calling party and the called party can communicate with each other normally.
- After the called party places the phone on the hook, the calling party can hear the busy tone.

Configuration File

The following part 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 0/0 0
interface vlanif 20
ip address 10.10.10.10 24
```

Configure the media and signaling IP address pools.

```
quit
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
```

Add an MG interface and then configure the attributes of the MG interface. An MG interface must be added manually and the configuration file cannot be imported directly.

```
quit
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 start-negotiate-version 0
```

Configure the ringing mapping of the MG interface.

```
mg-ringmode add 0 0 4
```

Configure the TID template of the PSTN user on the MG interface.

```
tid-format pstn prefix huawei template 6
```

An MG interface must be started manually and the configuration file cannot be imported directly.

```
reset coldstart
```

Query the running status of the MG interface.

```
quit
display if-h248 all
```

Configure the PSTN user data.

```
esl user
mgpstnuser batadd 0/3/0 0/3/31 0
```

Configure the local digitmap.

```
quit
local-digitmap add huawei normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|
0xxxxxxxxx)
```

Configure the polarity reversal charging function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse enable
```

Save the data.

```
quit
save
```

8.3.2 Configuration Example of the VoIP PSTN Service (Based on the SIP Protocol)

This topic describes how to configure the VoIP PSTN service based on the SIP protocol.

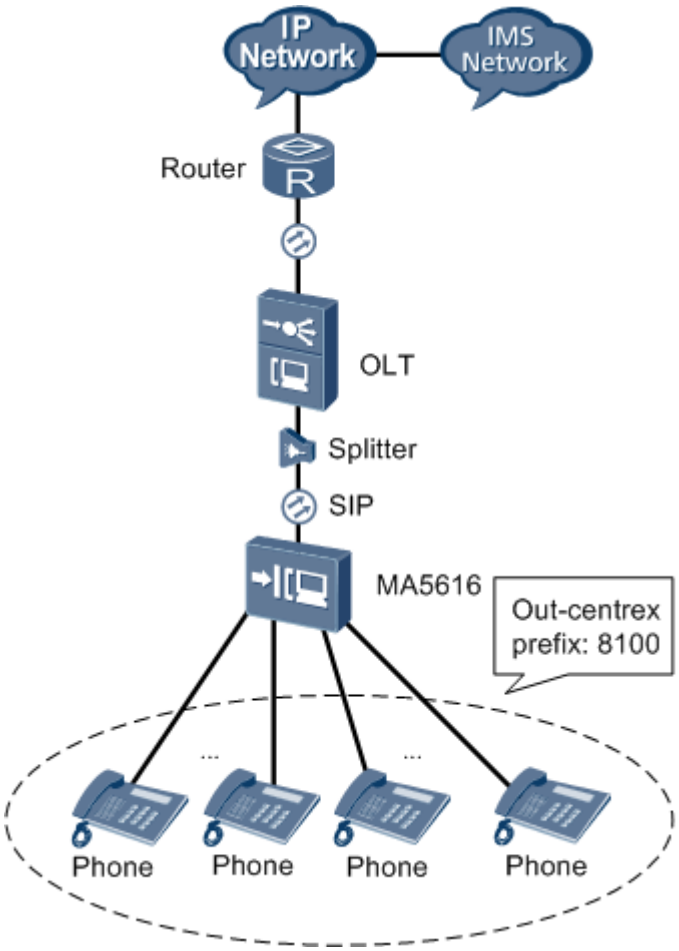
Prerequisites

- The voice service board ASRB must be installed in the specified slot.
- The SIP interface must be configured. For how to configure the SIP interface, see **7.2.1 Configuring the SIP Interface**.
- The PSTN user data corresponding to the SIP interface must be configured on the IMS.

Networking

Figure 8-8 shows the example network of the VoIP PSTN service based on the SIP protocol.

Figure 8-8 Example network of the VoIP PSTN service based on the SIP protocol



Data Plan

Run the **display system parameters** and **display oversea parameters** commands to query the system parameters and overseas parameters. If the parameter settings do meet the requirements, run the **system parameters** and **oversea parameters** commands to set the parameters to the required values.

In this example, the MA5616 is used in China. The default configurations of system parameters and overseas parameters can meet the standard and application requirements. Therefore, you need not configure these parameters.

Table 8-4 provides the data plan for configuring the VoIP PSTN service based on the SIP protocol.

Table 8-4 Data plan for configuring the VoIP PSTN service based on the SIP protocol

Item		Data
SIP interface	SIP interface ID	0
Local digitmap	Digitmap name	huawei0 and huawei1

Item		Data
	Digitmap type	The digitmap type of huawei0 is normal. The digitmap type of huawei1 is second-centrex. **NOTE** The parameters of the emergency digitmap use default values.
	Digitmap body	The digitmap body of huawei0 is ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S). The digitmap body of huawei1 is (8100).
Voice service board ASRB	Slot that houses the board	0/3
Data of the PSTN users in slot 0/3	Numbers of phone 0-phone 31	83110000-83110031
	User priority	The priority of phone 0 is Cat2 and the priority of phone 1-phone 31 is Cat3 (default priority).
	User type	The type of phone 0 is DEL and the type of phone 1-phone 31 is Payphone.
	PSTN port attribute	Phone 1-phone 31 support polarity reversal impulse.

Procedure

Step 1 Configure the local digitmap.

Configure the local call digitmap and two-stage dialing digitmap. The parameters of the emergency digitmap use the default values.

```
huawei(config)#local-digitmap add huawei0 normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|
13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)
huawei(config)#local-digitmap add huawei1 second-centrex (8100)
```

Step 2 Configure the PSTN user data.

1. Configure the data of the PSTN users (phone 0-phone 31) in slot 0/3.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/31 0 telno 83110000
   ```

2. Configure the priority of the PSTN user in slot 0/3/0 to Cat2.

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

3. Configure the type of the PSTN user in slot 0/3.

   ```
   huawei(config-esl-user)#sippstnuser attribute batset 0/3/1 0/3/31 potslinetype
   PayPhone
   ```

Step 3 Configure the PSTN port attribute.

Configure the PSTN port in slot 0/3 so that the port supports polarity reversal impulse.

```
huawei(config-esl-user)#quit
huawei(config)#pstnport
```

```
huawei(config-pstnport)#pstnport attribute batset 0/3/1 0/3/31 reverse-pole-pulse
enable
```

Step 4 Save the data.

```
huawei(config-pstnport)#quit
huawei(config)#save
```

----End

Result

After the configuration, phone 0-phone 31 can call each other.

- The calling party can hear the dial tone after picking up the phone off the hook.
- 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 ringback tone.

  NOTE

  When the calling party calls the number of a specified user, if the phone of the specified user does not ring but the phone of another user connected to the MA5616 rings, and the calling party hears the ringback tone, check whether the IMS is configured with the call forwarding service, causing the line cross.

  - If the IMS is configured with the call forwarding service, cancel the call forwarding service on the IMS.
  - If the IMS is not configured with the call forwarding service, contact Huawei technical support engineer to handle the fault.
- The calling party and the called party can communicate with each other normally.
- After the called party places the phone on the hook, the calling party can hear the busy tone.

Configuration File

The following part 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 local digitmap.

```
local-digitmap add huawei0 normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|
13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)
local-digitmap add huawei1 second-centrex (8100)
```

Configure the PSTN user data.

```
esl user
sippstnuser batadd 0/3/0 0/3/31 0 telno 83110000
sippstnuser attribute set 0/3/0 priority cat2
sippstnuser attribute batset 0/3/1 0/3/31 potslinetype PayPhone
```

Configure the PSTN port attribute.

```
quit
pstnport
pstnport attribute batset 0/3/1 0/3/31 reverse-pole-pulse enable
```

Save the data.

```
quit
save
```

8.3.3 Configuration Example of the VoIP ISDN BRA Service

When the H.248 protocol is used, the MA5616 can access the ISDN BRA service through the DSLD service board. Then, the service is sent upstream to the IP network through the control

board, implementing the ISDN BRA service. The ISDN BRA service on the MA5616 can be supported only by the H.248 protocol.

Prerequisites

- The devices on the network must be connected properly and must work in the normal state.
- The MA5616 must use the H.248 protocol to communicate with the MGC.
- The data on the MGC side must be configured correctly.
- NT1 must be connected properly and must work in the normal state.

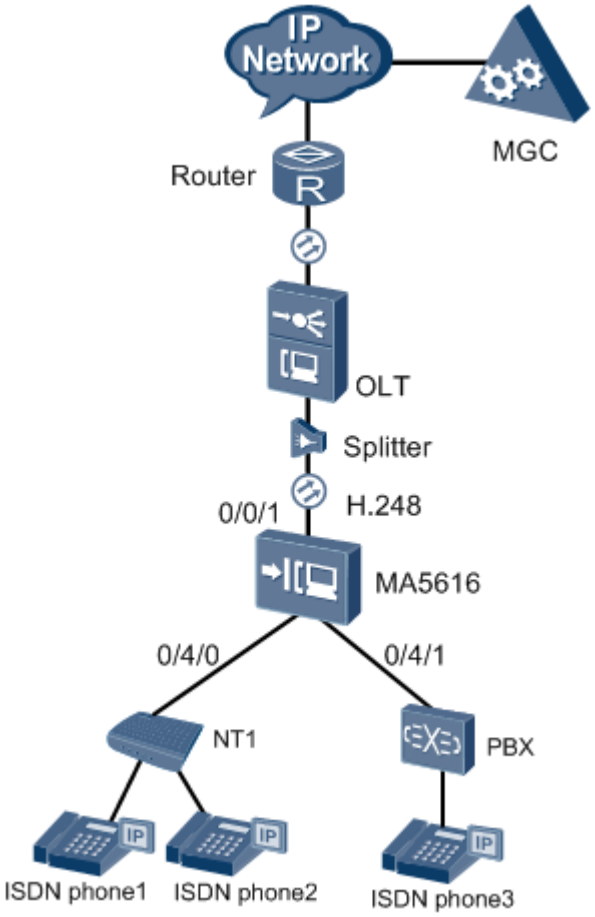
Context

- When the MG interface does not support the terminal layering, the terminal ID must be configured and must be different from the terminal ID of an existing PSTN user.
- When the MG interface supports terminal layering, the terminal ID cannot be configured, and the system automatically allocates the terminal ID according to the TID profile configured for the interface of the PSTN user.
- You can run the **display tid-format** to query the TID profile to which various users under the MG interface are bound, and then run the **display tid-template** command to check whether the TID profile supports the layering configuration. Hence, you can check whether the user supports terminal layering.
  - If the parameter list of the TID profile includes only keyword "G", it indicates that the TID profile is used by the non-layering users. Users bound with this profile do not support terminal layering.
  - If the parameter list of the TID profile includes only keywords "F", "S", "P", "B" ("B" is unavailable for PSTN users), it indicates that the TID profile is used by the layering users. Users bound with this profile support terminal layering.

Networking

Figure 8-9 shows the example network for configuring the ISDN BRA service.

Figure 8-9 Example network for configuring the ISDN BRA service



Data Plan

Table 8-5 provides the data plan for configuring the ISDN BRA service.

Table 8-5 Data plan for configuring the ISDN BRA service

Item		Data
Parameters of the media stream and signaling stream	IP address and mask of the VLAN L3 interface	10.13.4.116/16
	IP address of the media stream and signaling stream	10.13.4.116
	Upstream interface of the media stream and signaling stream	0/0/1
	Upstream VLAN of the media stream and signaling stream	VLAN ID: 10

Item		Data
	Default media gateway of the MG interface	10.13.1.1
TID profile	ID of the TID profile used by the ISDN BRA user	2 (default, no configuration is required)
	TID terminal prefix used by the ISDN BRA user	A (default, no configuration is required)
Static route from the MG to the MGC	IP address of the destination network segment	10.14.0.0
	IP address of the gateway	10.13.1.1
Attribute parameters of the MG interface	MG interface ID	0
	Coding type of the MG interface	text
	Protocol supported by the MG interface	H.248
	Signaling port ID of the MG interface	2944
	Media/Signaling IP address of the MG interface	10.13.4.116
	Default media gateway of the MG interface	10.13.1.1
	IP address of the primary MGC to which the MG interface belongs	10.14.1.2
	Port ID of the primary MGC to which the MG interface belongs	2944
	Transmission mode of the MG interface	UDP
	Start negotiation version of the H.248 protocol for the MG interface	2
	Domain name	MA5616.com
Voice service board DSLD	Slot that houses the board	0/4
IUA link parameters	ID of the IUA link set	0
	IUA link ID	0

Item		Data
	Local port ID	1401
	Local IP address	10.13.4.116/16
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
BRA user data	ISDN phone1 and ISDN phone2	● Shelf/slot/port ID of the BRA user: 0/4/0 ● Phone number: 83110001 ● Working mode: point to multi-point ● Terminal ID: 2 ● IUA interface ID: 0 ● Priority of the user: Cat3 (default)
	ISDN phone3	● Shelf/slot/port ID of the BRA user: 0/4/1 ● Phone number: 83110002 ● Working mode: point to point ● Terminal ID: 4 ● IUA interface ID: 2 ● Priority of the user: Cat1 **NOTE** In the point to point mode, the terminal endpoint identifier (TEI) of the ISDN BRA digital phone is always 0.

Procedure

Step 1 Add a DSLD service board.

```
huawei(config)#board add 0/4 H832DSLD
  0 frame 4 slot board added successfully
```

Step 2 Create a VLAN and configure the VLAN L3 interface.

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.13.4.116 16
huawei(config-if-vlanif10)#quit
```

Step 3 Add the uplink port to the VLAN.

```
huawei(config)#port vlan 10 0/0 1
```

Step 4 Configure the media/signaling IP address.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.13.4.116 10.13.1.1
huawei(config-voip)#ip address signaling 10.13.4.116
```

NOTE

Ensure that the to-be-configured media/signaling IP address of the MG interface must exist in the corresponding address pool. You can run the **display ip address** command to query the information about the media IP address pool or the signaling IP address pool.

Step 5 Configure the static route.

```
huawei(config-voip)#quit
huawei(config)#ip route-static 10.14.0.0 16 10.13.1.1
```

Step 6 Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 7 Configure the attributes of the MG interface.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.13.4.116 mgport 2944 code
text transfer udp MIDType domainName domainName MA5616.com primary-mgc-ip1
 10.14.1.2 primary-mgc-port 2944 mg-media-ip1 10.13.4.116 start-negotiate-version 2
```

Step 8 Reset the MG interface.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

Step 9 Configure the working mode of the ISDN BRA port.

```
huawei(config-if-h248-0)#quit
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/4/0 workmode p2mp
huawei(config-braport)#braport attribute set 0/4/1 activemode stable-active
workmode p2p
```

NOTE

In the point to point mode, the L1 **activemode** of the ISDN BRA port must be set to **stable-active** to make the configuration take effect.

Step 10 Add an IUA link set and IUA links.

```
huawei(config-braport)#quit
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 0
huawei(config-sigtran)#iua-link add 0 0 1401 10.13.4.116 1400 10.14.1.2
```

Step 11 Add an ISDN BRA user and configure the data.

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/4/0 0 0 interfaceid 0 terminalid 2 priority
cat3 telno 83110001
 Are you sure to configure the working mode of the DSL board to normal and reset
 the board automatically? (y/n)
[n]:y
huawei(config-esl-user)#mgbrauser add 0/4/1 0 0 interfaceid 2 terminalid 4 pr
iority cat1 telno 83110002
```

Step 12 Save the data.

```
huawei(config-esl-user)#quit
huawei(config)#save
```

----End

Result

- ISDN phone1 and ISDN phone2 can communicate with ISDN phone3 by dialing number 83110002.

- When ISDN phone3 dials number 83110001, ISDN phone1 and ISDN phone2 can hear the ringing tone at the same time. In addition, ISDN phone1 and ISDN phone2 can communicate with ISDN phone3 at the same time.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported at a time.

Add the DSLD service board.

```
board add 0/4 H832DSLD
```

Create a service VLAN and configure its L3 interface.

```
vlan 10
interface vlanif 10
ip address 10.13.4.116 16
quit
```

Add an uplink port to the service VLAN.

```
port vlan 10 0/0 1
```

Configure the media IP address pool and the signaling IP address pool.

```
voip
ip address media 10.13.4.116 10.13.1.1
ip address signaling 10.13.4.116
```

Configure a static route.

```
quit
ip route-static 10.14.0.0 16 10.13.1.1
```

Add an MG interface.

```
interface h248 0
```

Configure the attributes of the MG interface.

```
if-h248 attribute mgip 10.13.4.116 mgport 2944 code text transfer udp MIDType
domainName domainName MA5616.com primary-mgc-ip1 10.14.1.2 primary-mgc-port 2944
mg-media-ip1 10.13.4.116 start-negotiate-version 2
```

Enable the MG interface.

```
reset coldstart
```

Configure the working mode of the ISDN BRA port.

```
quit
braport
braport attribute set 0/4/0 workmode p2mp
```
braport attribute set 0/4/1 activemode stable-active workmode p2p

Add an IUA link set and IUA links.

```
quitsigtran
iua-linkset add 0
iua-link add 0 0 1401 10.13.4.116 1400 10.14.1.2
```

Add an ISDN BRA user and configure the data.

```
quit
esl user
```

```
mgbrauser add 0/4/0 0 0 interfaceid 0 terminalid 2 priority cat3 telno 83110001
mgbrauser add 0/4/1 0 0 interfaceid 2 terminalid 4 priority cat1 telno 83110002
```

Save the data.

```
quit
save
```

8.4 Configuration Example of the VLAN Stacking Wholesale Service

This topic describes the VLAN stacking wholesale service and how to configure the VLAN stacking wholesale service on the MA5616.

8.4.1 Configuration Example of the VLAN Stacking Wholesale Service

This topic describes how to configure the wholesale service so that the service provided by the ISP can be delivered promptly to a specified user group.

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 control board and the corresponding service boards must be in the normal state.

Context

In a L2 switched 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.

Service Requirements

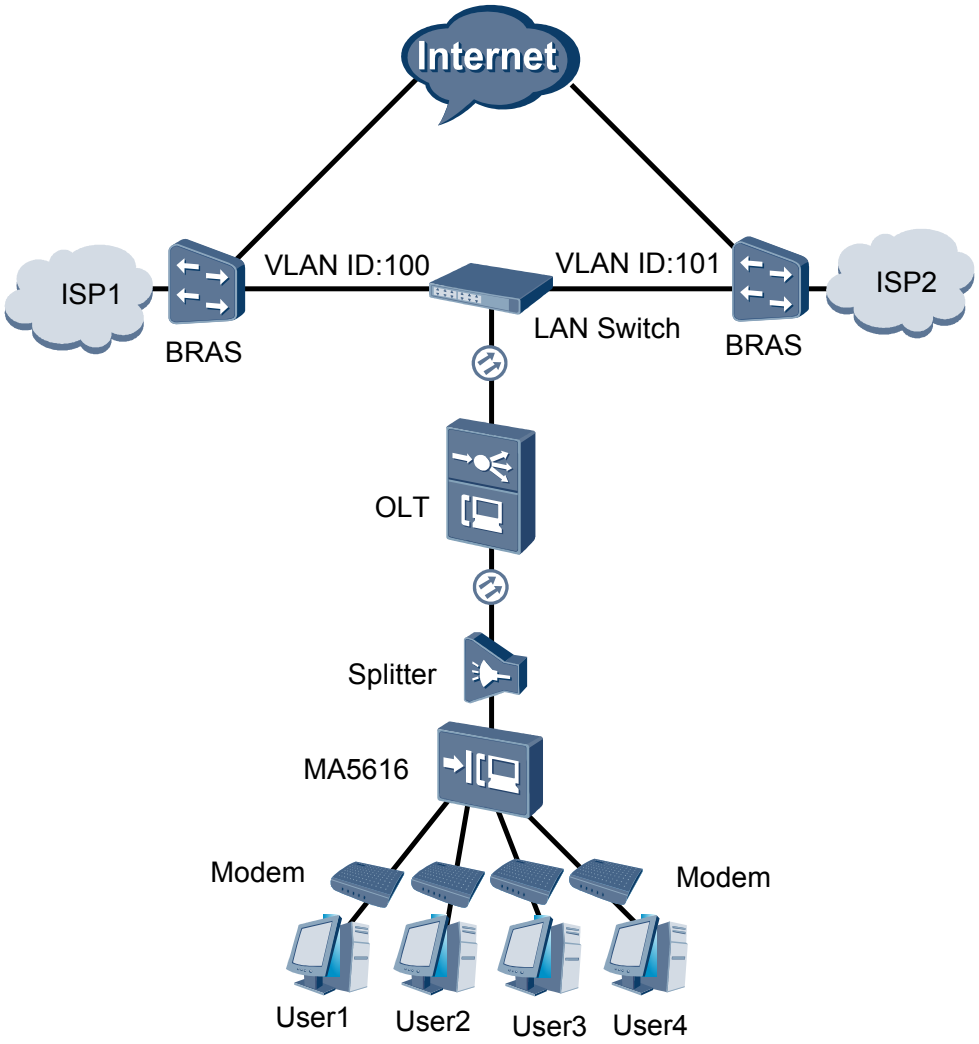
- The user accesses the Internet through the PPPoE dialup.
- The device adds an outer VLAN tag to user packets to identify ISPs, and adds an inner VLAN tag to identify users.

Networking

Figure 8-10 shows the example network for configuring the VLAN stacking wholesale service.

Users 1 and 2, and users 3 and 4 obtain the broadband service from different ISPs. The MA5616 supports the VLAN stacking function to implement the multi-ISP wholesale service. The device adds an outer VLAN tag to user packets to identify ISPs and adds an inner VLAN tag to identify users. Then, the device transmits the packets upstream over the GPON network and forwards the packets to the L2 network through the OLT. The L2 switch forwards the user packets to a specified ISP BRAS based on the outer VLAN tags. The ISP BRAS removes the outer VLAN tags and identifies the user based on the inner VLAN tags. After being authenticated by the ISP BRAS, the users can obtain the services provided by the ISP.

Figure 8-10 Example network for configuring the VLAN stacking wholesale service



Data Plan

Table 8-6 provides the data plan for configuring the VLAN stacking wholesale service.

Table 8-6 Data plan for configuring the VLAN stacking wholesale service

Item	Data
ISP 1 user group	Uplink port: 0/0/1
	Network-side VLAN ID (outer VLAN tag): 100
	VLAN attribute: stacking VLAN
	User 1: ● Access port: 0/1/0 ● Inner VLAN tag: 11

Item	Data
	User 2: ● Access port: 0/1/1 ● Inner VLAN tag: 12
ISP 2 user group	Uplink port: 0/0/1
	Network-side VLAN ID (outer VLAN tag): 101
	VLAN attribute: stacking VLAN
	User 3: ● Access port: 0/1/2 ● Inner VLAN tag: 11
	User 4: ● Access port: 0/1/3 ● Inner VLAN tag: 12

Procedure

Step 1 Create VLANs.

Network-side VLAN IDs are 100 and 101, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 100-101 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
```

Step 2 Set the VLAN attribute to stacking VLAN.

NOTE

You can run the **stacking outer-ethertype** command to set the type of outer Ethernet protocol supported by VLAN stacking on the MA5616. You can also run the **stacking inner-ethertype** command to set the type of inner Ethernet protocol supported by VLAN stacking on the MA5616. To ensure that Huawei device is interconnected with the device of other vendors, the type of the inner/outer Ethernet protocol must be the same as that of the interconnect device.

```
huawei(config)#vlan attrib 100-101 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
```

Step 3 Add an uplink port to the VLAN.

Add uplink port 0/0/1 to VLAN 100 and VLAN 101.

```
huawei(config)#port vlan 100-101 0/0 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
```

```
  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 service ports to VLANs.

Create service ports for users 1, 2, 3, and 4, and then add the service ports to VLAN 100 and VLAN 101.

```
huawei(config)#service-port 1 vlan 100 vdsl mode ptm 0/1/0 multi-service user-encap
pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan  100 vdsl mode ptm 0/1/1 multi-service user-
encap pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 3 vlan 101 vdsl mode ptm 0/1/2 multi-service user-encap
pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 4 vlan 101 vdsl mode ptm 0/1/3 multi-service user-encap
pppoe
rx-cttr 6 tx-cttr 6
```

Step 5 Set the inner VLAN tag.

The inner VLAN tag is used to identify the user. An inner VLAN tag under the same ISP must be unique. The VLAN tags under different ISPs can be the same with each other.

```
huawei(config)#display service-port all
{ <cr>|sort-by<K>||<K> }:

  Command:
          display service-port all
  ------------------------------------------------------------------------
  INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX  TX STATE
        ID   ATTR     TYPE                    TYPE  PARA
  ------------------------------------------------------------------------
      0  100 stacking vdl  0/1/ 0  -    -     encap pppoe       6   6 up
      1  100 stacking vdl  0/1/ 1  -    -     encap pppoe       6   6 up
      2  101 stacking vdl  0/1/ 2  -    -     encap pppoe       6   6 up
      3  101 stacking vdl  0/1/ 3  -    -     encap pppoe       6   6 up
  ------------------------------------------------------------------------
   Total : 4  (Up/Down :    4/0)
huawei(config)#stacking label service-port 1 11
huawei(config)#stacking label service-port 2 12
huawei(config)#stacking label service-port 3 11
huawei(config)#stacking label service-port 4 12
```

NOTE

In the actual configuration, the index of the traffic stream may vary according to the number of traffic streams in the system. You only need to ensure that the actual index corresponds to the inner VLAN tag.

Step 6 Save the data.

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

----End

Result

- After being authenticated by the ISP 1 BRAS, users 1 and 2 can obtain the services provided by ISP 1.
- After being authenticated by the ISP 2 BRAS, users 3 and 4 can obtain the services provided by ISP 2.

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.

Create VLANs.

```
vlan 100 to 101 smart
```

Set the VLAN attribute.

```
vlan attrib 100 to 101 stacking
```

Add an uplink port to VLANs.

```
port vlan 100 to 101 0/0 1
```

Add service ports to VLANs.

```
vlan 100 to 101 smart
vlan attrib 100 to 101 stacking
port vlan 100 to 101 0/0 1
service-port 1 vlan 100 vdsl mode ptm 0/1/0 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 2 vlan 100 vdsl mode ptm 0/1/1 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 3 vlan 101 vdsl mode ptm 0/1/2 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 4 vlan 101 vdsl mode ptm 0/1/3 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
```

Set inner VLAN tag.

```
stacking label service-port 1 11
stacking label service-port 2 12
stacking label service-port 3 11
stacking label service-port 4 12
```

8.4.2 Configuration Example of the VLAN ID Extension Service

This topic describes how to configure the VLAN ID extension for increasing the number of users that can be identified according to the VLAN ID by the BRAS.

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 control board and the involved service boards must be in the normal state.

Context

In the application of the VLAN ID extension, the outer and inner VLAN tags are used to identify the user, or the outer VLAN tag is used to identify the access device and the inner tag is used to identify the users that access the device. The BRAS identifies the access users based on the L2 VLAN tag to increase the number of users identified by the VLAN ID, thus increasing the number of users that access the BRAS.

In this example, outer VLAN tags 100 and 101 identify MA5616_A and MA5616_B respectively, and an inner VLAN tag identifies a device user.

Service Requirements

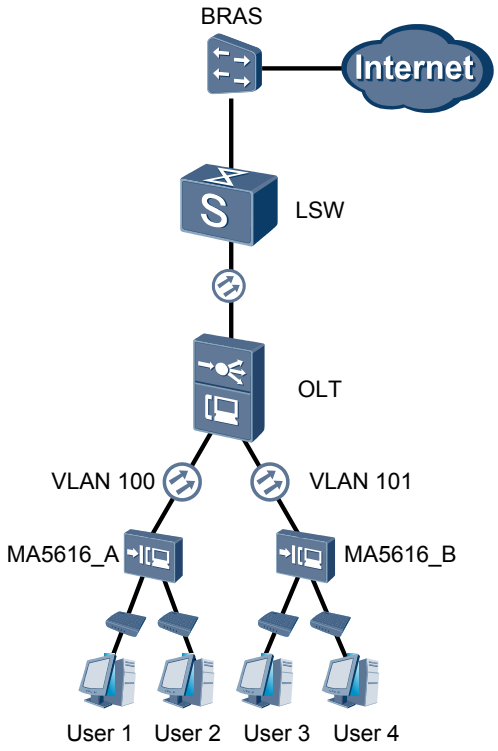
- The Internet access service is deployed on the network.
- Two VLAN IDs are allocated on the BRAS to identify four access users.
- The MA5616 is used on the GPON upstream transmission network.

Networking

Figure 8-11 shows the example network for configuring the VLAN ID extension.

Broadband users through multiple MA5616s are authenticated on a BRAS to obtain the broadband service provided by the carrier. The BRAS supports the user identification through L2 VLAN. The outer VLAN tag identifies the MA5616 that accesses users, and the inner VLAN tag identifies the users of the device.

Figure 8-11 Example network for configuring the VLAN ID extension



Data Plan

Table 8-7 provides the data plan for configuring the VLAN ID extension.

Table 8-7 Data plan for configuring the VLAN ID extension

Item	Data
MA5616_A	Uplink port: 0/0/1

Item	Data
	Upstream VLAN ID (outer VLAN tag): 100 VLAN attribute: Stacking VLAN
	User 1: ● Access port: 0/1/2 ● Inner VLAN tag: 11
	User 2: ● Access port: 0/1/3 ● Inner VLAN tag: 12
MA5616_B	Uplink port: 0/0/1
	Upstream VLAN ID (outer VLAN tag): 101 VLAN attribute: Stacking VLAN
	User 3: ● Access port: 0/1/2 ● Inner VLAN tag: 11
	User 4: ● Access port: 0/1/3 ● Inner VLAN tag: 12

Procedure

- The procedure for configuring the VLAN ID extension on MA5616_A is as follows:
  1. Create a VLAN.
     ```
     huawei(config)#vlan 100 smart
     ```
  2. Set the VLAN attribute to stacking VLAN.
     ```
     huawei(config)#vlan attrib 100 stacking
     ```
  3. Add an uplink port to the VLAN.
     ```
     huawei(config)#port vlan 100 0/0 1
     ```
  4. Add service ports to the VLAN.
     ```
     huawei(config)#service-port vlan 100 vdsl mode ptm 0/1/2 multi-service
     user-encap pppoe
     rx-cttr 6 tx-cttr 6
     huawei(config)#service-port vlan 100 vdsl mode ptm 0/1/3 multi-service
     user-encap pppoe
     rx-cttr 6 tx-cttr 6
     ```
  5. Set the inner VLAN tag.
     ```
     huawei(config)#display service-port all

     { <cr>|sort-by<K>||<K> }:

       Command:
               display service-port all

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

```
  INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX  TX
STATE
        ID   ATTR     TYPE                    TYPE
PARA

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

      0  100 common   vdl  0/1 /2  -    -     encap pppoe       6   6
up
      1  100 common   vdl  0/1 /3  -    -     encap pppoe       6   6
up

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

   Total : 2  (Up/Down :    2/0)
huawei(config)#stacking label service-port 0 11
huawei(config)#stacking label service-port 1 12
```

NOTE

In the actual configuration, the index of the traffic stream may vary according to the number of traffic streams in the system. You only need to ensure that the actual index corresponds to the inner VLAN tag.

6. Save the data.

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

- The procedure for configuring the VLAN ID extension on MA5616_B is as follows:

  The configuration procedure of MA5616_B is the same as the configuration procedure of MA5616_A. The only difference lies in the upstream VLAN ID. Hence, it is not described here.

----End

Result

After being authenticated by the BRAS, the users on MA5616_A and MA5616_B can access the Internet.

Two users of the MA5616 can be identified according to one outer VLAN tag. In this manner, the number of the access user based on one VLAN tag is increased.

Configuration File

Configuration file of MA5616_A

Create a VLAN.

```
vlan 100 smart
```

Set the VLAN attribute to stacking VLAN.

```
vlan attrib 100 stacking
```

Add an uplink port to the VLAN.

```
port vlan 100 0/0 1
```

Add service ports to the VLAN.

```
service-port 0 vlan 100 vdsl mode ptm 0/1/2 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 1 vlan 100 vdsl mode ptm 0/1/3 multi-service user-encap pppoe  rx-cttr
```

```
6
tx-cttr 6
```

Set the inner VLAN tag.

```
stacking label service-port 0 11
stacking label service-port 1 12
```

Configuration file of MA5616_B

Create a VLAN.

```
vlan 101 smart
```

Set the VLAN attribute to stacking VLAN.

```
vlan attrib 101 stacking
```

Add an uplink port to the VLAN.

```
port vlan 101 0/0 1
```

Add service ports to the VLAN.

```
service-port 0 vlan 101 vdsl mode ptm 0/1/2 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 1 vlan 101 vdsl mode ptm 0/1/3 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
```

Set the inner VLAN tag.

```
stacking label service-port 0 11
stacking label service-port 1 12
```

8.5 Configuring the Triple Play Service

This topic describes the triple play service and how to configure the triple play service on the MA5616 that is used on the GPON upstream transmission network.

8.5.1 Configuring the Triple Play Service - Single PVC for Multiple Services Based on the User-Side VLAN

This topic describes how to configure the triple play service in the single-PVC for multiple services mode (based on the user-side VLAN).

Prerequisites

Before configuring the triple play service, make sure that:

- The network devices and lines are in the normal state.
- The CPE is already configured (the CPE supports different VLANs for different services).
- All boards of the device run in the normal state.
- The VDSL2 line template and alarm template that are bound to the port are already configured. For details on the configuration procedure, see **3.7.3 Configuring the VDSL2 Profile**.

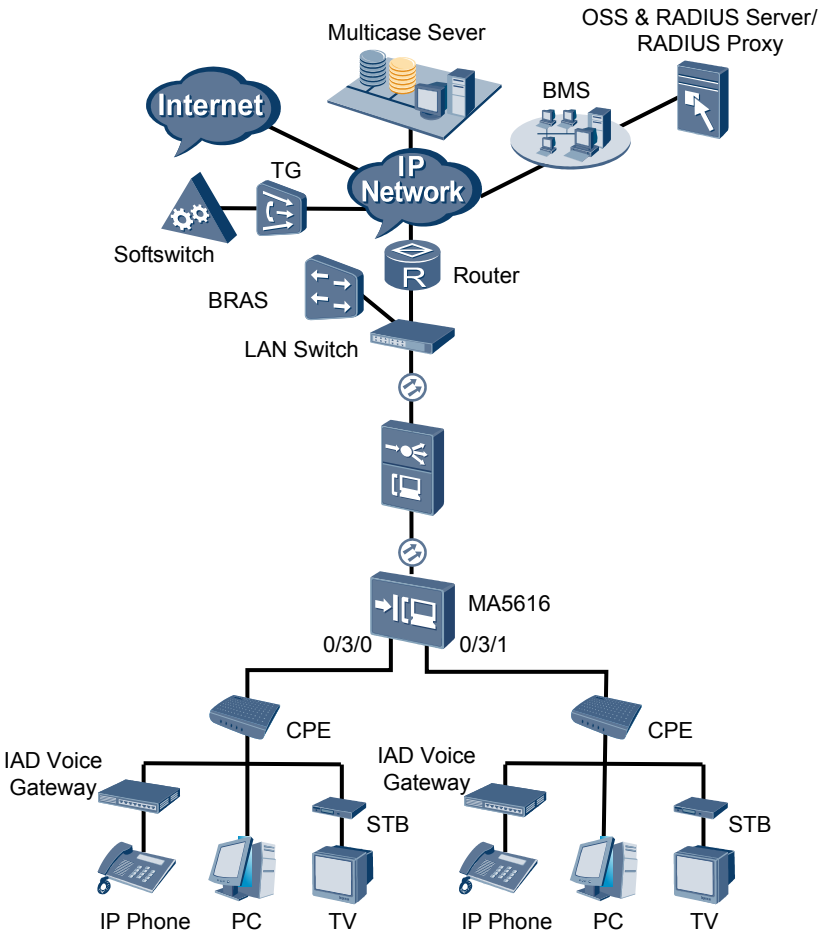
Service Requirements

- The MA5616 is used on the GPON upstream transmission network.
- VDSL2 user 1 and VDSL2 user 2 are connected to the MA5616 to implement the triple play.
- The Internet service is accessed in the PPPoE mode.
- After receiving different traffic streams through the same PVC, the MA5616 provides different QoS guarantees to the traffic streams according to the user-side VLANs.

Networking

Figure 8-12 shows the example network for configuring the triple play service based on the user-side VLAN.

Figure 8-12 Example network for configuring the triple play service based on the user-side VLAN



Data Plan

Table 8-8 provides the data plan of the triple play service based on the user-side VLAN.

Table 8-8 Data plan of the triple play service based on the user-side VLAN

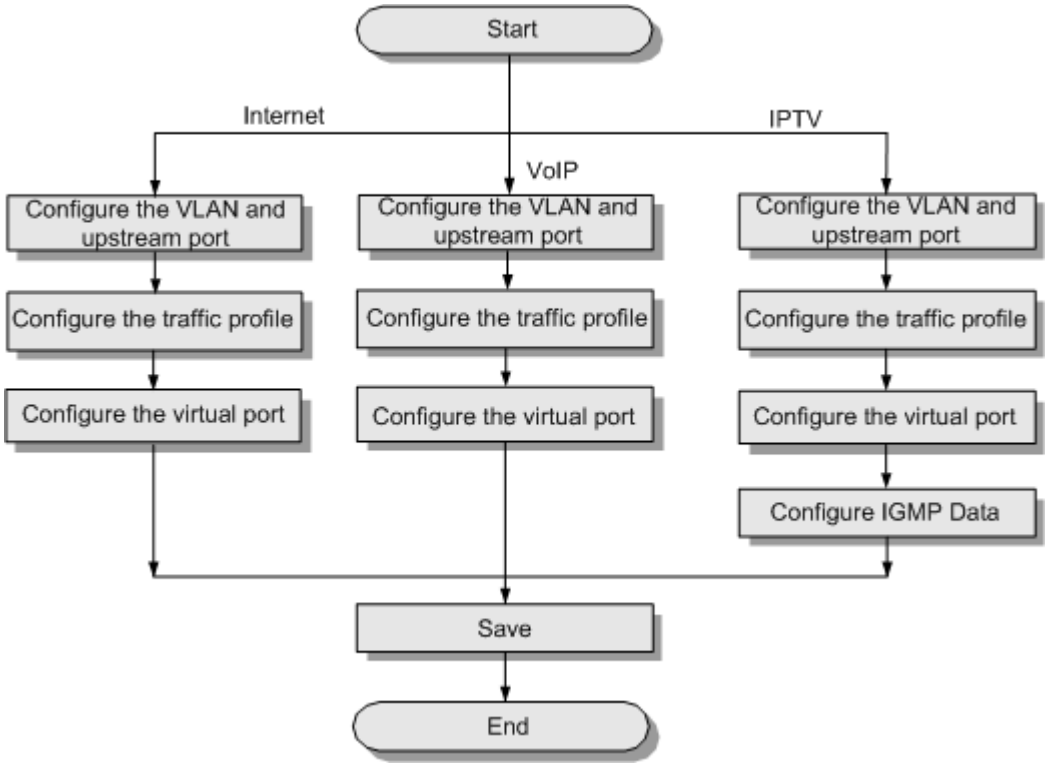
Item	Data
VDSE	Service ports: 0/1/0 and 0/1/1 Index of the VDSL2 line template bound to the port: 2, where: ● Index of the VDSL2 line profile: 3 ● Index of the VDSL2 channel profile: 3 Index of the VDSL2 alarm template bound to the port: 2, where: ● Index of the VDSL2 line alarm profile: 3 ● Index of the VDSL2 channel alarm profile: 3 VPI/VCI: 0/35
Traffic profile parameters	Internet service: 1 Mbit/s VoIP service: 64 Kbit/s IPTV service: no limit
Uplink port ID	0/0/1
Upstream VLANs	Internet service: smart VLAN 102 VoIP service: smart VLAN 103 IPTV service: smart VLAN 104
User-side VLANs	Internet service: smart VLAN 2 VoIP service: smart VLAN 3 IPTV service: smart VLAN 4
IGMP version	IGMP v3 (default IGMP version in the multicast VLAN mode)
Multicast source	Two multicast sources: ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
Multicast program library	Programs in multicast VLAN 104: Program 1: with IP address 224.1.1.1, the program source IP address being the same as the IP address of ISP 1 (10.10.10.10) Program 2: with IP address 224.1.1.2, the program source IP address being the same as the IP address of ISP 2 (10.10.10.11)
Right profile	Set right profile 0. Profile 0 has the right to watch program 1 in the program library.
Multicast users	User 1: User 1 (on port 0/1/0) can watch all the programs. User 2: User 2 (on port 0/1/1) can watch only program 1.

Item	Data
Upstream priority	The 802.1p priorities are used. The VoIP service has priority 6, IPTV service priority 5, and Internet service priority 1.

Configuration Flowchart

Figure 8-13 shows the flowchart for configuring the triple play service based on the user-side VLAN.

Figure 8-13 Flowchart for configuring the triple play service based on the user-side VLAN



Procedure

- Configure the Internet service.
  1. Create a VLAN and add an uplink port to the VLAN.

     ```
     huawei(config)#vlan 102 smart
     huawei(config)#port vlan 102 0/0 1
     ```

  2. Configure a traffic profile.
     - Because the VoIP, IPTV, and Internet 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 service. In this example, set the traffic profile index to 7 and the 802.1p priority of the Internet service to 1.

```
huawei(config)#traffic table ip index 7 cir 1024 priority 1 priority-
policy loca
l-Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-vlan 2 rx-cttr 7 tx-cttr 7
huawei(config)#service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-vlan 2 rx-cttr 7 tx-cttr 7
```

4. Save the data.

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

- Configure the VoIP service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 103 smart
huawei(config)#port vlan 103 0/0 1
```

2. Configure a traffic profile.

   Set the traffic profile index to 8 and the 802.1p priority of the VoIP service to 6.

```
huawei(config)#traffic table ip index 8 cir 64 priority 6 priority-policy
local-
Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
```

4. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 104-105
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
huawei(config)#port vlan 104-105 0/0
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
  The total of the VLANs having been processed is
```

```
2
  The total of the port VLAN(s) having been added is 2
```

2. Configure a traffic profile.

   Set the traffic profile index to 9 and the 802.1p priority of the IPTV service to 5.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
local-Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
```

CAUTION

On the MA5616, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

4. Configure the multicast data.

   To provision the multicast video service, you also need to configure IGMP proxy and programs.

   a. Add a multicast VLAN and configure the multicast mode.

```
huawei(config)#multicast-vlan 104
huawei(config-mvlan104)#igmp mode
proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   NOTE

   Select a multicast mode according to the actual requirements. In this example, the IGMP proxy mode is considered.

   b. Configure the multicast uplink port.

```
huawei(config-mvlan104)#igmp uplink-port 0/0/1
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp uplink-port-mode
default
  Are you sure to change the uplink port mode?(y/n)[n]:y
```

   c. Configure the program library.

```
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp program add name program1 ip 224.1.1.1
sourceip 10.
10.10.10
huawei(config-mvlan104)#igmp program add name program2 ip 224.1.1.2
sourceip 10.
10.10.11
```

   d. Configure the right profile.

```
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name
program1 watc
h
```

e. Configure multicast users.

```
huawei(config-btv)#igmp user add service-port 10
huawei(config-btv)#igmp user add service-port 11 auth
huawei(config-btv)#igmp user bind-profile service-port 11 profile-
name profile0
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp multicast-vlan member service-port 10
huawei(config-mvlan104)#igmp multicast-vlan member service-port 11
huawei(config-mvlan104)#quit
```

5. 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.

- Perform the PPPoE dialup on the PC. After the dialup is successful, the user can access the Internet.
- VoIP users can call each other.
- The IPTV user on port 0/1/0 can watch all the programs, and the IPTV user on port 0/1/1 can watch program 1 only.

Configuration File

Internet:

```
vlan 102 smart
port vlan 102 0/0 1
traffic table ip index 7 cir 1024 priority 1 priority-policy local-Setting
service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-vlan 2 rx-cttr 7 tx-cttr 7
service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-vlan 2 rx-cttr 7 tx-cttr 7
save
```

VoIP:

```
vlan 103 smart
port vlan 103 0/0 1
traffic table ip index 8 cir 64 priority 6 priority-policy local-Setting
service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
save
```

IPTV:

```
vlan 104-105 smart
y
port vlan 104-105 0/0 1
y
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
multicast-vlan 104
igmp mode proxy
y
```

```
igmp uplink-port 0/0/1
btv
igmp uplink-port-mode default
y
multicast-vlan 104
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name program1 watch
igmp user add service-port 10
igmp user add service-port 11 auth
igmp user bind-profile service-port 11 profile-name profile0
multicast-vlan 104
igmp multicast-vlan member service-port 10
igmp multicast-vlan member service-port 11
quit
save
```

8.5.2 Configuring the Triple Play Service - Single PVC for Multiple Services Based on the User-Side 802.1p

This topic describes how to configure the triple play service in the single-PVC for multiple services mode (based on the user-side 802.1p priority).

Prerequisites

Before configuring the triple play service, make sure that:

- The network devices and lines are in the normal state.
- The CPE is already configured (the CPE supports different user-side 802.1p priorities for different services).
- All boards of the device run in the normal state.
- The VDSL2 line template and alarm template that are bound to the port are already configured. For details on the configuration procedure, see **3.7.3 Configuring the VDSL2 Profile**.

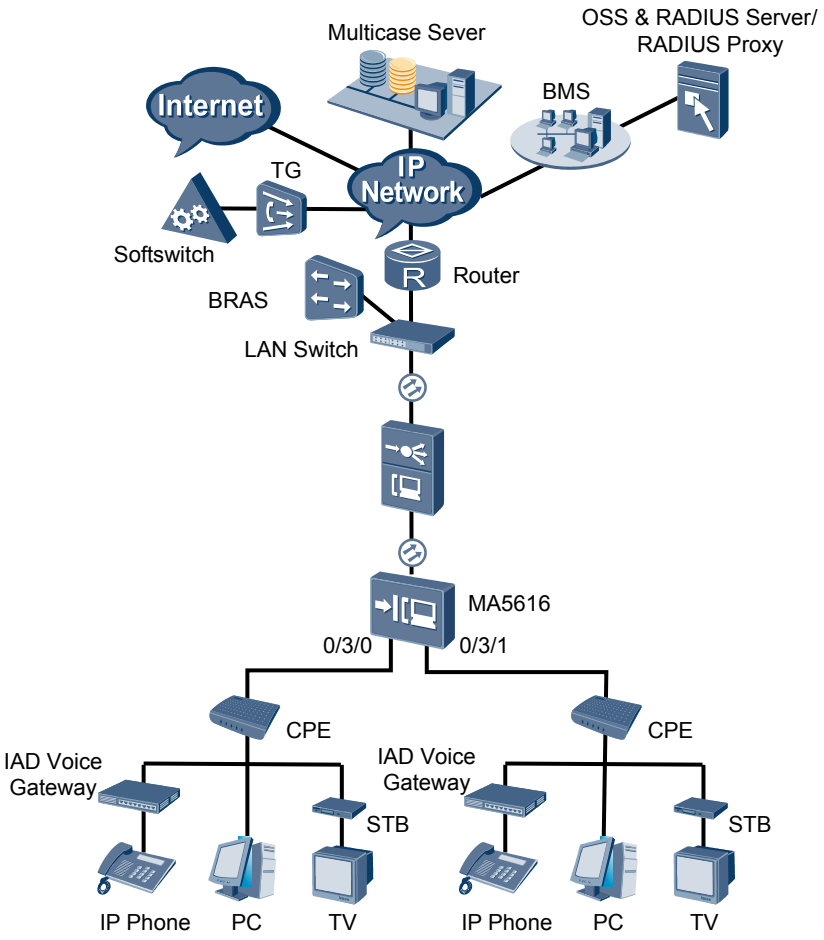
Service Requirements

- The MA5616 is used on the GPON upstream transmission network.
- VDSL2 user 1 and VDSL2 user 2 are connected to the MA5616 to implement the triple play.
- The Internet service is accessed in the PPPoE mode.
- After receiving different traffic streams through the same PVC, the MA5616 provides different QoS guarantees to the traffic streams according to the user-side 802.1p priority.

Networking

Figure 8-14 shows the example network for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Figure 8-14 Example network for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority



Data Plan

Table 8-9 provides the data plan for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Table 8-9 Data plan for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority

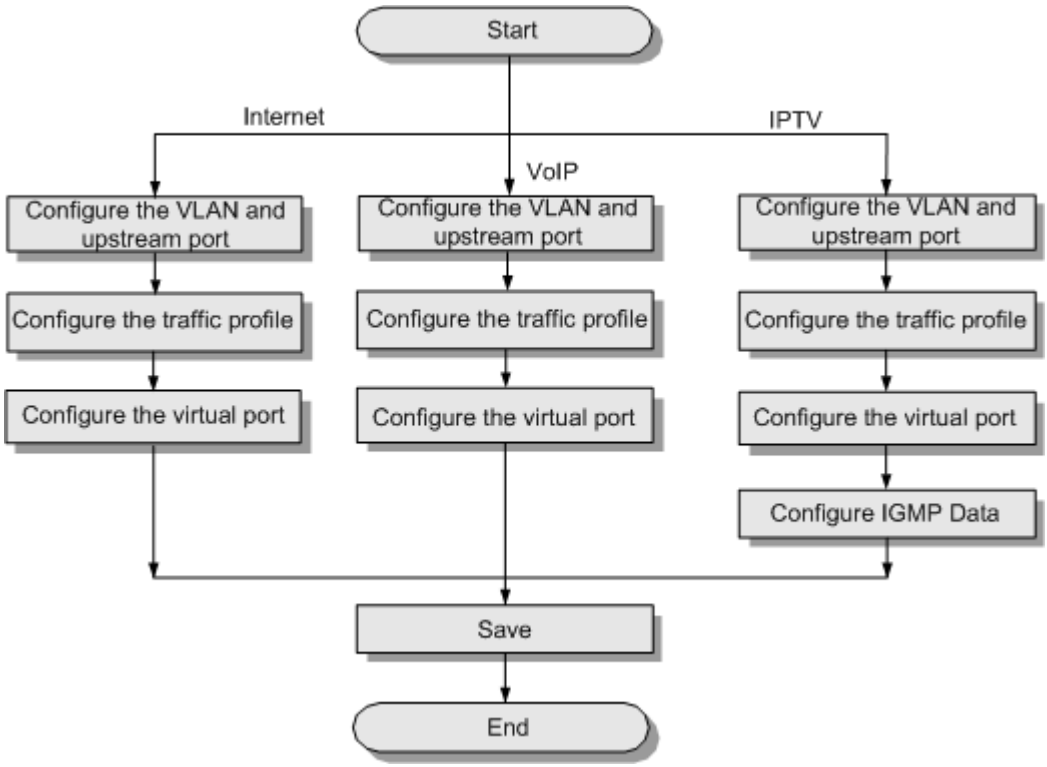
Item	Data
VDSE	Service ports: 0/1/0 and 0/1/1 Index of the VDSL2 line template bound to the port: 2, where: ● Index of the VDSL2 line profile: 3 ● Index of the VDSL2 channel profile: 3 Index of the VDSL2 alarm template bound to the port: 2, where: ● Index of the VDSL2 line alarm profile: 3 ● Index of the VDSL2 channel alarm profile: 3 VPI/VCI: 0/35
Traffic profile parameters	Internet service: 1 Mbit/s VoIP service: 64 Kbit/s IPTV service: no limit
Uplink port ID	0/0/1
Upstream VLANs	Internet service: smart VLAN 102 VoIP service: smart VLAN 103 IPTV service: smart VLAN 104
User-side 802.1p priorities	Internet service: 2 VoIP service: 3 IPTV service: 4
IGMP version	IGMP v3 (default IGMP version in the multicast VLAN mode)
Multicast source	Two multicast sources: ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
Multicast program library	Programs in multicast VLAN 104: Program 1: with IP address 224.1.1.1, the program source IP address being the same as the IP address of ISP 1 (10.10.10.10) Program 2: with IP address 224.1.1.2, the program source IP address being the same as the IP address of ISP 2 (10.10.10.11)
Right profile	Set right profile 0. Profile 0 has the right to watch program 1 in the program library.
Multicast users	User 1: User 1 (on port 0/3/0) can watch all the programs. User 2: User 2 (on port 0/3/1) can watch only program 1.

Item	Data
Upstream priority	The 802.1p priorities are used. The VoIP service has priority 6, IPTV service priority 5, and Internet service priority 1.

Configuration Flowchart

Figure 8-15 shows the flowchart for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Figure 8-15 Flowchart for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority



Procedure

- Configure the Internet service.
  1. Create a VLAN and add an uplink port to the VLAN.

     ```
     huawei(config)#vlan 102 smart
     huawei(config)#port vlan 102 0/0 1
     ```

  2. Configure a traffic profile.
     - Because the VoIP, IPTV, and Internet 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 service. In this example, set the traffic profile index to 7 and the 802.1p priority of the Internet service to 1.

```
huawei(config)#traffic table ip index 7 cir 1024 priority 1 priority-
policy loca
l-Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-8021p 2 rx-cttr 7 tx-cttr 7
huawei(config)#service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-8021p 2 rx-cttr 7 tx-cttr 7
```

4. Save the data.

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

- Configure the VoIP service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 103 smart
huawei(config)#port vlan 103 0/0 1
```

2. Configure a traffic profile.

   Set the traffic profile index to 8 and the 802.1p priority of the VoIP service to 6.

```
huawei(config)#traffic table ip index 8 cir 64 priority 6 priority-policy
local-
Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
```

4. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 104-105
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
huawei(config)#port vlan 104-105 0/0
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
  The total of the VLANs having been processed is
2
  The total of the port VLAN(s) having been added is 2
```

2. Configure a traffic profile.

   Set the traffic profile index to 9 and the 802.1p priority of the IPTV service to 5.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
local-Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
```

CAUTION

On the MA5616, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

4. Configure the multicast data.

   To provision the multicast video service, you also need to configure IGMP proxy and programs.

   a. Add a multicast VLAN and configure the multicast mode.

```
huawei(config)#multicast-vlan 104
huawei(config-mvlan104)#igmp mode
proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   NOTE

   Select a multicast mode according to the actual requirements. In this example, the IGMP proxy mode is considered.

   b. Configure the multicast uplink port.

```
huawei(config-mvlan104)#igmp uplink-port 0/0/1
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp uplink-port-mode
default
  Are you sure to change the uplink port mode?(y/n)[n]:y
```

   c. Configure the program library.

```
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp program add name program1 ip 224.1.1.1
sourceip 10.
10.10.10
huawei(config-mvlan104)#igmp program add name program2 ip 224.1.1.2
sourceip 10.
10.10.11
huawei(config-mvlan104)#quit
```

   d. Configure the right profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name
program1 watc
h
```

e. Configure multicast users.

```
huawei(config-btv)#igmp user add service-port 10
huawei(config-btv)#igmp user add service-port 11 auth
huawei(config-btv)#igmp user bind-profile service-port 11 profile-
name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 104
huawei(config-mvlan104)#igmp multicast-vlan member service-port 10
huawei(config-mvlan104)#igmp multicast-vlan member service-port 11
huawei(config-mvlan104)#quit
```

5. 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.

- Perform the PPPoE dialup on the PC. After the dialup is successful, the user can access the Internet.
- VoIP users can call each other.
- The IPTV user on port 0/1/0 can watch all the programs, and the IPTV user on port 0/1/1 can watch program 1 only.

Configuration File

Internet:

```
vlan 102 smart
port vlan 102 0/0 1
traffic table ip index 7 cir 1024 priority 1 priority-policy local-Setting
service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-8021p 2 rx-cttr 7 tx-cttr 7
service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-8021p 2 rx-cttr 7 tx-cttr 7
save
```

VoIP:

```
vlan 103 smart
port vlan 103 0/0 1
traffic table ip index 8 cir 64 priority 6 priority-policy local-Setting
service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
save
```

IPTV:

```
vlan 104-105 smart
y
port vlan 104-105 0/0 1
y
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
```

```
ice user-8021p 4 rx-cttr 9 tx-cttr 9
service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
multicast-vlan 104
igmp mode proxy
y
igmp uplink-port 0/0/1
btv
igmp uplink-port-mode default
y
multicast-vlan 104
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name program1 watch
igmp user add service-port 10
igmp user add service-port 11 auth
igmp user bind-profile service-port 11 profile-name profile0
multicast-vlan 104
igmp multicast-vlan member service-port 10
igmp multicast-vlan member service-port 11
quit
save
```

8.5.3 Configuring the Triple Play Service - Multiple PVCs for Multiple Services

This topic describes how to configure the triple play service in the multi-PVC for multiple services mode.

Prerequisites

Before configuring the triple play service, make sure that:

- The network devices and lines are in the normal state.
- The CPE is already configured (the CPE supports different PVCs for different services).
- All boards of the device run in the normal state.
- The VDSL2 line template and alarm template that are bound to the port are already configured. For details on the configuration procedure, see **3.7.3 Configuring the VDSL2 Profile**.

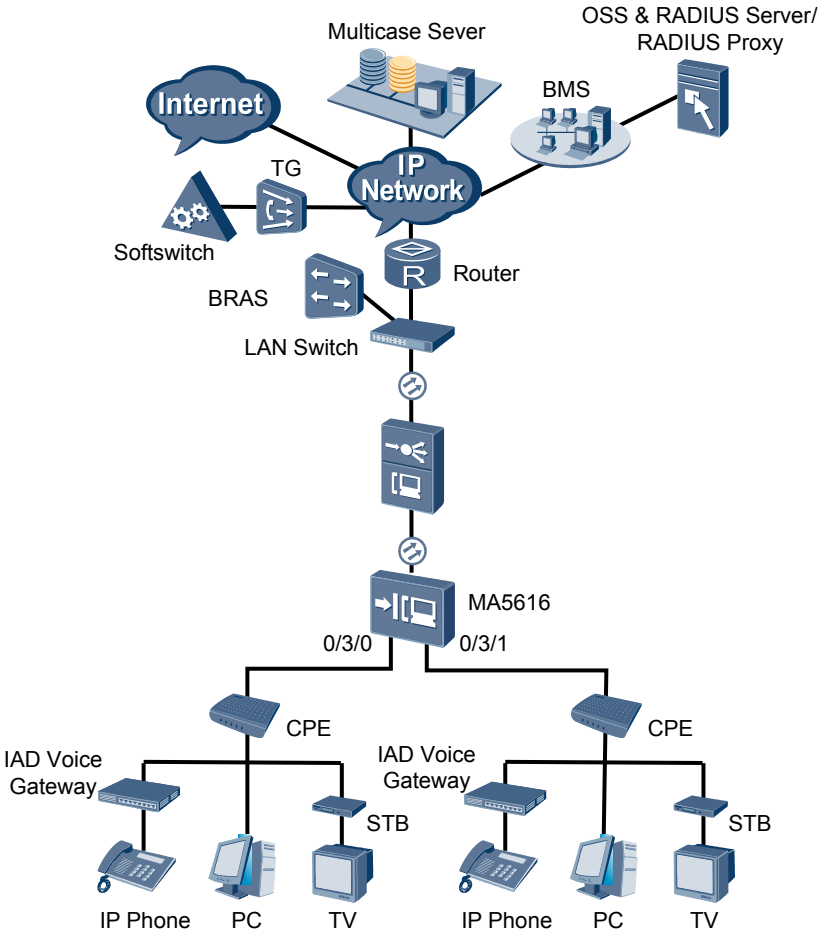
Service Requirements

- The MA5616 is used on the GPON upstream transmission network.
- VDSL2 user 1 and VDSL2 user 2 are connected to the MA5616 to implement the triple play.
- The Internet service is provided in the PPPoE mode.
- After receiving different traffic streams, the MA5616 provides different QoS guarantees to the traffic streams according to the traffic priorities in the PVC.

Networking

Figure 8-16 shows the example network of the triple play service in the multi-PVC for multiple services mode.

Figure 8-16 Example network of the triple play service in the multi-PVC for multiple services mode



Data Plan

Table 8-10 provides the data plan for configuring the triple play service in the multi-PVC for multiple services mode.

Table 8-10 Data plan for configuring the triple play service in the multi-PVC for multiple services mode

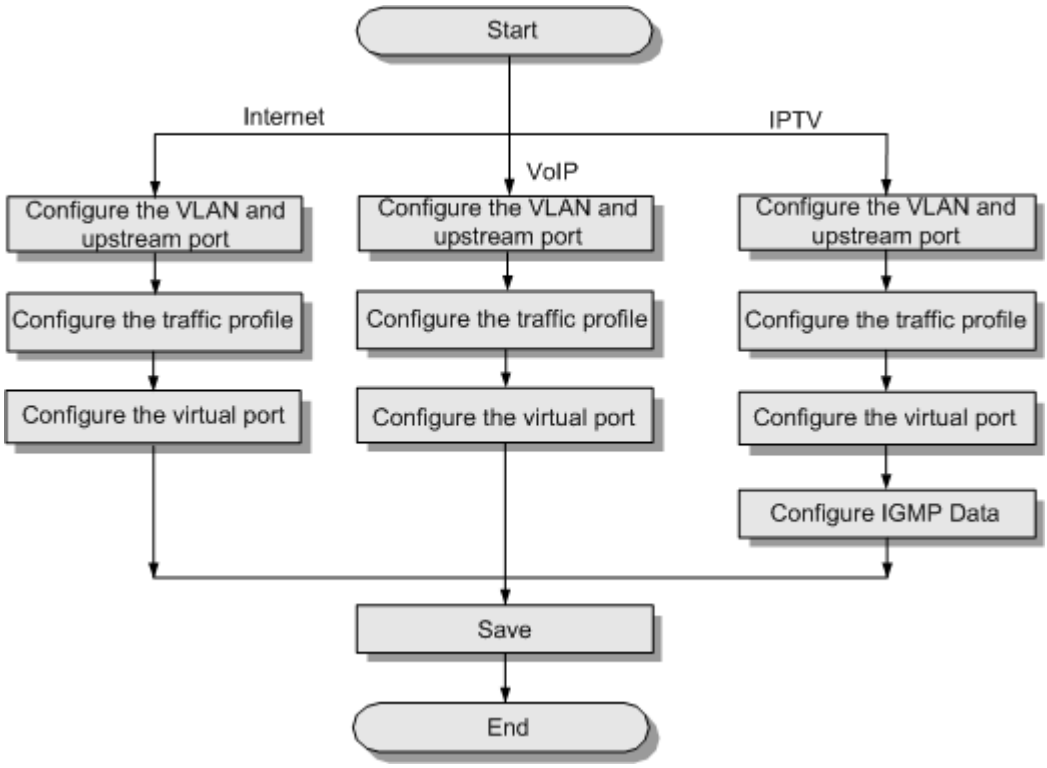
Item	Data
VDSE	Service ports: 0/1/0 and 0/1/1 Index of the VDSL2 line template bound to the port: 2, where: ● Index of the VDSL2 line profile: 3 ● Index of the VDSL2 channel profile: 3 Index of the VDSL2 alarm template bound to the port: 2, where: ● Index of the VDSL2 line alarm profile: 3 ● Index of the VDSL2 channel alarm profile: 3

Item	Data
	VPI/VCI for the Internet service: 0/37
	VPI/VCI for the VoIP service: 0/36
	VPI/VCI for the IPTV service: 0/35
Traffic profile parameters	Internet service: 1 Mbit/s VoIP service: 64 Kbit/s IPTV service: no limit
Uplink port ID	0/0/1
VLANs	Internet service: smart VLAN 102
	VoIP service: smart VLAN 103
	IPTV service: smart VLAN 104
IGMP version	IGMP v3 (default IGMP version in the multicast VLAN mode)
Multicast source	Two multicast sources: ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
Multicast program library	Programs in multicast VLAN 104: Program 1: with IP address 224.1.1.1, the program source IP address being the same as the IP address of ISP 1 (10.10.10.10) Program 2: with IP address 224.1.1.2, the program source IP address being the same as the IP address of ISP 2 (10.10.10.11)
Right profile	Set right profile 0. Profile 0 has the right to watch program 1 in the program library.
Multicast users	User 1: User 1 (on port 0/1/0) can watch all the programs. User 2: User 2 (on port 0/1/1) can watch only program 1.
Upstream priority	The 802.1p priorities are used. The VoIP service has priority 6, IPTV service priority 5, and Internet service priority 1.

Configuration Flowchart

Figure 8-17 shows the flowchart for configuring the triple play service in the multi-PVC for multiple services mode.

Figure 8-17 Flowchart for configuring the triple play service in the multi-PVC for multiple services mode



Procedure

- Configure the Internet service.
  1. Create a VLAN and add an uplink port to the VLAN.

     ```
     huawei(config)#vlan 102 smart
     huawei(config)#port vlan 102 0/0 1
     ```

  2. Configure a traffic profile.
     - Because the VoIP, IPTV, and Internet 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 service. In this example, set the traffic profile index to 7 and the 802.1p priority of the Internet service to 1.

     ```
     huawei(config)#traffic table ip index 7 cir 1024 priority 1 priority-
     policy loca
     l-Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 37 rx-
     cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/1 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 the uplink port to the VLAN.

     ```
     huawei(config)#vlan 103 smart
     huawei(config)#port vlan 103 0/0 1
     ```

  2. Configure a traffic profile.

     Set the traffic profile index to 8 and the 802.1p priority of the VoIP service to 6.

     ```
     huawei(config)#traffic table ip index 8 cir 64 priority 6 priority-policy
     local-
     Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 36 rx-
     cttr 8 tx-cttr 8
     huawei(config)#service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 36 rx-
     cttr 8 tx-cttr 8
     ```

  4. Save the data.

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

- Configure the IPTV service.
  1. Create a VLAN and add the uplink port to the VLAN.

     ```
     huawei(config)#vlan 104-105
     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
     huawei(config)#port vlan 104-105 0/0
     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
       The total of the VLANs having been processed is
     2
       The total of the port VLAN(s) having been added is 2
     ```

  2. Configure a traffic profile.

     Set the traffic profile index to 9 and the priority of the IPTV service to 5.

     ```
     huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
     local-Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35
     rx-cttr 9 tx-cttr 9
     huawei(config)#service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35
     rx-cttr 9 tx-cttr 9
     ```

NOTE

On the MA5616, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

4. Configure the multicast data.

   To provision the multicast video service, you also need to configure IGMP proxy and programs.

   a. Add a multicast VLAN and configure the multicast mode.

```
huawei(config)#multicast-vlan 104
huawei(config-mvlan104)#igmp mode
proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   NOTE

   Select a multicast mode according to the actual requirements. In this example, the IGMP proxy mode is considered.

   b. Configure the multicast uplink port.

```
huawei(config-mvlan104)#igmp uplink-port 0/0/1
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp uplink-port-mode
default
  Are you sure to change the uplink port mode?(y/n)[n]:y
```

   c. Configure the program library.

```
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp program add name program1 ip 224.1.1.1
sourceip 10.
10.10.10
huawei(config-mvlan104)#igmp program add name program2 ip 224.1.1.2
sourceip 10.
10.10.11
```

   d. Configure the right profile.

```
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name
program1 watc
h
```

   e. Configure multicast users.

```
huawei(config-btv)#igmp user add service-port 10
huawei(config-btv)#igmp user add service-port 11 auth
huawei(config-btv)#igmp user bind-profile service-port 11 profile-
name profile0
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp multicast-vlan member service-port 10
huawei(config-mvlan104)#igmp multicast-vlan member service-port 11
huawei(config-mvlan104)#quit
```

5. 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.

- Perform the PPPoE dialup on the PC. After the dialup is successful, the user can access the Internet.
- VoIP users can call each other.

- The IPTV user on port 0/1/0 can watch all the programs, and the IPTV user on port 0/1/1 can watch program 1 only.

Configuration File

Internet:

```
vlan 102 smart
port vlan 102 0/0 1
traffic table ip index 7 cir 1024 priority 1 priority-policy local-Setting
service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
save
```

VoIP:

```
vlan 103 smart
port vlan 103 0/0 1
traffic table ip index 8 cir 64 priority 6 priority-policy local-Setting
service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
save
```

IPTV:

```
vlan 104-105 smart
y
port vlan 104-105 0/0 1
y
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
multicast-vlan 104
igmp mode proxy
y
igmp uplink-port 0/0/1
btv
igmp uplink-port-mode default
y
multicast-vlan 104
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name program1 watch
igmp user add service-port 10
igmp user add service-port 11 auth
igmp user bind-profile service-port 11 profile-name profile0
multicast-vlan 104
igmp multicast-vlan member service-port 10
igmp multicast-vlan member service-port 11
quit
save
```

9 Configuration Example of Services on the MA5616 Through GE Upstream Transmission

About This Chapter

This topic describes how to configure Internet access service, multicast service, voice service, and triple play service on the MA5616 on different networks.

9.1 Configuration Example of the xDSL Internet Access Service

This topic describes how to configure the xDSL Internet access service in the PPPoE, IPoE, PPPoA and IPoA modes.

9.1.1 Configuration Example of the xDSL Internet Access Service Through PPPoE Dialup

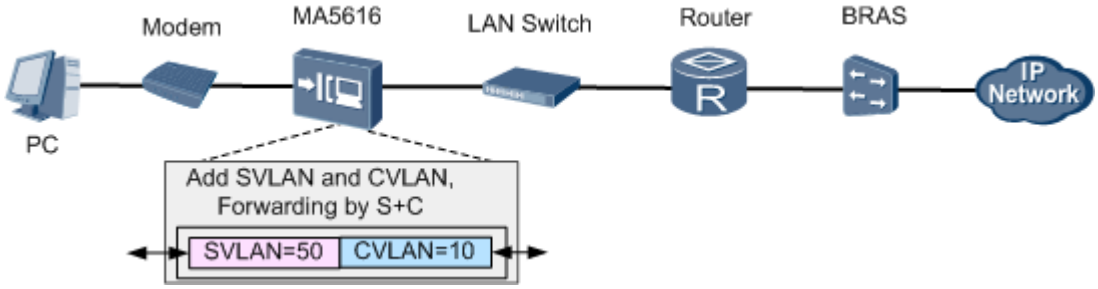
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode through the PPPoE dialup and at a rate of 2048 kbit/s, and the user packet goes upstream carrying two VLAN tags through the MA5616.

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.
- PITP is enabled to protect the user account against theft and roaming.
- 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 9-1 shows an example network of the xDSL Internet access service through the PPPoA dialup.

Figure 9-1 Example network of the xDSL Internet access service through the PPPoA dialup



Prerequisite

- The number of xDSL ports is limited by the licenses. Make sure that sufficient licenses are already applied for.
- Configure the AAA function.
  - To enable the AAA function on the device, see **3.12 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

MA5616 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 service-profile profile-id 1
huawei(config-vlan-srvprof-1)#forwarding vlan-connect
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 50 profile-id 1
```

Step 2 Configure upstream ports.

Add upstream ports 0/0/1 and 0/0/0 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/0 0
huawei(config)#port vlan 50 0/0 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 0/0 0 0/0 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 **3.7.1 Configuring the ADSL2+ Profile**. Here, 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 template-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(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
```

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 MA5616, 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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

   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 MA5616, 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 0/4/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/1/0 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. Here, the **cntel** is considered as an example.

```
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 **3.10.1 Configuring Anti-Theft and Roaming of User Account Through PITP**.

Step 7 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, 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.

Configuration File

Configuration File in the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan service-profile profile-id 1
forwarding vlan-connect
commit
quit
vlan bind service-profile 50 profile-id 1
port vlan 50 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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
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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/4
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/1/0 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
```

9.1.2 Configuration Example of the xDSL IPoE Internet Access Service

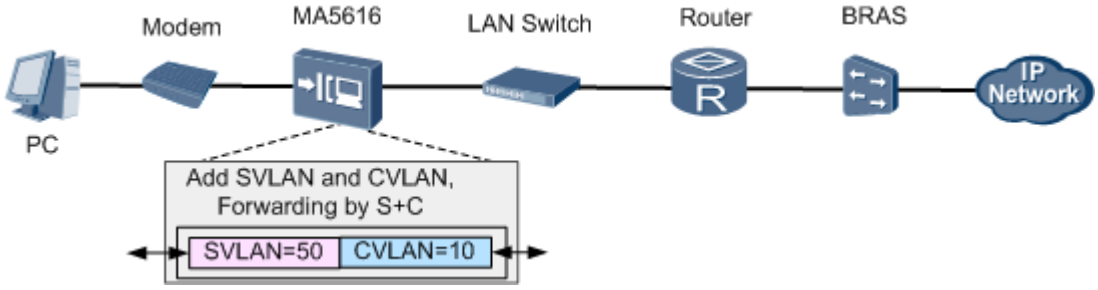
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode, and then access the Internet in the IPoE mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the IPoE mode. The account authentication is implemented through the DHCP option 82 field.
- 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.
- 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 9-2 shows an example network of the xDSL IPoE Internet access service.

Figure 9-2 Example network of the xDSL IPoE Internet access service



Prerequisite

The number of xDSL ports is under the control of licenses. Make sure that sufficient licenses are already requested.

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 service-profile profile-id 1
huawei(config-vlan-srvprof-1)#forwarding vlan-connect
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 50 profile-id 1
```

Step 2 Configure upstream ports.

Add upstream ports 0/0/1 and 0/0/0 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/0 0
huawei(config)#port vlan 50 0/0 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 0/0 0 0/0 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 **3.7.1 Configuring the ADSL2+ Profile**. Here, 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 template-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(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
```

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 MA5616, 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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

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 MA5616, 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 0/4/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/1/0 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.

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
```

NOTE

- For the details about the security of DHCP accounts, see **3.10.2 Configuring Anti-Theft and Roaming of User Accounts Through DHCP**.

Step 7 Save the data.

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

----End

Verification

- 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.

Configuration File

Configuration File for the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan service-profile profile-id 1
forwarding vlan-connect
commit
quit
vlan bind service-profile 50 profile-id 1
port vlan 50 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/4
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/4/0 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 0/1
deactivate 0
```

```
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/1/0 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
```

9.1.3 Configuration Example of the xDSL PPPoA Internet Access Service

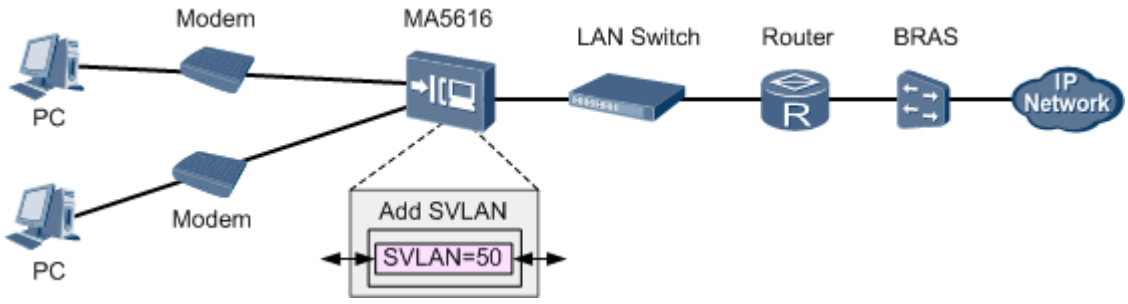
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode, and then access the Internet in the PPPoA mode at a rate of 2048 kbit/s.

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 9-3 shows an example network of the xDSL PPPoA Internet access service.

Figure 9-3 Example network of the xDSL PPPoA Internet access service



Prerequisite

- The number of xDSL ports is under the control of licenses. Make sure that sufficient licenses are already requested.
- Configure the AAA function.
  - To enable the AAA function on the device, see **3.12 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 MA5616 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 0/0/1 and 0/0/0 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/0 0
huawei(config)#port vlan 50 0/0 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 0/0 0 0/0 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 **3.7.1 Configuring the ADSL2+ Profile**. 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(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
```

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 MA5616, 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 MA5616HW/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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

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 MA5616, 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 0/4/0, 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 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 2 description MA5616HW/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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0, 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 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5616HW/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 0/4/0 vpi 1 vci 39 type pppoa llc
huawei(config)#encapsulation 0/1/0 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. Here, the **cntel** is considered as an example.

```
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 **3.10.1 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 MA5616HW/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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/4
deactivate 0
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5616HW/Vlanid:50/shdsl/smart
mac-address max-mac-count service-port 2 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/4/0 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5616HW/Vlanid:50/vdsl/smart
mac-address max-mac-count service-port 3 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/1/0 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

9.1.4 Configuration Example of the xDSL IPoA Internet Access Service

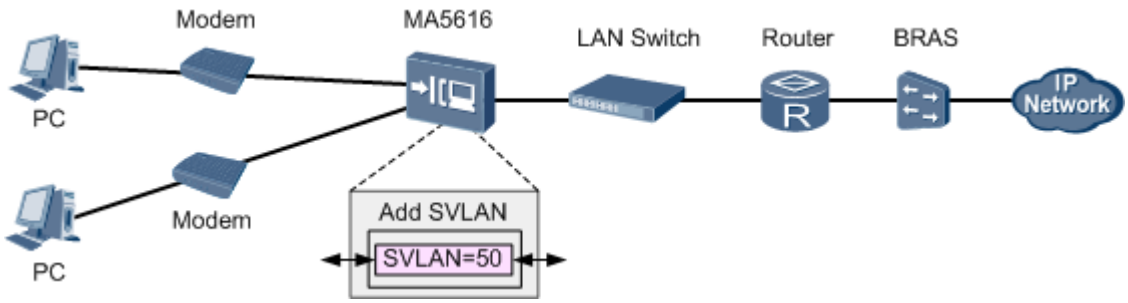
This topic describes how to configure a user so that the user can access the MA5616 in the xDSL mode, and then access the Internet in the IPoA mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the IPoA mode. The MA5616 works in the L2 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.
- 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 9-4 shows an example network of the xDSL IPoA Internet access service.

Figure 9-4 Example network of the xDSL IPoA Internet access service



Prerequisite

The number of xDSL ports is under the control of licenses. Make sure that sufficient licenses are already requested.

Procedure

Step 1 Create a VLAN.

Create smart VLAN 50.

```
huawei(config)#vlan 50 smart
```

Step 2 Configure upstream ports.

Add upstream ports 0/0/1 and 0/0/0 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/0 0
huawei(config)#port vlan 50 0/0 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 0/0 0 0/0 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 **3.7.1 Configuring the ADSL2+ Profile**. 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(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
```

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 MA5616, 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 MA5616HW/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 **3.7.2 Configuring the SHDSL Profile**. 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 0/4/0, 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 0/4
huawei(config-if-shl-0/4)#deactivate 0
huawei(config-if-shl-0/4)#activate 0 3
huawei(config-if-shl-0/4)#alarm-config 0 1
huawei(config-if-shl-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(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
```

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 MA5616, 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 0/4/0, 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 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 2 description MA5616HW/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 **3.7.3.2 Configuring the VDSL2 Profile (TI Mode)**.

1. Configure a VDSL profile. For details, see **3.7.3.1 Configuring the VDSL2 Profile (Normal 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 0/1/0, 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 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#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(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
```

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 MA5616, 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 0/1/0, 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 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5616HW/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 0/4/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
huawei(config)#encapsulation 0/1/0 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 MA5616HW/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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/4
deactivate 0
activate 0 3
alarm-config 0 1
quit
service-port 2 vlan 50 shdsl mode atm 0/4/0 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5616HW/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 0/4/0 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 0/0 0
port vlan 50 0/0 1
link-aggregation 0/0 0 0/0 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 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode atm 0/1/0 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
```

```
service-port desc 3 description MA5616HW/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 0/1/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

9.2 Configuration Example of the Multicast Service (Multicast VLAN Mode)

This topic describes how to configure the multicast service on the MA5616 in multicast VLAN mode.

9.2.1 Configuration Example of the Multicast Video Service (Static Configuration Mode)

This topic describes how to configure the multicast video service if the program in the multicast VLAN is configured statically.

Prerequisites

- Network devices and lines must be in the normal state.
- The multicast source must exist on the network and the IP address of the multicast source must be known.

Context

The program in the multicast VLAN can be configured statically or generated dynamically.

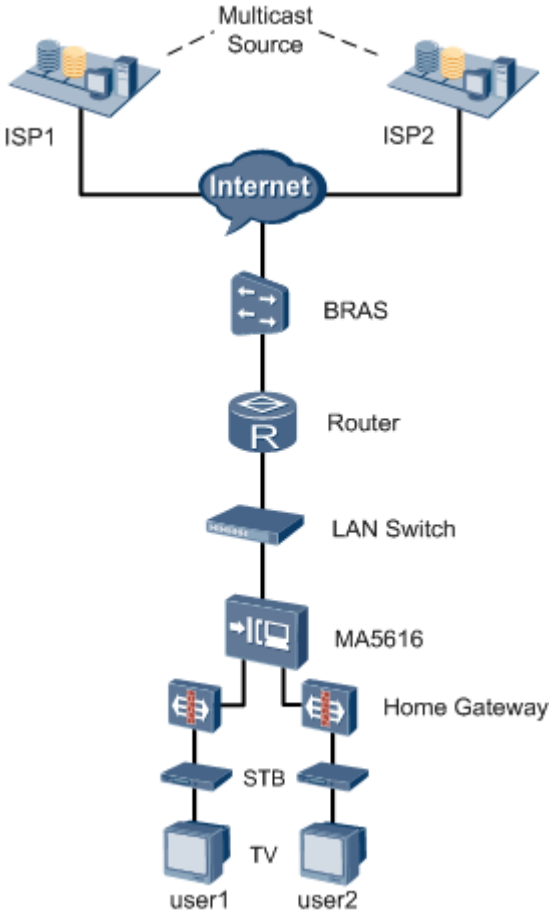
For the static configuration mode:

- The program list needs to be configured for the multicast VLAN. Then, the user can request for the program in this program list.
- The following functions are supported: bandwidth management of the multicast program, user bandwidth management, program preview, and program prejoin.
- The program in the multicast VLAN is configured statically by default.

Networking

Figure 9-5 shows the example network of the multicast service.

Figure 9-5 Example network of the multicast service



Data Plan

Table 9-1 provides the data plan for configuring the multicast service.

Table 9-1 Data plan for configuring the multicast service

Device	Item	Data
ONU: MA5616	Smart VLAN	● VLAN type: Smart VLAN ● VLAN ID: 4002-4005
	Uplink port	0/0/1
	IGMP version	IGMP V3 (default multicast version of the system in multicast VLAN mode)
	Multicast source	There are two multicast sources, namely, ISP 1 and ISP 2. ● ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ● ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2

Device	Item	Data
	Program library	Program in multicast VLAN 4002: Program 1: with IP address 224.1.1.1 and the IP address of the program source is the same as the IP address of ISP 1, namely, 10.10.10.10
		Program in multicast VLAN 4003: Program 2: with IP address 224.1.1.2 and the IP address of the program source is the same as the IP address of ISP 2, namely, 10.10.10.11
	Multicast user	Multicast user 1: ● VDSL2 port: 0/1/0 ● LAN port: 0/3/1 ● Multicast VLAN: 4002
		Multicast user 2: ● VDSL2 port: 0/1/1 ● LAN port: 0/3/2 ● Multicast VLAN: 4003

Procedure

Step 1 Create VLANs and add an uplink port to the VLANs.

```
huawei(config)#vlan 4002-4005 smart
huawei(config)#port vlan 4002-4005 0/0 1
```

Step 2 Configure service ports.

```
huawei(config)#service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-
vlan untagged
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-
vlan untagged
rx-cttr 6 tx-cttr 6
```

Step 3 Configure multicast VLANs and the IGMP mode.

NOTE

The IGMP mode can be configured to IGMP proxy or IGMP snooping according to the requirements. In this example, the IGMP mode is IGMP proxy. If the planned IGMP mode is IGMP snooping, you can configure the IGMP snooping mode by running the **igmp mode snooping** command in multicast VLAN mode.

The IGMP mode can be switched only when the IGMP mode is off.

```
huawei(config)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

Step 4 Configure the multicast uplink port.

```
huawei(config-mvlan4003)#igmp uplink-port 0/0/1
huawei(config-mvlan4003)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp uplink-port 0/0/1
```

Step 5 Configure multicast programs.

NOTE

- In static configuration mode, you can run the **igmp program add** command to add multicast programs. You cannot name a program, instead the system automatically names a program PROGRAM-M, in which M is the index of the added program.
- If the IGMP version of the multicast VLAN is V3, the source IP address of the program in the multicast VLAN must be configured. If the IGMP version of the multicast VLAN is V2, the source IP address of the program in the multicast VLAN cannot be configured.

```
huawei(config-mvlan4002)#igmp program add name program1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp program add name program2 ip 224.1.1.2 sourceip
10.10.10.11
```

Step 6 Configure multicast users.

```
huawei(config-mvlan4003)#btv
huawei(config-btv)#igmp user add service-port 100
huawei(config-btv)#igmp user add service-port 101
huawei(config-btv)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4003)#quit
```

Step 7 Save the data.

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

----End

Result

- User 1 belongs to multicast VLAN 4002 and user 1 can watch the program with IP address 224.1.1.1 provided by ISP1.
- User 2 belongs to multicast VLAN 4003 and user 2 can watch the program with IP address 224.1.1.2 provided by ISP2.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps need to be performed manually and the configuration file cannot be imported directly.

Create VLANs and add an uplink port to the VLANs. This step needs to be performed manually.

```
vlan 4002 to 4005 smart
port vlan 4002 to 4005 0/0 1
```

Create service ports.

```
service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-
cttr 6 tx-cttr 6
service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-vlan untagged rx-
cttr 6 tx-cttr 6
```

Configure multicast VLANs and the IGMP mode. This step needs to be performed manually.

```
multicast-vlan 4002
igmp mode proxy
multicast-vlan 4003
igmp mode proxy
```

Configure the multicast uplink port, multicast programs, and multicast users.

```
igmp uplink-port 0/0/1
multicast-vlan 4002
igmp uplink-port 0/0/1
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
multicast-vlan 4003
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp user add service-port 100
igmp user add service-port 101
multicast-vlan 4002
igmp multicast-vlan member service-port 100
multicast-vlan 4003
igmp multicast-vlan member service-port 101
quit
save
```

9.2.2 Configuration Example of the Multicast Video Service (Dynamic Generation Mode)

This topic describes how to configure the multicast video service if the program matching mode of the multicast VLAN is the dynamic generation mode.

Prerequisites

- Network devices and lines must be in the normal state.
- The multicast source must exist on the network and the IP address range of the multicast program must be known.
- The multicast program must be configured in dynamic generation mode.

Context

The program in the multicast VLAN can be configured statically or generated dynamically.

Dynamic generation mode: A program is dynamically generated according to the program requested by the user.

- In this mode, the program list is not required. You need to configure the IP address range of the program group that can be dynamically generated. The user can request for only the program whose IP address is within this IP address range.
- The following functions are not supported: bandwidth management of the multicast program, user bandwidth management, program preview, and program prejoin.

The program in the multicast VLAN is configured statically by default. Run the **igmp match mode disable** command to configure the dynamic generation mode.

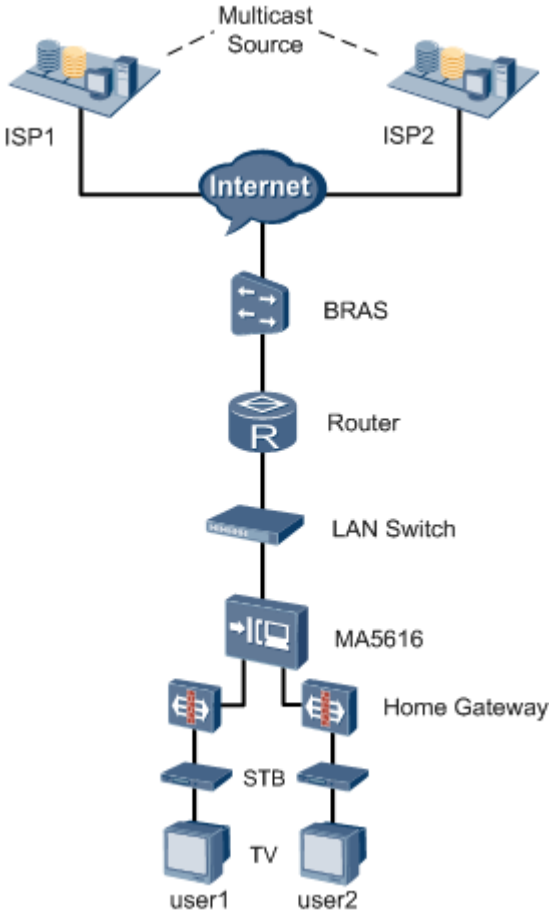
NOTE

The **igmp match mode** command for configuring the mode of the multicast program can be executed only when the IGMP mode is off.

Networking

Figure 9-6 shows the example network of the multicast service.

Figure 9-6 Example network of the multicast service



Data Plan

Table 9-2 provides the data plan for configuring the multicast service.

Table 9-2 Data plan for configuring the multicast service

Device	Item	Data
ONU: MA5616	Smart VLAN	● VLAN type: Smart VLAN ● VLAN ID: 4002-4005
	Uplink port	0/0/1
	IGMP version	IGMP V3 (default multicast version of the system in multicast VLAN mode)
	Multicast source	There are two multicast sources, namely, ISP 1 and ISP 2. ● ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ● ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2

Device	Item	Data
	Program library	Program in multicast VLAN 4002: Program 1: with IP address 224.1.1.1 and the IP address of the program source is the same as the IP address of ISP 1, namely, 10.10.10.10
		Program in multicast VLAN 4003: Program 2: with IP address 224.1.1.2 and the IP address of the program source is the same as the IP address of ISP 2, namely, 10.10.10.11
	Multicast user	Multicast user 1: ● VDSL2 port: 0/1/0 ● LAN port: 0/3/1 ● Multicast VLAN: 4002
		Multicast user 2: ● VDSL2 port: 0/1/1 ● LAN port: 0/3/2 ● Multicast VLAN: 4003

Procedure

Step 1 Create VLANs and add an uplink port to the VLANs.

```
huawei(config)#vlan 4002-4005 smart
huawei(config)#port vlan 4002-4005 0/0 1
```

Step 2 Configure service ports.

```
huawei(config)#service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-
vlan untagged
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-
vlan untagged
rx-cttr 6 tx-cttr 6
```

Step 3 Configure multicast VLANs and the multicast mode.

NOTE

The IGMP mode can be configured to IGMP proxy or IGMP snooping according to the requirements. In this example, the IGMP mode is IGMP proxy. If the planned IGMP mode is IGMP snooping, you can configure the IGMP snooping mode by running the **igmp mode snooping** command in multicast VLAN mode.

The IGMP mode can be switched only when the IGMP mode is off.

```
huawei(config)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

Step 4 Configure the multicast uplink port.

```
huawei(config-mvlan4003)#igmp uplink-port 0/0/1
huawei(config-mvlan4003)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp uplink-port 0/0/1
```

Step 5 Configure multicast programs.

Configure the program in the multicast VLAN in dynamic generation mode, and specify the IP address range of the program that can be requested by the user to 224.1.1.1-224.1.1.2.

NOTE

The execution of the **igmp match mode** command for configuring the mode of the multicast program will cause the user to go offline. Therefore, plan the multicast program mode before configuring the multicast program. This command can be executed only when the IGMP function is disabled.

```
huawei(config-mvlan4002)#igmp match mode disable
huawei(config-mvlan4002)#igmp match group ip 224.1.1.1 to-ip 224.1.1.2
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp match mode disable
huawei(config-mvlan4003)#igmp match group ip 224.1.1.1 to-ip 224.1.1.2
```

Step 6 Configure multicast users.

```
huawei(config-mvlan4002)#btv
huawei(config-btv)#igmp user add service-port 100
huawei(config-btv)#igmp user add service-port 101
huawei(config-btv)#multicast-vlan 4002
huawei(config-mvlan4002)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4002)#multicast-vlan 4003
huawei(config-mvlan4003)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4003)#quit
```

Step 7 Save the data.

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

----End

Result

- User 1 belongs to multicast VLAN 4002 and user 1 can watch the program with IP address 224.1.1.1 provided by ISP1.
- User 2 belongs to multicast VLAN 4003 and user 2 can watch the program with IP address 224.1.1.2 provided by ISP2.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps need to be performed manually and the configuration file cannot be imported directly.

Create VLANs and add an uplink port to the VLANs. This step needs to be performed manually.

```
vlan 4002 to 4005 smart
port vlan 4002 to 4005 0/0 1
```

Create service ports.

```
service-port 100 vlan 4004 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
service-port 101 vlan 4005 vdsl mode ptm 0/1/1 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
```

Configure multicast VLANs and the IGMP mode. This step needs to be performed manually.

```
multicast-vlan 4002
igmp mode proxy
multicast-vlan 4003
igmp mode proxy
```

Configure the multicast uplink port, multicast programs, and multicast users.

```
igmp uplink-port 0/0/1
multicast-vlan 4002
igmp uplink-port 0/0/1
igmp match mode disable
igmp match group ip 224.1.1.1 to-ip 224.1.1.2
multicast-vlan 4003
igmp match mode disable
igmp match group ip 224.1.1.1 to-ip 224.1.1.2
btv
igmp user add service-port 100
igmp user add service-port 101
multicast-vlan 4002
igmp multicast-vlan member service-port 100
multicast-vlan 4003
igmp multicast-vlan member service-port 101
quit
save
```

9.3 Configuration Example of the VoIP Service

This topic describes how to configure the VoIP service based on the H.248 or SIP protocol.

9.3.1 Configuration Example of the VoIP PSTN Service (Based on the H.248 Protocol)

This topic describes how to configure the VoIP service based on the H.248 protocol.

Service Requirements

In an office, the MA5616 that adopts the H.248 protocol is newly deployed. Data plan and configuration, however, are not performed on the MGC (softswitch) connected to the MA5616. The following voice services are required:

- POTS service needs to be provided for phone 0-phone 31 for 32 users.
- Polarity reversal charging is adopted.

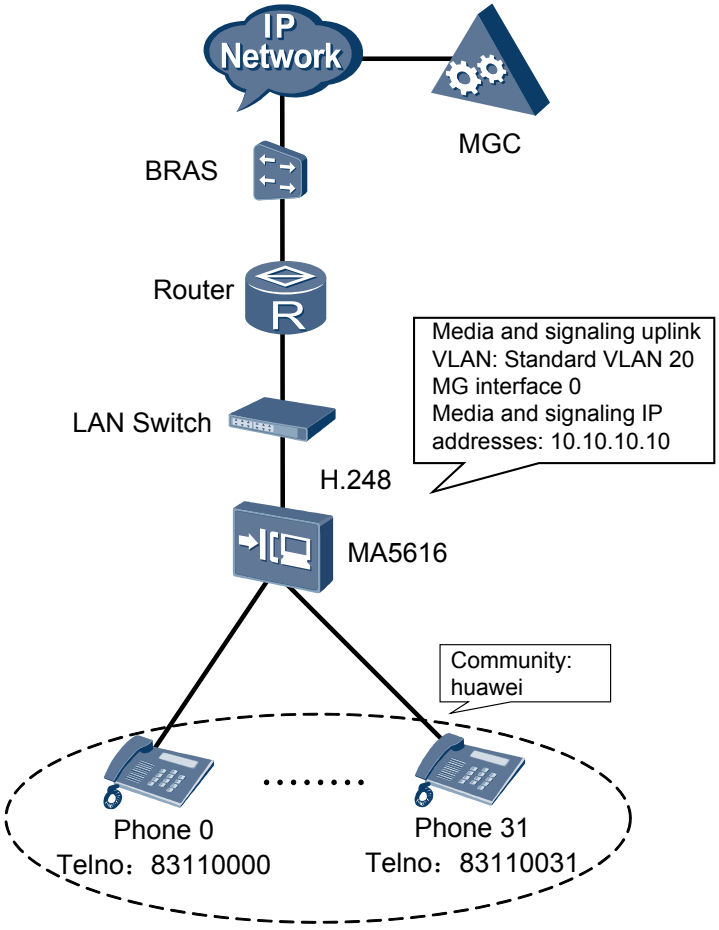
Prerequisite

- According to the actual network, a route from the MA5616 to the MGC must be configured to ensure that the MA5616 and the MGC are reachable to each other.
- POTS service board ASRB must be inserted into the planned slot, and the RUN ALM indicator on the board must be green and must be on for 1s and off for 1s repeatedly.

Networking

Figure 9-7 shows the example network of the VoIP service based on the H.248 protocol.

Figure 9-7 Example network of the VoIP service based on the H.248 protocol



Data Plan

After the service requirements are further confirmed and analyzed with engineers of the office, the data plan is made by considering the interconnection with the MGC and according to the data plan described in **7.1 Configuring the VoIP PSTN Service (Based on the H.248 Protocol)**. **Table 9-3** provides the data plan for configuring the VoIP service based on the H.248 protocol.

Table 9-3 Data plan for configuring the VoIP service based on the H.248 protocol

Item			Data
MG interface data (The data configuration must be consistent with the data	Parameters of the media stream and signaling stream	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the voice service. In this section, standard VLAN 20 is adopted.
		Media and signaling upstream port	0/0/1

Item			Data
configuration on the MGC.)		Media IP address and signaling IP address	These two IP addresses are both 10.10.10.10.
		Default IP address of the MG	Confirmed with the engineers of this office, the IP address of the next hop from the MA5616 to the MGC is 10.10.10.1.
	Attribute parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be started if these parameters are not configured.	MG interface ID	0, indicating that the negotiation is based on the profile
		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 network of the office does not support dual homing. 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 MA5616.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	The **text** coding mode is adopted.
		Transmission mode of the MG interface	UDP
		Domain name of the MG interface	The message ID (MID) adopts the IP address (default), and may not be configured with a domain name.
		Device name of the MG interface	The MID adopts the IP address (default), and may not be configured with a device name.
		Start negotiation version of the H.248 protocol for the MG interface	0
	Digitmap of an MG Interface		Special applications such as emergency calls and emergency standalone are not configured. Therefore, the digitmap is not configured.

Item			Data
	Software Parameters of an MG Interface		According to the Context in **Software Parameters of an MG Interface** and confirmed with the engineers of the office, the default configuration can meet the service requirements. Therefore, the software parameters are not configured.
	Ringing Mode of an MG Interface		Confirmed with the engineers of the office, the value of the ringing parameter (corresponding to the users) specified 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.
	TID Format of an MG Interface		To differentiate users by terminal ID (TID), the engineers of the office require that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the slot ID/shelf 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.
Voice service data (The data configuration must be consistent with the data configuration on the MGC.)	Slot that houses the voice service board		The user is accessed through the 0/3 port on the ASRB board.
	User Data	Phone number	The emergency standalone is not supported. Therefore, you need not configure the phone number when adding a user. Phone numbers allocated by the MGC for phone 0-phone 31 are 83110000-83110031. **NOTE** Generally, No telephone number (namely, parameter telno) is configured on the MG, because telephone numbers are specified by the MGC.
		TID	The terminal layering is supported. Therefore, the TID need not be allocated manually.

Item			Data
		User priority	Users are common users, and the user priority uses the default priority, namely, cat3.
		User type	Users are common users, and the user type uses the default user type, namely, DEL.
	System Parameters		According to the Context in **7.1.2.2 (Optional) Configuring the System Parameters** and confirmed with the engineers of the office, the default configuration can meet the service requirements. Therefore, the system parameters are not configured.
	Overseas Parameters		According to the Context in **7.1.2.3 (Optional) Configuring the Overseas Parameters** and confirmed with the engineers of the office, the default configuration can meet the service requirements. Therefore, the overseas parameters are not configured.
	Local Digitmap **CAUTION** By default, these parameters need not be configured if the H.248 protocol is used. You can configure these parameters according to the requirements.	Digitmap name	huawei
		Digitmap type	Only the normal digitmap is supported if the H.248 protocol is used.
		Digitmap body	Plan this parameter according to the prefix of the local phone number. In this example, the ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx) digitmap body is used.
	Attributes of a PSTN Port		The polarity reversal charging is required for the service. Therefore, you need to configure the PSTN port to which the user belongs so that the PSTN port supports the polarity reversal impulse. The other attributes of the PSTN port need not be modified.

Item		Data
	Attributes of the Ringing Current	The ringing attribute need not be configured unless otherwise specified.

Procedure

Step 1 Configure the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/0/1 to the VLAN, and configure the IP address of the L3 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 0/0 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
```

Step 2 Configure the media and signaling IP address pools.

Add the IP address of the VLAN L3 interface configured in the previous step to the media and signaling IP address pools respectively. Thus, 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-if-vlanif20)#quit
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
```

Step 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-voip)#quit
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
start-negotiate-version 0
```

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 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 template of the PSTN user on MG interface 0.

Configure the TID generation mode. According to the data plan, the terminal prefix of the PSTN user needs to be configured to **huawei**, and the TID template adopts layering template 6.

CAUTION

The MA5616 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 Start 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 manners (see Parameter Description of the **reset** command). For a newly configured MG interface, start the MG interface in a cold start manner.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

Step 7 Query the running status of the MG interface.

After the MG interface is interconnected with the MGC successfully, the MG interface needs to be in the normal state, indicating that the MG interface works in the normal state.

```
huawei(config-if-h248-0)#quit
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
  ------------------------------------------------------------------------------
```

Step 8 Confirm the service board.

Confirm the ASRB 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 phone 0-phone 31 so that the users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0
```

Step 10 Configure the local digitmap.

After the configuration, the MA5616 matches the phone number according to the local digitmap if the MGC does not send the detailed digitmap to the MA5616.

```
huawei(config-esl-user)#quit
huawei(config)#local-digitmap add huawei normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|
13xxxxxxxxx|0xxxxxxxxx)
```

Step 11 Configure the polarity reversal charging function.

Configure the physical attributes of the PSTN port to which the user belongs to support the polarity reversal pulse, so that the user can support the polarity reversal charging.

```
huawei(config)#pstnport
```

```
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
```

Step 12 Save the data.

```
huawei(config-pstnport)#quit
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 service can be provided normally. In normal cases, phone 0-phone 31 can call each other.

- The calling party can hear the dial tone after picking up the phone off the hook.
- 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 ringback tone.

  NOTE

  When the calling party calls the number of a specified user, if the phone of the specified user does not ring but the phone of another user connected to the MA562X rings, and the calling party hears the ringback tone, check whether the MGC is configured with the call forwarding service, causing the line cross.

  - If the MGC is configured with the call forwarding service, cancel the call forwarding service on the MGC.
  - If the MGC is not configured with the call forwarding service, contact Huawei technical support engineer to handle the fault.
- The calling party and the called party can communicate with each other normally.
- After the called party places the phone on the hook, the calling party can hear the busy tone.

Configuration File

The following part 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 0/0 0
interface vlanif 20
ip address 10.10.10.10 24
```

Configure the media and signaling IP address pools.

```
quit
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
```

Add an MG interface and then configure the attributes of the MG interface. An MG interface must be added manually and the configuration file cannot be imported directly.

```
quit
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 start-negotiate-version 0
```

Configure the ringing mapping of the MG interface.

```
mg-ringmode add 0 0 4
```

Configure the TID template of the PSTN user on the MG interface.

```
tid-format pstn prefix huawei template 6
```

An MG interface must be started manually and the configuration file cannot be imported directly.

```
reset coldstart
```

Query the running status of the MG interface.

```
quit
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
```

Configure the local digitmap.

```
quit
local-digitmap add huawei normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|
0xxxxxxxxx)
```

Configure the polarity reversal charging function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse enable
```

Save the data.

```
quit
save
```

9.3.2 Configuration Example of the VoIP PSTN Service (Based on the SIP Protocol)

This topic describes how to configure the VoIP PSTN service based on the SIP protocol.

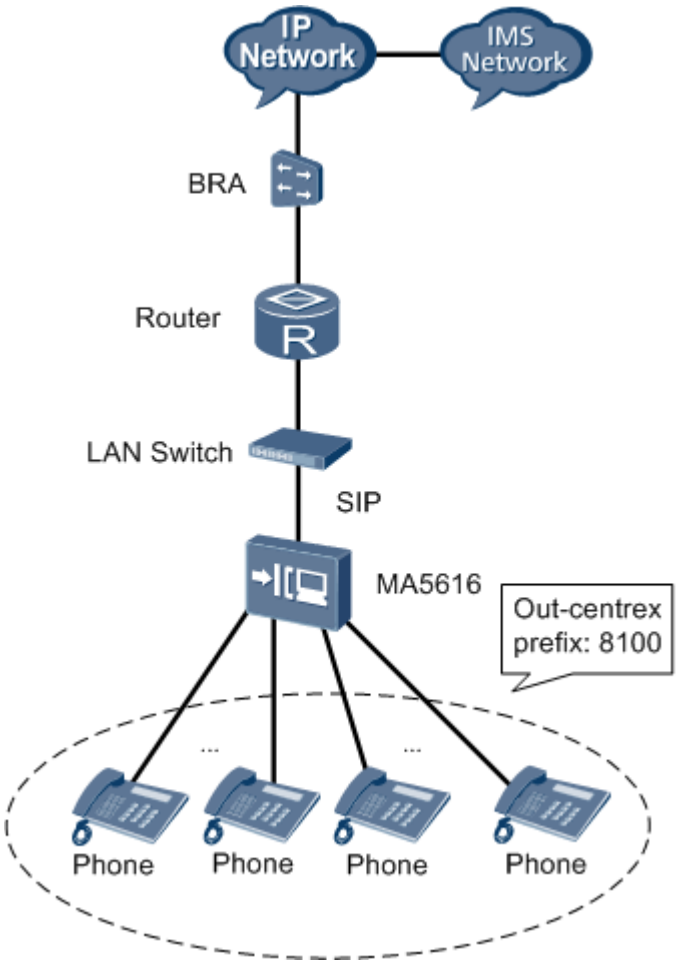
Prerequisites

- The voice service board ASRB must be installed in the specified slot.
- The SIP interface must be configured. For how to configure the SIP interface, see **7.2.1 Configuring the SIP Interface**.
- The PSTN user data corresponding to the SIP interface must be configured on the IMS.

Networking

Figure 9-8 shows the example network of the VoIP PSTN service based on the SIP protocol.

Figure 9-8 Example network of the VoIP PSTN service based on the SIP protocol



Data Plan

Run the **display system parameters** and **display oversea parameters** commands to query the system parameters and overseas parameters. If the parameter settings do meet the requirements, run the **system parameters** and **oversea parameters** commands to set the parameters to the required values.

In this example, the MA5616 is used in China. The default configurations of system parameters and overseas parameters can meet the standard and application requirements. Therefore, you need not configure these parameters.

Table 9-4 provides the data plan for configuring the VoIP PSTN service based on the SIP protocol.

Table 9-4 Data plan for configuring the VoIP PSTN service based on the SIP protocol

Item		Data
SIP interface	SIP interface ID	0
Local digitmap	Digitmap name	huawei0 and huawei1

Item		Data
	Digitmap type	The digitmap type of huawei0 is normal. The digitmap type of huawei1 is second-centrex. **NOTE** The parameters of the emergency digitmap use default values.
	Digitmap body	The digitmap body of huawei0 is ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S). The digitmap body of huawei1 is (8100).
Voice service board ASRB	Slot that houses the board	0/3
Data of the PSTN users in slot 0/3	Numbers of phone 0-phone 31	83110000-83110031
	User priority	The priority of phone 0 is Cat2 and the priority of phone 1-phone 31 is Cat3 (default priority).
	User type	The type of phone 0 is DEL and the type of phone 1-phone 31 is Payphone.
	PSTN port attribute	Phone 1-phone 31 support polarity reversal impulse.

Procedure

Step 1 Configure the local digitmap.

Configure the local call digitmap and two-stage dialing digitmap. The parameters of the emergency digitmap use the default values.

```
huawei(config)#local-digitmap add huawei0 normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|
13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)
huawei(config)#local-digitmap add huawei1 second-centrex (8100)
```

Step 2 Configure the PSTN user data.

1. Configure the data of the PSTN users (phone 0-phone 31) in slot 0/3.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/31 0 telno 83110000
   ```

2. Configure the priority of the PSTN user in slot 0/3/0 to Cat2.

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

3. Configure the type of the PSTN user in slot 0/3.

   ```
   huawei(config-esl-user)#sippstnuser attribute batset 0/3/1 0/3/31 potslinetype
   PayPhone
   ```

Step 3 Configure the PSTN port attribute.

Configure the PSTN port in slot 0/3 so that the port supports polarity reversal impulse.

```
huawei(config-esl-user)#quit
huawei(config)#pstnport
```

```
huawei(config-pstnport)#pstnport attribute batset 0/3/1 0/3/31 reverse-pole-pulse
enable
```

Step 4 Save the data.

```
huawei(config-pstnport)#quit
huawei(config)#save
```

----End

Result

After the configuration, phone 0-phone 31 can call each other.

- The calling party can hear the dial tone after picking up the phone off the hook.
- 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 ringback tone.

  NOTE

  When the calling party calls the number of a specified user, if the phone of the specified user does not ring but the phone of another user connected to the MA5616 rings, and the calling party hears the ringback tone, check whether the IMS is configured with the call forwarding service, causing the line cross.

  - If the IMS is configured with the call forwarding service, cancel the call forwarding service on the IMS.
  - If the IMS is not configured with the call forwarding service, contact Huawei technical support engineer to handle the fault.
- The calling party and the called party can communicate with each other normally.
- After the called party places the phone on the hook, the calling party can hear the busy tone.

Configuration File

The following part 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 local digitmap.

```
local-digitmap add huawei0 normal ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|
13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)
local-digitmap add huawei1 second-centrex (8100)
```

Configure the PSTN user data.

```
esl user
sippstnuser batadd 0/3/0 0/3/31 0 telno 83110000
sippstnuser attribute set 0/3/0 priority cat2
sippstnuser attribute batset 0/3/1 0/3/31 potslinetype PayPhone
```

Configure the PSTN port attribute.

```
quit
pstnport
pstnport attribute batset 0/3/1 0/3/31 reverse-pole-pulse enable
```

Save the data.

```
quit
save
```

9.3.3 Configuration Example of the VoIP ISDN BRA Service

When the H.248 protocol is used, the MA5616 can access the ISDN BRA service through the DSLD service board. Then, the service is sent upstream to the IP network through the control

board, thus implementing the ISDN BRA service. The ISDN BRA service on the MA5616 can be supported only by the H.248 protocol.

Prerequisites

- The devices on the network must be connected properly and must work in the normal state.
- The MA5616 must use the H.248 protocol to communicate with the MGC.
- The data on the MGC side must be configured correctly.
- NT1 must be connected properly and must work in the normal state.

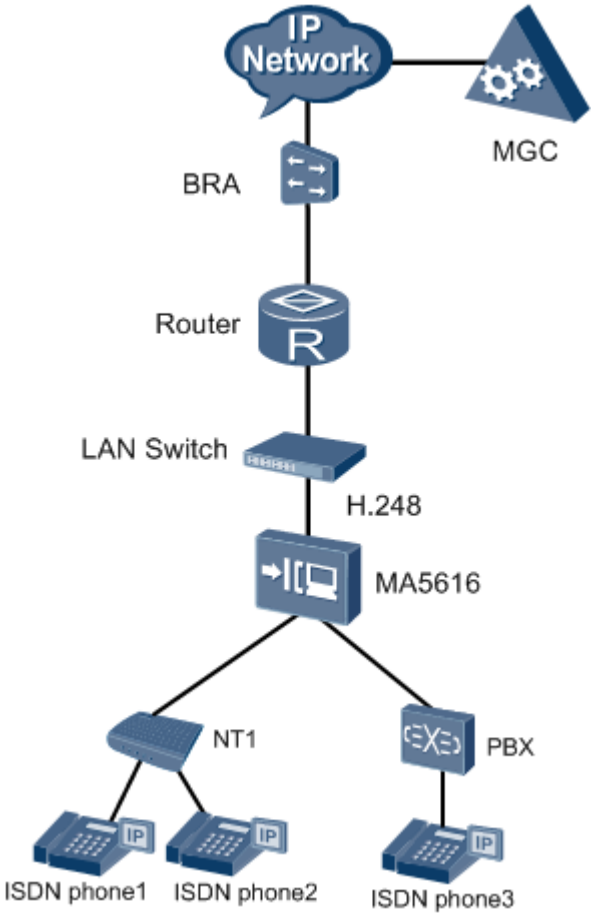
Context

- When the MG interface does not support the terminal layering, the terminal ID must be configured and must be different from the terminal ID of an existing PSTN user.
- When the MG interface supports terminal layering, the terminal ID cannot be configured, and the system automatically allocates the terminal ID according to the TID profile configured for the interface of the PSTN user.
- You can run the **display tid-format** to query the TID profile to which various users under the MG interface are bound, and then run the **display tid-template** command to check whether the TID profile supports the layering configuration. Hence, you can check whether the user supports terminal layering.
  - If the parameter list of the TID profile includes only keyword "G", it indicates that the TID profile is used by the non-layering users. Users bound with this profile do not support terminal layering.
  - If the parameter list of the TID profile includes only keywords "F", "S", "P", "B" ("B" is unavailable for PSTN users), it indicates that the TID profile is used by the layering users. Users bound with this profile support terminal layering.

Networking

Figure 9-9 shows the example network for configuring the ISDN BRA service.

Figure 9-9 Example network for configuring the ISDN BRA service



Data Plan

Table 9-5 provides the data plan for configuring the ISDN BRA service.

Table 9-5 Data plan for configuring the ISDN BRA service

Item		Data
Parameters of the media stream and signaling stream	IP address and mask of the VLAN L3 interface	10.13.4.116/16
	IP address of the media stream and signaling stream	10.13.4.116
	Upstream interface of the media stream and signaling stream	0/0/1
	Upstream VLAN of the media stream and signaling stream	VLAN ID: 10

Item		Data
	Default media gateway of the MG interface	10.13.1.1
TID profile	ID of the TID profile used by the ISDN BRA user	2 (default, no configuration is required)
	TID terminal prefix used by the ISDN BRA user	A (default, no configuration is required)
Static route from the MG to the MGC	IP address of the destination network segment	10.14.0.0
	IP address of the gateway	10.13.1.1
Attribute parameters of the MG interface	MG interface ID	0
	Coding type of the MG interface	text
	Protocol supported by the MG interface	H.248
	Signaling port ID of the MG interface	2944
	Media/Signaling IP address of the MG interface	10.13.4.116
	Default media gateway of the MG interface	10.13.1.1
	IP address of the primary MGC to which the MG interface belongs	10.14.1.2
	Port ID of the primary MGC to which the MG interface belongs	2944
	Transmission mode of the MG interface	UDP
	Start negotiation version of the H.248 protocol for the MG interface	2
	Domain name	MA5616.com
Voice service board DSLD	Slot that houses the board	0/4
IUA link parameters	ID of the IUA link set	0
	IUA link ID	0

Item		Data
	Local port ID	1401
	Local IP address	10.13.4.116/16
	MGC port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
BRA user data	ISDN phone1 and ISDN phone2	● Shelf/slot/port ID of the BRA user: 0/4/0 ● Phone number: 83110001 ● Working mode: point to multi-point ● Terminal ID: 2 ● IUA interface ID: 0 ● Priority of the user: Cat3 (default)
	ISDN phone3	● Shelf/slot/port ID of the BRA user: 0/4/1 ● Phone number: 83110002 ● Working mode: point to point ● Terminal ID: 4 ● IUA interface ID: 2 ● Priority of the user: Cat1 **NOTE** In the point to point mode, the terminal endpoint identifier (TEI) of the ISDN BRA digital phone is always 0.

Procedure

Step 1 Add a DSLD service board.

```
huawei(config)#board add 0/4 H832DSLD
  0 frame 4 slot board added successfully
```

Step 2 Create a VLAN and configure the VLAN L3 interface.

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.13.4.116 16
huawei(config-if-vlanif10)#quit
```

Step 3 Add the uplink port to the VLAN.

```
huawei(config)#port vlan 10 0/0 1
```

Step 4 Configure the media/signaling IP address.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.13.4.116 10.13.1.1
huawei(config-voip)#ip address signaling 10.13.4.116
```

NOTE

Ensure that the to-be-configured media/signaling IP address of the MG interface must exist in the corresponding address pool. You can run the **display ip address** command to query the in formation about the media IP address pool or the signaling IP address pool.

Step 5 Configure the static route.

```
huawei(config-voip)#quit
huawei(config)#ip route-static 10.14.0.0 16 10.13.1.1
```

Step 6 Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 7 Configure the attributes of the MG interface.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.13.4.116 mgport 2944 code
text transfer udp MIDType domainName domainName MA5616.com primary-mgc-ip1
10.14.1.2
 primary-mgc-port 2944 mg-media-ip1 10.13.4.116 start-negotiate-version 2
```

Step 8 Reset the MG interface.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

Step 9 Configure the working mode of the ISDN BRA port.

```
huawei(config-if-h248-0)#quit
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/4/0 workmode p2mp
huawei(config-braport)#braport attribute set 0/4/1 activemode stable-active
workmode p2p
```

NOTE

In the point to point mode, the L1 **activemode** of the ISDN BRA port must be set to **stable-active** to make the configuration take effect.

Step 10 Add an IUA link set and IUA links.

```
huawei(config-braport)#quit
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 0
huawei(config-sigtran)#iua-link add 0 0 1401 10.13.4.116 1400 10.14.1.2
```

Step 11 Add an ISDN BRA user and configure the data.

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/4/0 0 0 interfaceid 0 terminalid 2 priority
cat3 telno 83110001
 Are you sure to configure the working mode of the DSL board to normal and reset
 the board automatically? (y/n)
[n]:y
huawei(config-esl-user)#mgbrauser add 0/4/1 0 0 interfaceid 2 terminalid 4 pr
iority cat1 telno 83110002
```

Step 12 Save the data.

```
huawei(config-esl-user)#quit
huawei(config)#save
```

----End

Result

- ISDN phone1 and ISDN phone2 can communicate with ISDN phone3 by dialing number 83110002.

- When ISDN phone3 dials number 83110001, ISDN phone1 and ISDN phone2 can hear the ringing tone at the same time. In addition, ISDN phone1 and ISDN phone2 can communicate with ISDN phone3 at the same time.

Configuration File

The following part describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported at a time.

Add the DSLD service board.

```
board add 0/4 H832DSLD
```

Create a service VLAN and configure its L3 interface.

```
vlan 10
interface vlanif 10
ip address 10.13.4.116 16
quit
```

Add an uplink port to the service VLAN.

```
port vlan 10 0/0 1
```

Configure the media IP address pool and the signaling IP address pool.

```
voip
ip address media 10.13.4.116 10.13.1.1
ip address signaling 10.13.4.116
```

Configure a static route.

```
quit
ip route-static 10.14.0.0 16 10.13.1.1
```

Add an MG interface.

```
interface h248 0
```

Configure the attributes of the MG interface.

```
if-h248 attribute mgip 10.13.4.116 mgport 2944 code text transfer udp MIDType
domainName domainName MA5616.com primary-mgc-ip1 10.14.1.2 primary-mgc-port 2944
mg-media-ip1 10.13.4.116 start-negotiate-version 2
```

Enable the MG interface.

```
reset coldstart
```

Configure the working mode of the ISDN BRA port.

```
quit
braport
braport attribute set 0/4/0 workmode p2mp
```
braport attribute set 0/4/1 activemode stable-active workmode p2p

Add an IUA link set and IUA links.

```
quitsigtran
iua-linkset add 0
iua-link add 0 0 1401 10.13.4.116 1400 10.14.1.2
```

Add an ISDN BRA user and configure the data.

```
quit
esl user
```

```
mgbrauser add 0/4/0 0 0 interfaceid 0 terminalid 2 priority cat3 telno 83110001
mgbrauser add 0/4/1 0 0 interfaceid 2 terminalid 4 priority cat1 telno 83110002
```

Save the data.

```
quit
save
```

9.4 Configuration Example of the VLAN Stacking Wholesale Service

This topic describes the VLAN stacking wholesale service and how to configure the VLAN stacking wholesale service on the MA5616.

9.4.1 Configuration Example of the VLAN Stacking Wholesale Service

This topic describes how to configure the wholesale service so that the service provided by the ISP can be delivered promptly to a specified user group.

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 control board and the corresponding service boards must be in the normal state.

Service Requirements

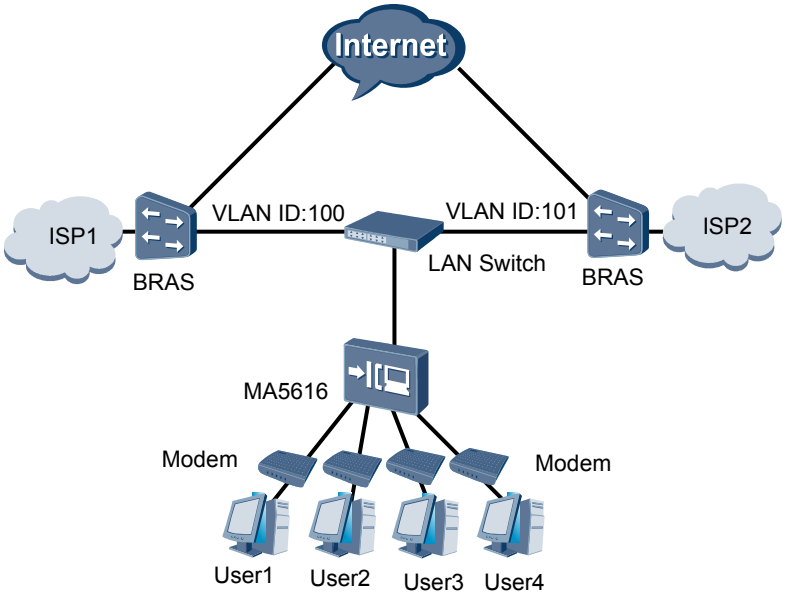
- The user accesses the Internet through the PPPoE dialup.
- The device adds an outer VLAN tag to user packets to identify ISPs, and adds an inner VLAN tag to identify users.

Networking

Figure 9-10 shows an example network for configuring the VLAN stacking wholesale service.

Users 1 and 2, and users 3 and 4 obtain the broadband service from different ISPs. The MA5616 supports the VLAN stacking function to implement the multi-ISP wholesale service. The device adds an outer VLAN tag to user packets to identify ISPs and adds an inner VLAN tag to identify users. Then, the device forwards the packets to the L2 network. The L2 switch forwards the user packets to a specified ISP BRAS based on the outer VLAN tags. The ISP BRAS removes the outer VLAN tags and identifies the user based on the inner VLAN tags. After being authenticated by the ISP BRAS, the users can obtain the services provided by the ISP.

Figure 9-10 Example network for configuring the VLAN stacking wholesale service



Data Plan

Table 9-6 provides the data plan for configuring the VLAN stacking wholesale service.

Table 9-6 Data plan for configuring the VLAN stacking wholesale service

Item	Data
ISP 1 user group	Uplink port: 0/0/1
	Network-side VLAN ID (outer VLAN tag): 100
	VLAN attribute: stacking VLAN
	User 1: ● Access port: 0/1/0 ● Inner VLAN tag: 11
	User 2: ● Access port: 0/1/1 ● Inner VLAN tag: 12
ISP 2 user group	Uplink port: 0/0/1
	Network-side VLAN ID (outer VLAN tag): 101
	VLAN attribute: stacking VLAN
	User 3: ● Access port: 0/1/2 ● Inner VLAN tag: 11

Item	Data
	User 4: ● Access port: 0/1/3 ● Inner VLAN tag: 12

Procedure

Step 1 Create VLANs.

Network-side VLAN IDs are 100 and 101, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 100-101 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
```

Step 2 Set the VLAN attribute to stacking VLAN.

NOTE

You can run the **stacking outer-ethertype** command to set the type of outer Ethernet protocol supported by VLAN stacking on the MA5616. You can also run the **stacking inner-ethertype** command to set the type of inner Ethernet protocol supported by VLAN stacking on the MA5616. To ensure that Huawei device is interconnected with the device of other vendors, the type of the inner/outer Ethernet protocol must be the same as that of the interconnect device.

```
huawei(config)#vlan attrib 100-101 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
```

Step 3 Add an uplink port to the VLAN.

Add uplink port 0/0/1 to VLAN 100 and VLAN 101.

```
huawei(config)#port vlan 100-101 0/0 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
  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 service ports to VLANs.

Create service ports for users 1, 2, 3, and 4, and then add the service ports to VLAN 100 and VLAN 101.

```
huawei(config)#service-port 1 vlan 100 vdsl mode ptm 0/1/0 multi-service user-encap
pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan  100 vdsl mode ptm 0/1/1 multi-service user-
encap pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 3 vlan 101 vdsl mode ptm 0/1/2 multi-service user-encap
pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#service-port 4 vlan 101 vdsl mode ptm 0/1/3 multi-service user-encap
```

```
pppoe
rx-cttr 6 tx-cttr 6
```

Step 5 Set the inner VLAN tag.

The inner VLAN tag is used to identify the user. An inner VLAN tag under the same ISP must be unique. The VLAN tags under different ISPs can be the same with each other.

```
huawei(config)#display service-port all
{ <cr>|sort-by<K>||<K> }:

  Command:
          display service-port all
  ------------------------------------------------------------------------
  INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX  TX STATE
        ID   ATTR     TYPE                    TYPE  PARA
  ------------------------------------------------------------------------
      0  100 stacking vdl  0/1/ 0  -    -     encap pppoe       6   6 up
      1  100 stacking vdl  0/1/ 1  -    -     encap pppoe       6   6 up
      2  101 stacking vdl  0/1/ 2  -    -     encap pppoe       6   6 up
      3  101 stacking vdl  0/1/ 3  -    -     encap pppoe       6   6 up
  ------------------------------------------------------------------------
   Total : 4  (Up/Down :    4/0)
huawei(config)#stacking label service-port 1 11
huawei(config)#stacking label service-port 2 12
huawei(config)#stacking label service-port 3 11
huawei(config)#stacking label service-port 4 12
```

NOTE

In the actual configuration, the index of the traffic stream may vary according to the number of traffic streams in the system. You only need to ensure that the actual index corresponds to the inner VLAN tag.

Step 6 Save the data.

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

----End

Result

- After being authenticated by the ISP 1 BRAS, users 1 and 2 can obtain the services provided by ISP 1.
- After being authenticated by the ISP 2 BRAS, users 3 and 4 can obtain the services provided by ISP 2.

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.

Create VLANs.

```
vlan 100 to 101 smart
```

Set the VLAN attribute.

```
vlan attrib 100 to 101 stacking
```

Add an uplink port to VLANs.

```
port vlan 100 to 101 0/0 1
```

Add service ports to VLANs.

```
vlan 100 to 101 smart
vlan attrib 100 to 101 stacking
```

```
port vlan 100 to 101 0/0 1
service-port 1 vlan 100 vdsl mode ptm 0/1/0 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 2 vlan 100 vdsl mode ptm 0/1/1 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 3 vlan 101 vdsl mode ptm 0/1/2 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 4 vlan 101 vdsl mode ptm 0/1/3 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
```

Set inner VLAN tag.

```
stacking label service-port 1 11
stacking label service-port 2 12
stacking label service-port 3 11
stacking label service-port 4 12
```

9.4.2 Configuration Example of the VLAN ID Extension Service

This topic describes how to configure the VLAN ID extension for increasing the number of users that can be identified according to the VLAN ID by the BRAS.

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 control board and the involved service boards must be in the normal state.

Service Requirements

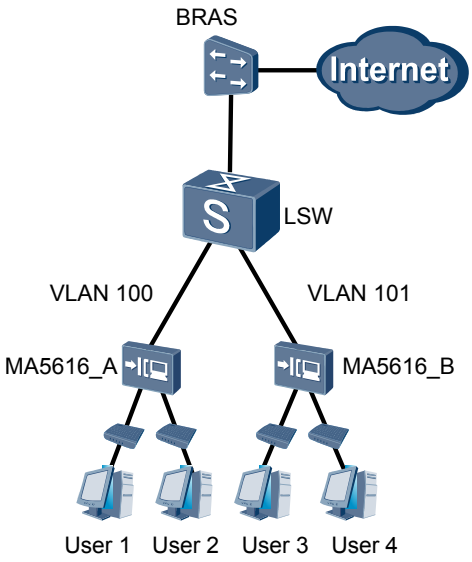
- The Internet access service is deployed on the network.
- Two VLAN IDs are allocated on the BRAS to identify four access users.
- The MA5616 is used on the GE upstream transmission network.

Networking

Figure 9-11 shows the example network for configuring the VLAN ID extension.

Broadband users through multiple MA5616s are authenticated on a BRAS to obtain the broadband service provided by the carrier. The BRAS supports the user identification through L2 VLAN. The outer VLAN tag identifies the MA5616 that accesses users, and the inner VLAN tag identifies the users of the device.

Figure 9-11 Example network for configuring the VLAN ID extension



Data Plan

Table 9-7 provides the data plan for configuring the VLAN ID extension.

Table 9-7 Data plan for configuring the VLAN ID extension

Item	Data
MA5616_A	Uplink port: 0/0/1
	Upstream VLAN ID (outer VLAN tag): 100 VLAN attribute: Stacking VLAN
	User 1: ● Access port: 0/1/2 ● Inner VLAN tag: 11
	User 2: ● Access port: 0/1/3 ● Inner VLAN tag: 12
MA5616_B	Uplink port: 0/0/1
	Upstream VLAN ID (outer VLAN tag): 101 VLAN attribute: Stacking VLAN
	User 3: ● Access port: 0/1/2 ● Inner VLAN tag: 11

Item	Data
	User 4: ● Access port: 0/1/3 ● Inner VLAN tag: 12

Procedure

- The procedure for configuring the VLAN ID extension on MA5616_A is as follows:
  1. Create a VLAN.

     ```
     huawei(config)#vlan 100 smart
     ```

  2. Set the VLAN attribute to stacking VLAN.

     ```
     huawei(config)#vlan attrib 100 stacking
     ```

  3. Add an uplink port to the VLAN.

     ```
     huawei(config)#port vlan 100 0/0 1
     ```

  4. Add service ports to the VLAN.

     ```
     huawei(config)#service-port vlan 100 vdsl mode ptm 0/1/2 multi-service
     user-encap pppoe
     rx-cttr 6 tx-cttr 6
     huawei(config)#service-port vlan 100 vdsl mode ptm 0/1/3 multi-service
     user-encap pppoe
     rx-cttr 6 tx-cttr 6
     ```

  5. Set the inner VLAN tag.

     ```
     huawei(config)#display service-port all

     { <cr>|sort-by<K>||<K> }:

       Command:
               display service-port all

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

       INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX  TX
     STATE
             ID   ATTR     TYPE                    TYPE
     PARA

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

           0  100 common   vdl  0/1 /2  -    -     encap pppoe       6   6
     up
           1  100 common   vdl  0/1 /3  -    -     encap pppoe       6   6
     up

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

        Total : 2  (Up/Down :    2/0)
     huawei(config)#stacking label service-port 0 11
     huawei(config)#stacking label service-port 1 12
     ```

     NOTE

     In the actual configuration, the index of the traffic stream may vary according to the number of traffic streams in the system. You only need to ensure that the actual index corresponds to the inner VLAN tag.

  6. Save the data.

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

- The procedure for configuring the VLAN ID extension on MA5616_B is as follows:

  The configuration procedure of MA5616_B is the same as the configuration procedure of MA5616_A. The only difference lies in the upstream VLAN ID. Hence, it is not described here.

----End

Result

After being authenticated by the BRAS, the users on MA5616_A and MA5616_B can access the Internet.

Two users of the MA5616 can be identified according to one outer VLAN tag. In this manner, the number of the access user based on one VLAN tag is increased.

Configuration File

Configuration file of MA5616_A

Create a VLAN.

```
vlan 100 smart
```

Set the VLAN attribute to stacking VLAN.

```
vlan attrib 100 stacking
```

Add an uplink port to the VLAN.

```
port vlan 100 0/0 1
```

Add service ports to the VLAN.

```
service-port 0 vlan 100 vdsl mode ptm 0/1/2 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
service-port 1 vlan 100 vdsl mode ptm 0/1/3 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
```

Set the inner VLAN tag.

```
stacking label service-port 0 11
stacking label service-port 1 12
```

Configuration file of MA5616_B

Create a VLAN.

```
vlan 101 smart
```

Set the VLAN attribute to stacking VLAN.

```
vlan attrib 101 stacking
```

Add an uplink port to the VLAN.

```
port vlan 101 0/0 1
```

Add service ports to the VLAN.

```
service-port 0 vlan 101 vdsl mode ptm 0/1/2 multi-service user-encap pppoe  rx-cttr
```

```
6
tx-cttr 6
service-port 1 vlan 101 vdsl mode ptm 0/1/3 multi-service user-encap pppoe  rx-cttr
6
tx-cttr 6
```

Set the inner VLAN tag.

```
stacking label service-port 0 11
stacking label service-port 1 12
```

9.5 Configuring the Triple Play Service

This topic describes the triple play service and how to configure the triple play service on the MA5616 on the GE upstream transmission network.

9.5.1 Configuration Example of the Triple Play Service - Single PVC for Multiple Services Based on the User-Side VLAN

This topic describes how to configure the triple play service in the single-PVC for multiple services mode based on the user-side VLAN.

Prerequisites

Before configuring the triple play service, make sure that:

- The network devices and lines are in the normal state.
- The CPE is already configured (the CPE supports different VLANs for different services).
- All boards of the device run in the normal state.
- The VDSL2 line template and alarm template that are bound to the port are already configured. For details on the configuration procedure, see **3.7.3 Configuring the VDSL2 Profile**.

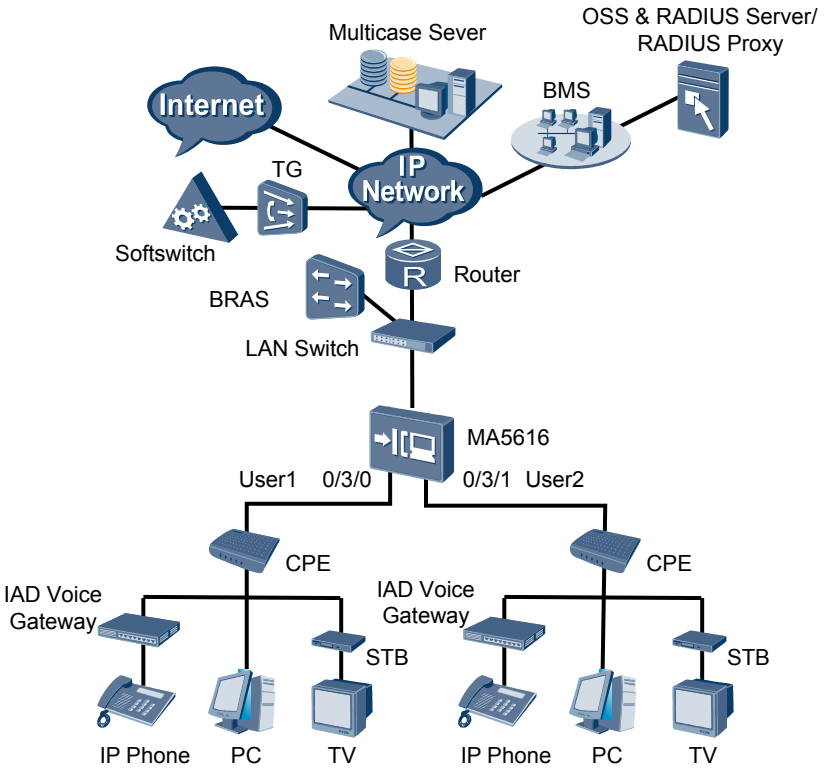
Service Requirements

- The MA5616 is used on the GE upstream transmission network.
- VDSL2 user 1 and VDSL2 user 2 are connected to the MA5616 to implement the triple play.
- The Internet service is accessed in the PPPoE mode.
- After receiving different traffic streams through the same PVC, the MA5616 provides different QoS guarantees to the traffic streams according to the user-side VLANs.

Networking

Figure 9-12 shows the example network for configuring the triple play service based on the user-side VLAN.

Figure 9-12 Example network for configuring the triple play service based on the user-side VLAN



Data Plan

Table 9-8 provides the data plan of the triple play service based on the user-side VLAN.

Table 9-8 Data plan of the triple play service based on the user-side VLAN

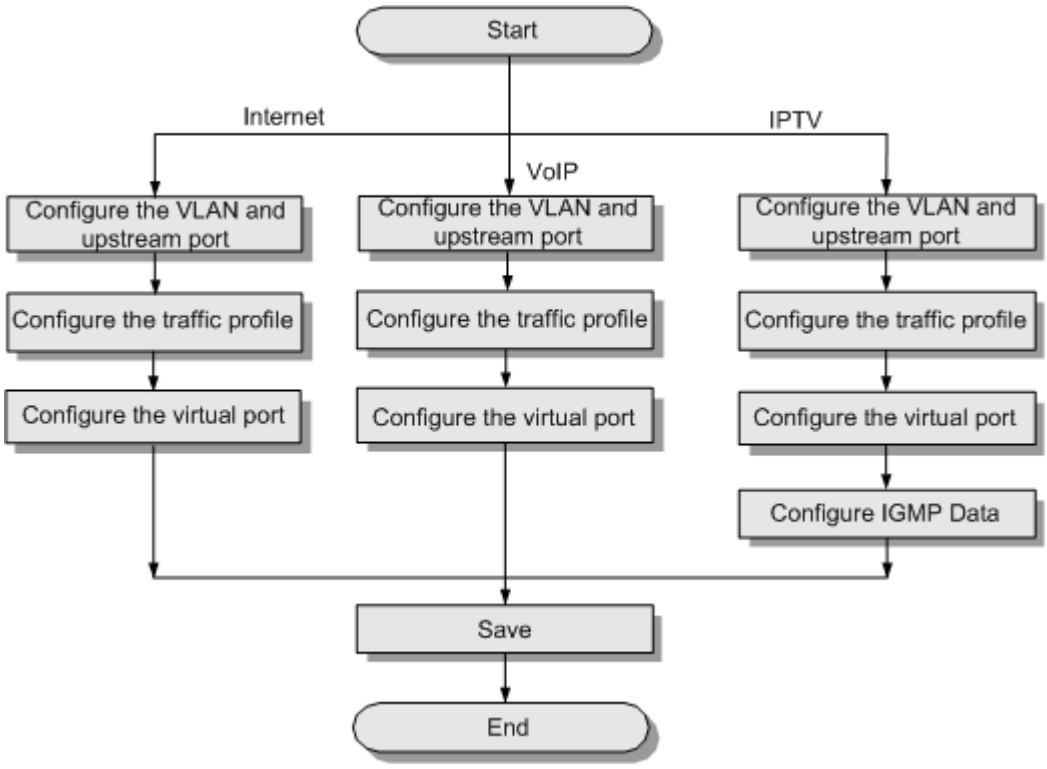
Item	Data
VDSE	Service ports: 0/1/0 and 0/1/1 Index of the VDSL2 line template bound to the port: 2, where: ● Index of the VDSL2 line profile: 3 ● Index of the VDSL2 channel profile: 3 Index of the VDSL2 alarm template bound to the port: 2, where: ● Index of the VDSL2 line alarm profile: 3 ● Index of the VDSL2 channel alarm profile: 3 VPI/VCI: 0/35
Traffic profile parameters	Internet service: 1 Mbit/s VoIP service: 64 Kbit/s IPTV service: no limit

Item	Data
Uplink port ID	0/0/1
Upstream VLANs	Internet service: smart VLAN 102 VoIP service: smart VLAN 103 IPTV service: smart VLAN 104
User-side VLANs	Internet service: smart VLAN 2 VoIP service: smart VLAN 3 IPTV service: smart VLAN 4
IGMP version	IGMP v3 (default IGMP version in the multicast VLAN mode)
Multicast source	Two multicast sources: ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
Multicast program library	Programs in multicast VLAN 104: Program 1: with IP address 224.1.1.1, the program source IP address being the same as the IP address of ISP 1 (10.10.10.10) Program 2: with IP address 224.1.1.2, the program source IP address being the same as the IP address of ISP 2 (10.10.10.11)
Right profile	Set right profile 0. Profile 0 has the right to watch program 1 in the program library.
Multicast users	User 1: User 1 (on port 0/1/0) can watch all the programs. User 2: User 2 (on port 0/1/1) can watch only program 1.
Upstream priority	The 802.1p priorities are used. The VoIP service has priority 6, IPTV service priority 5, and Internet service priority 1.

Configuration Flowchart

Figure 9-13 shows the flowchart for configuring the triple play service based on the user-side VLAN.

Figure 9-13 Flowchart for configuring the triple play service based on the user-side VLAN



Procedure

- Configure the Internet service.
  1. Create a VLAN and add an uplink port to the VLAN.

     ```
     huawei(config)#vlan 102 smart
     huawei(config)#port vlan 102 0/0 1
     ```

  2. Configure a traffic profile.
     - Because the VoIP, IPTV, and Internet 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 service. In this example, set the traffic profile index to 7 and the 802.1p priority of the Internet service to 1.

     ```
     huawei(config)#traffic table ip index 7 cir 1024 priority 1 priority-
     policy loca
     l-Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35
     multi-serv
     ice user-vlan 2 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35
     multi-serv
     ice user-vlan 2 rx-cttr 7 tx-cttr 7
     ```

4. Save the data.

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

- Configure the VoIP service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 103 smart
huawei(config)#port vlan 103 0/0 1
```

2. Configure a traffic profile.

   Set the traffic profile index to 8 and the 802.1p priority of the VoIP service to 6.

```
huawei(config)#traffic table ip index 8 cir 64 priority 6 priority-policy
local-
Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
```

4. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 104-105
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
huawei(config)#port vlan 104-105 0/0
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
  The total of the VLANs having been processed is
2
  The total of the port VLAN(s) having been added is 2
```

2. Configure a traffic profile.

   Set the traffic profile index to 9 and the 802.1p priority of the IPTV service to 5.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
local-Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
```

CAUTION

On the MA5616, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

4. Configure the multicast data.

   To provision the multicast video service, you also need to configure IGMP proxy and programs.

   a. Add a multicast VLAN and configure the multicast mode.

   ```
   huawei(config)#multicast-vlan 104
   huawei(config-mvlan104)#igmp mode
   proxy
     Are you sure to change IGMP mode?(y/n)[n]:y
   ```

   NOTE

   Select a multicast mode according to the actual requirements. In this example, the IGMP proxy mode is considered.

   b. Configure the multicast uplink port.

   ```
   huawei(config-mvlan104)#igmp uplink-port 0/0/1
   huawei(config-mvlan104)#btv
   huawei(config-btv)#igmp uplink-port-mode
   default
     Are you sure to change the uplink port mode?(y/n)[n]:y
   ```

   c. Configure the program library.

   ```
   huawei(config-btv)#multicast-vlan 104
   huawei(config-mvlan104)#igmp program add name program1 ip 224.1.1.1
   sourceip 10.
   10.10.10
   huawei(config-mvlan104)#igmp program add name program2 ip 224.1.1.2
   sourceip 10.
   10.10.11
   ```

   d. Configure the right profile.

   ```
   huawei(config-mvlan104)#btv
   huawei(config-btv)#igmp profile add profile-name profile0
   huawei(config-btv)#igmp profile profile-name profile0 program-name
   program1 watc
   h
   ```

   e. Configure multicast users.

   ```
   huawei(config-btv)#igmp user add service-port 10
   huawei(config-btv)#igmp user add service-port 11 auth
   huawei(config-btv)#igmp user bind-profile service-port 11 profile-
   name profile0
   huawei(config-btv)#multicast-vlan 104
   huawei(config-mvlan104)#igmp multicast-vlan member service-port 10
   huawei(config-mvlan104)#igmp multicast-vlan member service-port 11
   huawei(config-mvlan104)#quit
   ```

5. 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.

- Perform the PPPoE dialup on the PC. After the dialup is successful, the user can access the Internet.
- VoIP users can call each other.
- The IPTV user on port 0/1/0 can watch all the programs, and the IPTV user on port 0/1/1 can watch program 1 only.

Configuration File

Internet:

```
vlan 102 smart
port vlan 102 0/0 1
traffic table ip index 7 cir 1024 priority 1 priority-policy local-Setting
service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-vlan 2 rx-cttr 7 tx-cttr 7
service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-vlan 2 rx-cttr 7 tx-cttr 7
save
```

VoIP:

```
vlan 103 smart
port vlan 103 0/0 1
traffic table ip index 8 cir 64 priority 6 priority-policy local-Setting
service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-vlan 3 rx-cttr 8 tx-cttr 8
save
```

IPTV:

```
vlan 104-105 smart
y
port vlan 104-105 0/0 1
y
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-vlan 4 rx-cttr 9 tx-cttr 9
multicast-vlan 104
igmp mode proxy
y
igmp uplink-port 0/0/1
btv
igmp uplink-port-mode default
y
multicast-vlan 104
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name program1 watch
igmp user add service-port 10
igmp user add service-port 11 auth
igmp user bind-profile service-port 11 profile-name profile0
multicast-vlan 104
igmp multicast-vlan member service-port 10
igmp multicast-vlan member service-port 11
```

```
quit
save
```

9.5.2 Configuration Example of the Triple Play Service - Single PVC for Multiple Services Based on the User-Side 802.1p

This topic describes how to configure the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Prerequisites

Before configuring the triple play service, make sure that:

- The network devices and lines are in the normal state.
- The CPE is already configured (the CPE supports different user-side 802.1p priorities for different services).
- All boards of the device run in the normal state.
- The VDSL2 line template and alarm template that are bound to the port are already configured. For details on the configuration procedure, see **3.7.3 Configuring the VDSL2 Profile**.

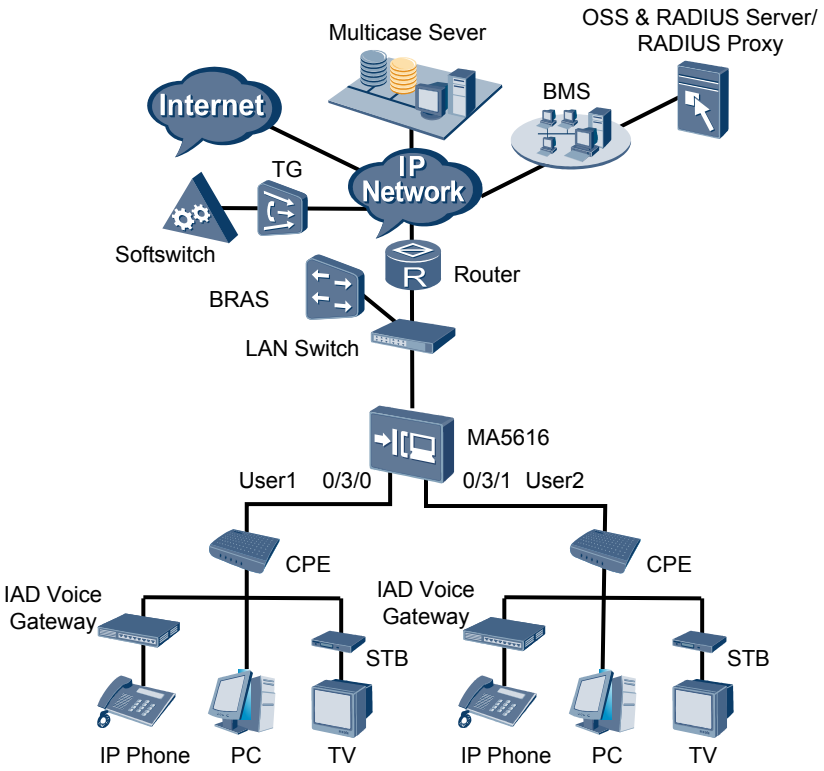
Service Requirements

- The MA5616 is used on the GE upstream transmission network.
- VDSL2 user 1 and VDSL2 user 2 are connected to the MA5616 to implement the triple play.
- The Internet service is accessed in the PPPoE mode.
- After receiving different traffic streams through the same PVC, the MA5616 provides different QoS guarantees to the traffic streams according to the user-side 802.1p priority.

Networking

Figure 9-14 shows the example network for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Figure 9-14 Example network for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority



Data Plan

Table 9-9 provides the data plan for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Table 9-9 Data plan for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority

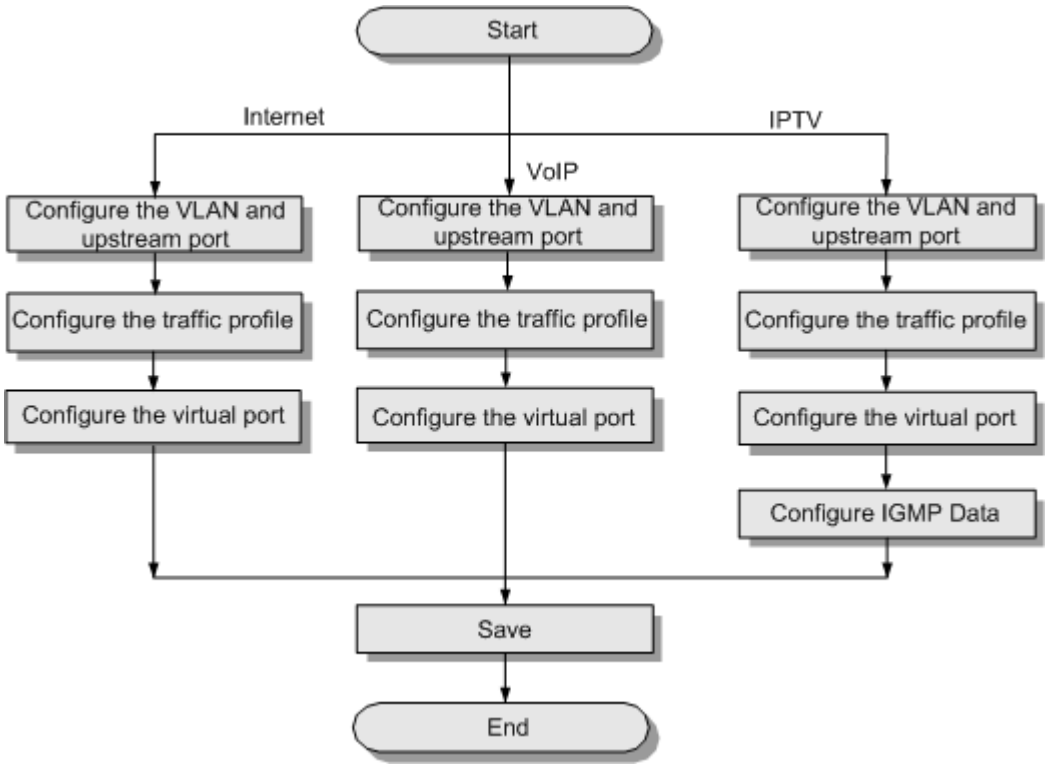
Item	Data
VDSE	Service ports: 0/1/0 and 0/1/1 Index of the VDSL2 line template bound to the port: 2, where: ● Index of the VDSL2 line profile: 3 ● Index of the VDSL2 channel profile: 3 Index of the VDSL2 alarm template bound to the port: 2, where: ● Index of the VDSL2 line alarm profile: 3 ● Index of the VDSL2 channel alarm profile: 3 VPI/VCI: 0/35

Item	Data
Traffic profile parameters	Internet service: 1 Mbit/s VoIP service: 64 Kbit/s IPTV service: no limit
Uplink port ID	0/0/1
Upstream VLANs	Internet service: smart VLAN 102 VoIP service: smart VLAN 103 IPTV service: smart VLAN 104
User-side 802.1p priorities	Internet service: 2 VoIP service: 3 IPTV service: 4
IGMP version	IGMP v3 (default IGMP version in the multicast VLAN mode)
Multicast source	Two multicast sources: ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
Multicast program library	Programs in multicast VLAN 104: Program 1: with IP address 224.1.1.1, the program source IP address being the same as the IP address of ISP 1 (10.10.10.10) Program 2: with IP address 224.1.1.2, the program source IP address being the same as the IP address of ISP 2 (10.10.10.11)
Right profile	Set right profile 0. Profile 0 has the right to watch program 1 in the program library.
Multicast users	User 1: User 1 (on port 0/3/0) can watch all the programs. User 2: User 2 (on port 0/3/1) can watch only program 1.
Upstream priority	The 802.1p priorities are used. The VoIP service has priority 6, IPTV service priority 5, and Internet service priority 1.

Configuration Flowchart

Figure 9-15 shows the flowchart for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority.

Figure 9-15 Flowchart for configuring the triple play service in the single-PVC for multiple services mode based on the user-side 802.1p priority



Procedure

- Configure the Internet service.
  1. Create a VLAN and add an uplink port to the VLAN.

     ```
     huawei(config)#vlan 102 smart
     huawei(config)#port vlan 102 0/0 1
     ```

  2. Configure a traffic profile.
     - Because the VoIP, IPTV, and Internet 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 service. In this example, set the traffic profile index to 7 and the 802.1p priority of the Internet service to 1.

     ```
     huawei(config)#traffic table ip index 7 cir 1024 priority 1 priority-
     policy loca
     l-Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35
     multi-serv
     ice user-8021p 2 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35
     multi-serv
     ice user-8021p 2 rx-cttr 7 tx-cttr 7
     ```

4. Save the data.

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

- Configure the VoIP service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 103 smart
huawei(config)#port vlan 103 0/0 1
```

2. Configure a traffic profile.

   Set the traffic profile index to 8 and the 802.1p priority of the VoIP service to 6.

```
huawei(config)#traffic table ip index 8 cir 64 priority 6 priority-policy
local-
Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
huawei(config)#service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
```

4. Save the data.

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

- Configure the IPTV service.

1. Create a VLAN and add the uplink port to the VLAN.

```
huawei(config)#vlan 104-105
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
huawei(config)#port vlan 104-105 0/0
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
  The total of the VLANs having been processed is
2
  The total of the port VLAN(s) having been added is 2
```

2. Configure a traffic profile.

   Set the traffic profile index to 9 and the 802.1p priority of the IPTV service to 5.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
local-Setting
```

3. Add service ports to the VLAN.

   Add service ports to the VLAN and use the traffic profile configured in the preceding step.

```
huawei(config)#service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35
multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35
multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
```

CAUTION

On the MA5616, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

4. Configure the multicast data.

   To provision the multicast video service, you also need to configure IGMP proxy and programs.

   a. Add a multicast VLAN and configure the multicast mode.

   ```
   huawei(config)#multicast-vlan 104
   huawei(config-mvlan104)#igmp mode
   proxy
     Are you sure to change IGMP mode?(y/n)[n]:y
   ```

   NOTE

   Select a multicast mode according to the actual requirements. In this example, the IGMP proxy mode is considered.

   b. Configure the multicast uplink port.

   ```
   huawei(config-mvlan104)#igmp uplink-port 0/0/1
   huawei(config-mvlan104)#btv
   huawei(config-btv)#igmp uplink-port-mode
   default
     Are you sure to change the uplink port mode?(y/n)[n]:y
   ```

   c. Configure the program library.

   ```
   huawei(config-btv)#multicast-vlan 104
   huawei(config-mvlan104)#igmp program add name program1 ip 224.1.1.1
   sourceip 10.
   10.10.10
   huawei(config-mvlan104)#igmp program add name program2 ip 224.1.1.2
   sourceip 10.
   10.10.11
   huawei(config-mvlan104)#quit
   ```

   d. Configure the right profile.

   ```
   huawei(config)#btv
   huawei(config-btv)#igmp profile add profile-name profile0
   huawei(config-btv)#igmp profile profile-name profile0 program-name
   program1 watc
   h
   ```

   e. Configure multicast users.

   ```
   huawei(config-btv)#igmp user add service-port 10
   huawei(config-btv)#igmp user add service-port 11 auth
   huawei(config-btv)#igmp user bind-profile service-port 11 profile-
   name profile0
   huawei(config-btv)#quit
   huawei(config)#multicast-vlan 104
   huawei(config-mvlan104)#igmp multicast-vlan member service-port 10
   huawei(config-mvlan104)#igmp multicast-vlan member service-port 11
   huawei(config-mvlan104)#quit
   ```

5. 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.

- Perform the PPPoE dialup on the PC. After the dialup is successful, the user can access the Internet.
- VoIP users can call each other.
- The IPTV user on port 0/1/0 can watch all the programs, and the IPTV user on port 0/1/1 can watch program 1 only.

Configuration File

Internet:

```
vlan 102 smart
port vlan 102 0/0 1
traffic table ip index 7 cir 1024 priority 1 priority-policy local-Setting
service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-8021p 2 rx-cttr 7 tx-cttr 7
service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-8021p 2 rx-cttr 7 tx-cttr 7
save
```

VoIP:

```
vlan 103 smart
port vlan 103 0/0 1
traffic table ip index 8 cir 64 priority 6 priority-policy local-Setting
service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-8021p 3 rx-cttr 8 tx-cttr 8
save
```

IPTV:

```
vlan 104-105 smart
y
port vlan 104-105 0/0 1
y
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35 multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35 multi-serv
ice user-8021p 4 rx-cttr 9 tx-cttr 9
multicast-vlan 104
igmp mode proxy
y
igmp uplink-port 0/0/1
btv
igmp uplink-port-mode default
y
multicast-vlan 104
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name program1 watch
igmp user add service-port 10
igmp user add service-port 11 auth
igmp user bind-profile service-port 11 profile-name profile0
multicast-vlan 104
igmp multicast-vlan member service-port 10
igmp multicast-vlan member service-port 11
```

```
quit
save
```

9.5.3 Configuration Example of the Triple Play Service - Multiple PVCs for Multiple Services

This topic describes how to configure the triple play service in the multi-PVC for multiple services mode.

Prerequisites

Before configuring the triple play service, make sure that:

- The network devices and lines are in the normal state.
- The CPE is already configured (the CPE supports different PVCs for different services).
- All boards of the device run in the normal state.
- The VDSL2 line template and alarm template that are bound to the port are already configured. For details on the configuration procedure, see **3.7.3 Configuring the VDSL2 Profile**.

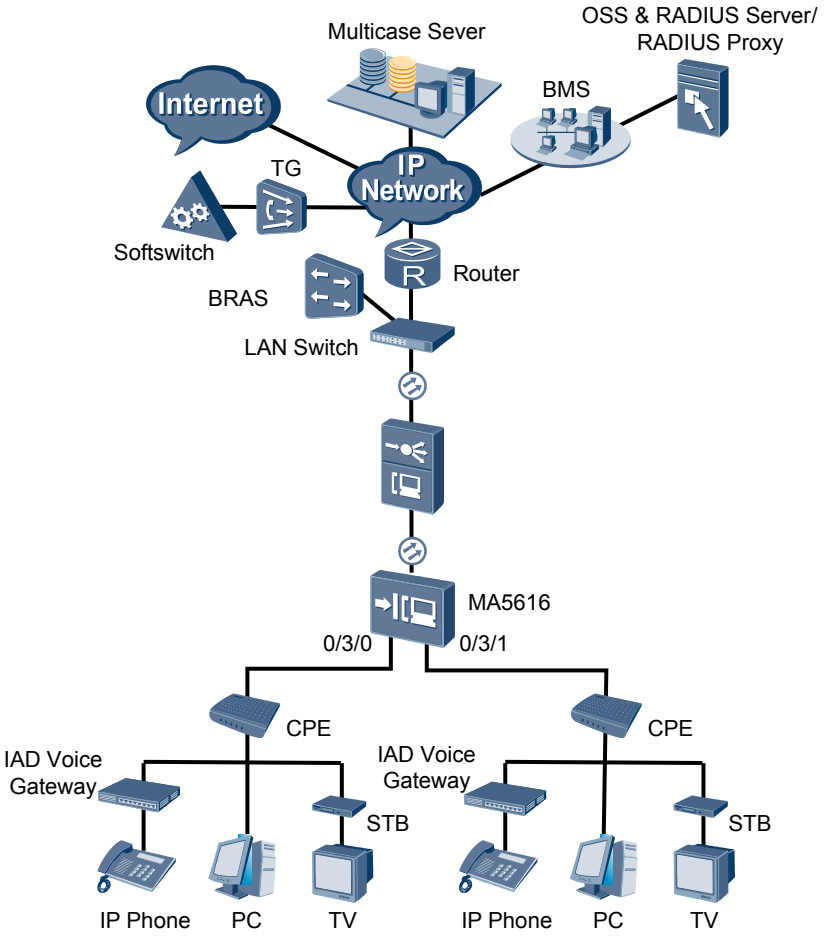
Service Requirements

- The MA5616 is used on the GE upstream transmission network.
- VDSL2 user 1 and VDSL2 user 2 are connected to the MA5616 to implement the triple play.
- The Internet service is provided in the PPPoE mode.
- After receiving different traffic streams, the MA5616 provides different QoS guarantees to the traffic streams according to the traffic priorities in the PVC.

Networking

Figure 9-16 shows the example network of the triple play service in the multi-PVC for multiple services mode.

Figure 9-16 Example network of the triple play service in the multi-PVC for multiple services mode



Data Plan

Table 9-10 provides the data plan for configuring the triple play service in the multi-PVC for multiple services mode.

Table 9-10 Data plan for configuring the triple play service in the multi-PVC for multiple services mode

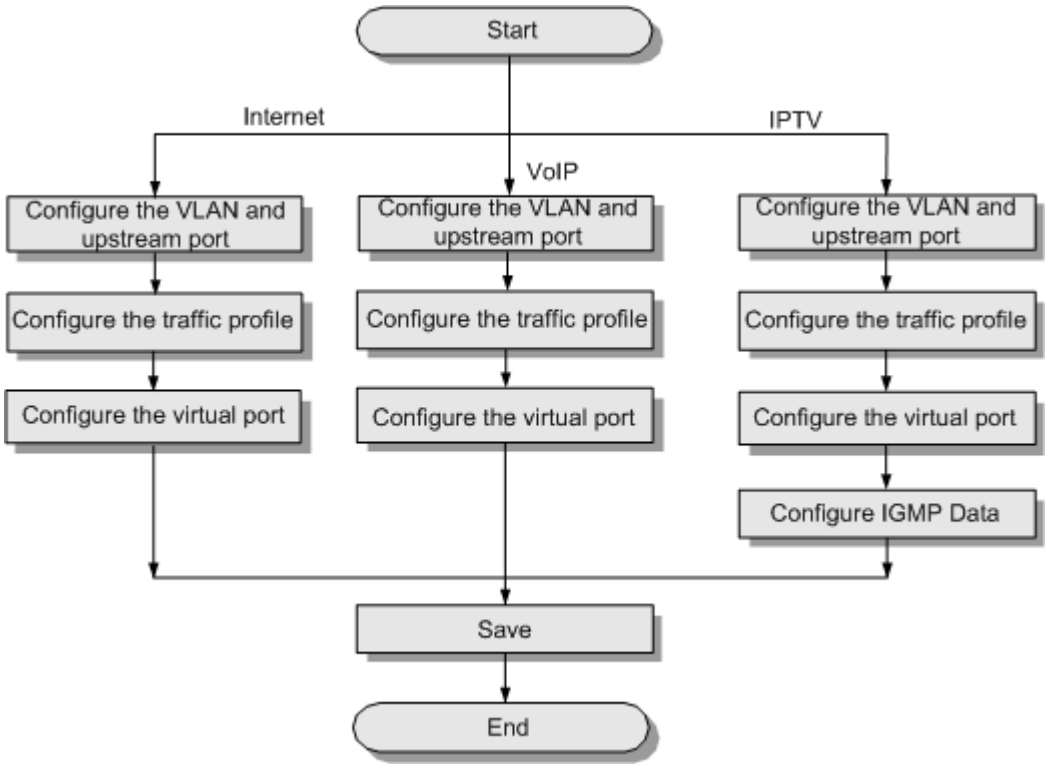
Item	Data
VDSE	Service ports: 0/1/0 and 0/1/1 Index of the VDSL2 line template bound to the port: 2, where: ● Index of the VDSL2 line profile: 3 ● Index of the VDSL2 channel profile: 3 Index of the VDSL2 alarm template bound to the port: 2, where: ● Index of the VDSL2 line alarm profile: 3 ● Index of the VDSL2 channel alarm profile: 3

Item	Data
	VPI/VCI for the Internet service: 0/37
	VPI/VCI for the VoIP service: 0/36
	VPI/VCI for the IPTV service: 0/35
Traffic profile parameters	Internet service: 1 Mbit/s VoIP service: 64 Kbit/s IPTV service: no limit
Uplink port ID	0/0/1
VLANs	Internet service: smart VLAN 102
	VoIP service: smart VLAN 103
	IPTV service: smart VLAN 104
IGMP version	IGMP v3 (default IGMP version in the multicast VLAN mode)
Multicast source	Two multicast sources: ISP 1: with IP address 10.10.10.10, providing the multicast program with IP address 224.1.1.1 ISP 2: with IP address 10.10.10.11, providing the multicast program with IP address 224.1.1.2
Multicast program library	Programs in multicast VLAN 104: Program 1: with IP address 224.1.1.1, the program source IP address being the same as the IP address of ISP 1 (10.10.10.10) Program 2: with IP address 224.1.1.2, the program source IP address being the same as the IP address of ISP 2 (10.10.10.11)
Right profile	Set right profile 0. Profile 0 has the right to watch program 1 in the program library.
Multicast users	User 1: User 1 (on port 0/1/0) can watch all the programs. User 2: User 2 (on port 0/1/1) can watch only program 1.
Upstream priority	The 802.1p priorities are used. The VoIP service has priority 6, IPTV service priority 5, and Internet service priority 1.

Configuration Flowchart

Figure 9-17 shows the flowchart for configuring the triple play service in the multi-PVC for multiple services mode.

Figure 9-17 Flowchart for configuring the triple play service in the multi-PVC for multiple services mode



Procedure

- Configure the Internet service.
  1. Create a VLAN and add an uplink port to the VLAN.

     ```
     huawei(config)#vlan 102 smart
     huawei(config)#port vlan 102 0/0 1
     ```

  2. Configure a traffic profile.
     - Because the VoIP, IPTV, and Internet 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 service. In this example, set the traffic profile index to 7 and the 802.1p priority of the Internet service to 1.

     ```
     huawei(config)#traffic table ip index 7 cir 1024 priority 1 priority-
     policy loca
     l-Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 37 rx-
     cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 102 vdsl mode atm 0/1/1 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 the uplink port to the VLAN.

     ```
     huawei(config)#vlan 103 smart
     huawei(config)#port vlan 103 0/0 1
     ```

  2. Configure a traffic profile.

     Set the traffic profile index to 8 and the 802.1p priority of the VoIP service to 6.

     ```
     huawei(config)#traffic table ip index 8 cir 64 priority 6 priority-policy
     local-
     Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 36 rx-
     cttr 8 tx-cttr 8
     huawei(config)#service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 36 rx-
     cttr 8 tx-cttr 8
     ```

  4. Save the data.

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

- Configure the IPTV service.
  1. Create a VLAN and add the uplink port to the VLAN.

     ```
     huawei(config)#vlan 104-105
     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
     huawei(config)#port vlan 104-105 0/0
     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
       The total of the VLANs having been processed is
     2
       The total of the port VLAN(s) having been added is 2
     ```

  2. Configure a traffic profile.

     Set the traffic profile index to 9 and the priority of the IPTV service to 5.

     ```
     huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
     local-Setting
     ```

  3. Add service ports to the VLAN.

     Add service ports to the VLAN and use the traffic profile configured in the preceding step.

     ```
     huawei(config)#service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35
     rx-cttr 9 tx-cttr 9
     huawei(config)#service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35
     rx-cttr 9 tx-cttr 9
     ```

NOTE

On the MA5616, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

4. Configure the multicast data.

   To provision the multicast video service, you also need to configure IGMP proxy and programs.

   a. Add a multicast VLAN and configure the multicast mode.

```
huawei(config)#multicast-vlan 104
huawei(config-mvlan104)#igmp mode
proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   NOTE

   Select a multicast mode according to the actual requirements. In this example, the IGMP proxy mode is considered.

   b. Configure the multicast uplink port.

```
huawei(config-mvlan104)#igmp uplink-port 0/0/1
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp uplink-port-mode
default
  Are you sure to change the uplink port mode?(y/n)[n]:y
```

   c. Configure the program library.

```
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp program add name program1 ip 224.1.1.1
sourceip 10.
10.10.10
huawei(config-mvlan104)#igmp program add name program2 ip 224.1.1.2
sourceip 10.
10.10.11
```

   d. Configure the right profile.

```
huawei(config-mvlan104)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name
program1 watc
h
```

   e. Configure multicast users.

```
huawei(config-btv)#igmp user add service-port 10
huawei(config-btv)#igmp user add service-port 11 auth
huawei(config-btv)#igmp user bind-profile service-port 11 profile-
name profile0
huawei(config-btv)#multicast-vlan 104
huawei(config-mvlan104)#igmp multicast-vlan member service-port 10
huawei(config-mvlan104)#igmp multicast-vlan member service-port 11
huawei(config-mvlan104)#quit
```

5. 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.

- Perform the PPPoE dialup on the PC. After the dialup is successful, the user can access the Internet.
- VoIP users can call each other.

- The IPTV user on port 0/1/0 can watch all the programs, and the IPTV user on port 0/1/1 can watch program 1 only.

Configuration File

Internet:

```
vlan 102 smart
port vlan 102 0/0 1
traffic table ip index 7 cir 1024 priority 1 priority-policy local-Setting
service-port vlan 102 vdsl mode atm 0/1/0 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
service-port vlan 102 vdsl mode atm 0/1/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
save
```

VoIP:

```
vlan 103 smart
port vlan 103 0/0 1
traffic table ip index 8 cir 64 priority 6 priority-policy local-Setting
service-port vlan 103 vdsl mode atm 0/1/0 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
service-port vlan 103 vdsl mode atm 0/1/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
save
```

IPTV:

```
vlan 104-105 smart
y
port vlan 104-105 0/0 1
y
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 10 vlan 105 vdsl mode atm 0/1/0 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
service-port 11 vlan 105 vdsl mode atm 0/1/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
multicast-vlan 104
igmp mode proxy
y
igmp uplink-port 0/0/1
btv
igmp uplink-port-mode default
y
multicast-vlan 104
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.11
btv
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name program1 watch
igmp user add service-port 10
igmp user add service-port 11 auth
igmp user bind-profile service-port 11 profile-name profile0
multicast-vlan 104
igmp multicast-vlan member service-port 10
igmp multicast-vlan member service-port 11
quit
save
```

10 Configuration Examples of the FTTx

About This Chapter

The FTTx solution configuration guide describes how to configure typical FTTH, FTTB/C, FTTO, and FTTM services (such as high-speed Internet access, multicast, VoIP, and mobile backhaul services) on the OLT and the ONU step by step through examples.

10.1 FTTx Network and Product

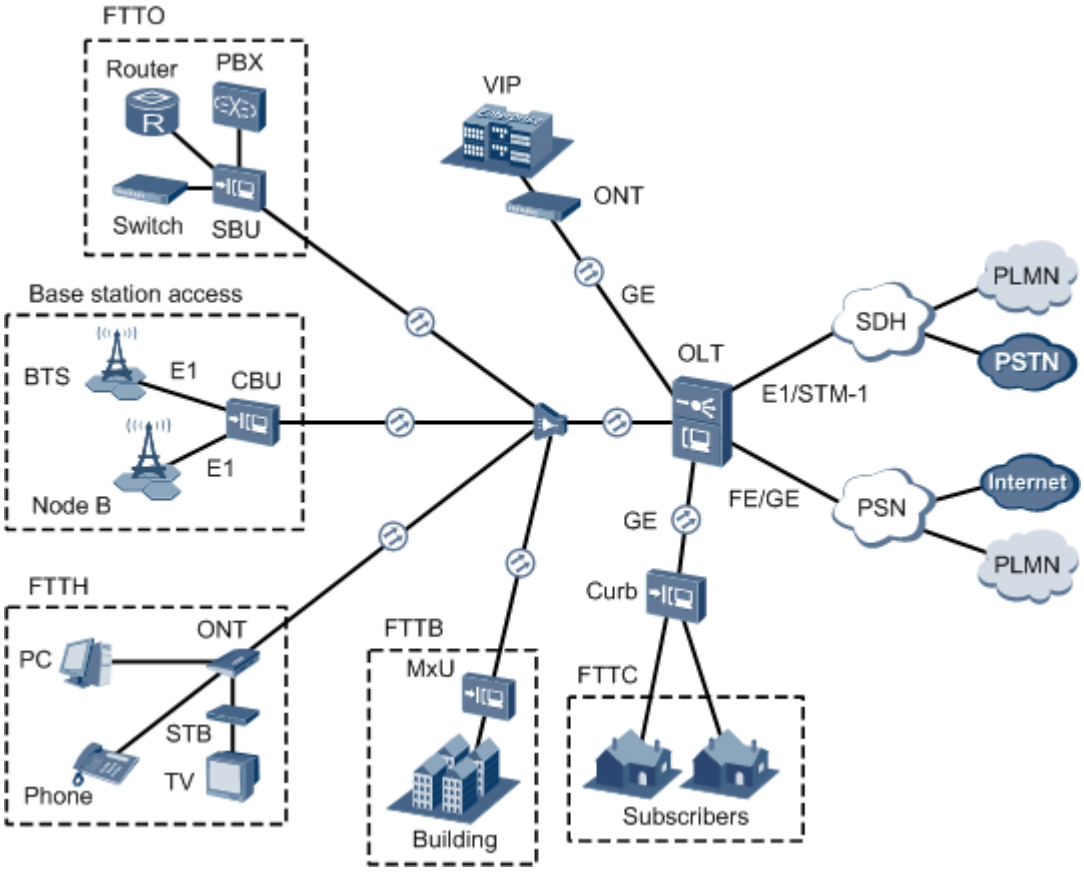
FTTx applications include FTTH, FTTB, FTTC, FTTO, Base station access, and VIP P2P access.

Network

Figure 10-1 shows an example network of full access services in the FTTx scenario. FTTx applications include FTTH, FTTB, FTTC, FTTO, Base station access, and VIP P2P access.

- FTTH indicates fiber to the home. The ONT is connected to the OLT in the PON mode to implement FTTH. The voice, data, and video services are provided through a single optical fiber.
- FTTB/FTTC indicates fiber to the building/fiber to the curb. The MDU is connected to the OLT in the PON mode or GE mode to implement FTTB/FTTC, and provides voice, data, and video services for the users in communities.
- FTTO indicates fiber to the office. The SBU is connected to the OLT in the PON mode to implement FTTO. In this way, the Intranet TDM PBX, Intranet IP PBX, and Intranet private line services are provided.
- Base station access indicates fiber to the mobile base station. The CBU is connected to the OLT in the PON mode to implement base station backhaul.
- P2P indicates point to point. The VIP household and enterprise users can be directly connected to the OLT through GE optical fibers to implement end-to-end QoS.

Figure 10-1 Example network of full access services in the FTTx scenario



Configuration Products

Table 10-1 lists the configuration products for the FTTx solution.

Table 10-1 Configuration products for the FTTx solution

Network Positioning	Configuration Product	Version	Description
OLT	MA5600T and MA5603T	V800R008C01/C02	Supports functioning as an OLT in the FTTH, FTTB, FTTC, Base station access, or FTTO network.
MDU	MA5620, MA5626, MA5612, MA5652G	V800R308C00	Supports functioning as an MDU in the FTTB or FTTC network.
	MA5616, MA5628	V800R308C01	
CBU	MA5612	V800R308C00/C01	Supports functioning as a CBU in the Base station access network.
SBU	MA5612	V800R308C00/C01	Supports functioning as an SBU in the FTTO network.
ONT	HG series	V100R001/ V100R002	Supports functioning as an ONT in the FTTH network.

10.2 FTTx Data Plan (GPON Access)

This topic plans the data in a unified manner for connecting to the OLT in the FTTx GPON access mode for various example networks. The subsequent examples are configured based on the following data plan.

Data Plan

Table 10-2 provides the unified data plan for configuring the HSI, IPTV, VoIP, emulation services, and private line services in an FTTx network.

NOTE

The ONU in the data plan refers to the ONT and the MDU collectively.

Table 10-2 Data plan for the FTTx GPON access

Service Classification	Item	Data	Remarks
Network data	FTTH	OLT PON port: 0/1/1 ONT ID: 1-2	In the current network, FTTH, FTTB, and FTTC can be implemented on the same OLT. Generally, different slots are used for the implementation. Implementing various FTTx networks concurrently, however, is not recommended in general.
	FTTB/C	OLT PON port: 0/2/1 ONT ID: 1-2	
	FTTO/M	OLT PON port: 0/3/1 ONT ID: 1	
	P2P	FE ports of the OPFA board on the OLT: ● 0/5/1 ● 0/5/2 ● 0/5/3	
Device management	Inband NMS IP address of the OLT	192.168.50.1/24	To configure the MDU from the OLT by logging in to the MDU through Telnet, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment. In the GPON access, the network management protocol of the MDU adopts SNMP and that of the ONT adopts OMCI.
	Management VLAN of the OLT	8	
	Inband NMS IP address of the MDU	ONU 1: 192.168.50.2/24 ONU 2: 192.168.50.3/24	
	Management VLAN of the MDU	8	

Service Classification	Item	Data	Remarks
Service VLAN	HSI service	ONU upstream VLAN: 1001-1016 OLT VLANs: ● CVLAN: CVALN ID = 256 x GPON port ID + 256 x optical ratio x (optical splitter port ID - 1) + ONU port ID + 1 ● SVLAN: 100 (stacking VLAN)	For the Internet access service, you can use two precisely-bound VLAN tags to extend VLANs and identify users. On the OLT, each OLT, each slot of the OLT, or each PON port is allocated with an SVLAN. Each user is allocated with a CVLAN. CVLANs of the same OLT are planned in a unified manner and each VLAN ID is unique. The recommended allocation rule is as follows: CVLAN ID = 256 x GPON port ID + 256 x optical ratio x (optical splitter port ID - 1) + ONU port ID + 1 Upstream VLANs for ONUs of the same type are recommended to be the same. This prevents configuration differences of different ONUs. This makes configuration and maintenance easier.
	IPTV service	Multicast VLAN: 1000	Generally, multicast VLANs are divided according to multicast sources.
	VoIP service	ONU VLAN: 200 OLT VLAN (VLAN transparently transmitting the ONU service): 200	Generally, the VoIP service can be identified by a single VLAN tag. Each OLT, each slot of the OLT, or each PON port can be allocated with a VLAN to reduce VLAN broadcast domains.
	Emulation service	TDM emulation SVLAN: 500 ATM emulation SVLAN: 700 ETH emulation SVLAN: 800	They are the SVLANs of the OLT that transparently transmit the ONU service.
	QinQ private line service	ONU SVLAN: 2000 OLT VLAN (VLAN transparently transmitting the ONU service): 2000	QinQ is used to implement the Layer 2 VPN private line service. In the case of FTTH, enable QinQ on the OLT; in the case of FTTB/FTTC, enable QinQ on the ONU. Each slot of the OLT can be allocated with an SVLAN to reduce VLAN broadcast domains.
QoS (priority and queue	HSI service	Priority: 1; queue scheduling: WRR	Generally, the QoS priorities are NMS service and IP voice service > private line service > IPTV service > Internet access service in a descending order.

Service Classification	Item	Data	Remarks
scheduling)	IPTV service	Priority: 4; queue scheduling: WRR	The queue scheduling mode is configured globally. Queues with higher priorities adopt PQ mode and queues with lower priorites adopt WRR mode. In FTTH networks, service priorities are set on the OLT. In other FTTx networks, service priorities are set on ONUs and the OLT transparently transmits the priorities.
	VoIP service	Priority: 6; queue scheduling: PQ	
	Emulation service	Priority: 6; queue scheduling: PQ	
	QinQ private line service	Priority: 5; queue scheduling: PQ	
QoS (DBA)	HSI service	● Profile name: PPPOE ● Profile type: Type4 ● Maximum bandwidth (FTTH): 20 Mbit/s ● Maximum bandwidth (FTTB/C): 100 Mbit/s ● T-CONT ID: 4	DBA is used to control the upstream bandwidth of the ONU. DBA profiles are bound to TCONTs. Different TCONTs are planned for different bandwidth assurance types. Generally, the service with a high priority adopts a fixed bandwidth or an assured bandwidth, and the service with a low priority adopts the maximum bandwidth or best effort.
	IPTV service	● Profile name: IPTV ● Profile type: Type4 ● Maximum bandwidth (FTTH): 1 Mbit/s ● Maximum bandwidth (FTTB/C): 60 Mbit/s ● T-CONT ID: 3	

Service Classification	Item	Data	Remarks
	VoIP service	● Profile name: VOIP ● Profile type: Type3 ● Assured bandwidth (FTTH): 0.1 Mbit/s ● Maximum bandwidth (FTTH): 1 Mbit/s ● Assured bandwidth (FTTB/C): 15 Mbit/s ● Maximum bandwidth (FTTB/C): 30 Mbit/s ● T-CONT ID: 2	
	Emulation service	● Profile name: – For TDM emulation: TDM – For ADM emulation: ATM – For ETH emulation: ETH ● Profile type: Type1 ● Fixed bandwidth 32 Mbit/s ● T-CONT ID: 1	

Service Classification	Item	Data	Remarks
	QinQ private line service	● Profile name: PrivateLine ● Profile type: Type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s ● T-CONT ID: 5	
QoS (CAR)	Emulation service	No rate limitation in the upstream and downstream directions	Traffic control can be implemented on the BRAS, or on the OLT or ONU by using port rate limitation or using a traffic profile to limit the upstream and downstream traffic. Generally, in the case of FTTH, limit the rate on the OLT; in the case of FTTB/ FTTC, limit the rate on the ONU.
	VoIP service	No rate limitation in the upstream and downstream directions	
	IPTV service	No rate limitation in the upstream and downstream directions	
	HSI service	Upstream and downstream bandwidth: 4 Mbit/s	
IPTV service data	Multicast protocol	OLT: IGMP proxy ONU: IGMP snooping	-
	Multicast version	IGMP V3	IGMP v3 and IGMP v2 are supported, and IGMP v3 is compatible with IGMP v2.
	Multicast program configuration mode	Static configuration mode	The OLT can also generate a multicast program library, that is, dynamically generate a program list according to the programs requested by users. In this mode, the program list need not be configured or maintained; however, the functions such as program management, user multicast bandwidth management, program preview, and program prejoin are not supported.

Service Classification	Item	Data	Remarks
	IP address of the multicast server	10.10.10.10	-
	Multicast program	224.1.1.10	-
VoIP service data	Signaling and media IP addresses	17.10.10.10/24	H.248 and SIP support separate media and signaling. The media and signaling IP address can be the same or different.
	Gateway IP address	17.10.10.1/24	-
	MG interface (H.248) **NOTE** The parameters of the MG interface must be the same as the parameters on the MGC. H.248 has many negotiation parameters, and the parameters here are mandatory.	MG interface ID: 0	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: 2944	It is the transport layer protocol port ID used for the signaling exchange between the MG and the MGC.
		IP address of the primary MGC to which the MG interface belongs: 200.200.200.200/24	When dual homing is configured, the IP address and the port ID of the secondary MGC must also be configured.
		Port ID of the primary MGC to which the MG interface belongs: 2944	
		Coding mode of the MG interface: text	-
		Transmission mode of the MG interface: UDP	The transmission mode of the MG interface is selected according to the requirements on the MGC. Generally, UDP is adopted.

Service Classification	Item	Data	Remarks
		Index of the profile used by the MG interface	Different profile indexes are used for interconnection with non-Huawei softswitches. You can run the **if-h248 attribute profile-index** command to query the profile index. For interconnection with a ZTE softswitch, use profile 5; for interconnection with a Bell softswitch, no constant profile is used. Profile 0 can be used and the data is negotiated with the Bell softswitch.
	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.	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: 5056	-
		IP address of the primary softswitch to which the SIP interface belongs: 200.200.200.200/24	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: 5060/24	
		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	-
		Index of the profile used by the SIP interface: 1	-
	PSTN users	phone1-phone24: 83110001-83110024	-

Service Classification	Item	Data	Remarks
		User priorities: Phone 1: Cat2; Phone 2-Phone 24: Cat3 (default)	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)
Emulation service data	Local LSR ID	10.10.10.10/32	Generally, the IP address of the loopback interface is used as the LSR ID.
	Remote (OLT) LSR ID	10.20.20.20/32	
	Remote (PTN) LSR ID	30.30.30.30/32	

10.3 Configuring Upstream Link Aggregation

Configure the upstream link aggregation group to improve the bandwidth and reliability of the upstream link of the OLT.

Service Requirements

- The bandwidth of a single upstream port of the OLT is insufficient and two upstream ports are required.
- Two upstream ports of the OLT provide load balancing function.
- Two upstream ports of the OLT back up each other. When one port is faulty, the other port ensures the normal forwarding of the service.

Table 10-3 Data plan

Item	Data
Upstream ports	0/19/0 and 0/19/1
Aggregation group	Packet allocation mode: according to the source MAC address Working mode: lacp-static

Procedure

Step 1 Configure an aggregation group.

Configure upstream ports 0/19/0 and 0/19/1 as an aggregation group. Each member port in the aggregation group is allocated with packets according to the source MAC address. The working mode is LACP static aggregation.

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

NOTE

- Types of the two aggregated ports must be the same.
- An aggregation group can implement inter-board aggregation between two GIU slots.
- An aggregation group can implement inter-board aggregation between two SPUA boards.
- When only one control board is configured, inter-board aggregation is supported between the SCUN board and the GIU slot.

Step 2 Save the data.

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

----End

Result

Run the **display link-aggregation** command to query the information about the aggregation group. The displayed information is the same as the configuration.

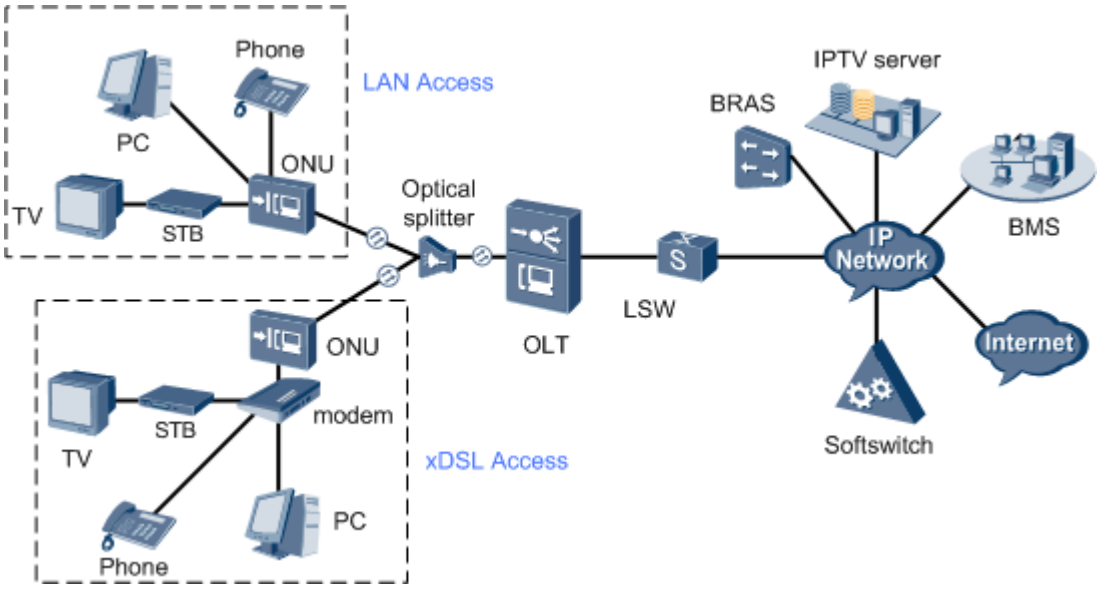
10.4 Configuring the FTTB and FTTC Access Services

This topic describes how to configure the Internet access, voice and multicast in the FTTB and FTTC Access Services.

Context

In the FTTB and FTTC Access Services, the user can access to the ONU by LAN or xDSL. The ONU is connected to the OLT through an GPON port to provide users with the high-speed Internet access service, VoIP service and IPTV service.

Figure 10-2 Example network of the multiple service in FTTB and FTTC service



10.4.1 Configuring the FTTB and FTTC Internet Access Services (ADSL2+ Access)

The OLT is connected to a remote ONU that supports ADSL2+ access by using the GPON port to provide users with the high-speed Internet access service.

Service Requirements

- VLANs are divided are isolated different user groups, preventing broadcast storms and facilitating O&M.
- Users perform PPPoE dialup on PCs to implement high-speed Internet access.
- Two VLAN tags are used to precisely identify services and users.
- The same QoS is used for the same type of services on the same type of ONUs, facilitating management.

Prerequisite

- The example network as shown in **Figure 10-2** is complete.
- Corresponding ONU version: V800R309C00. If another version is used, the configuration differs slightly. For details, see the configuration guide of the corresponding ONU version.
- The ADSL mode of ONU is NGADSL (namely RFC4706).

  NOTE

  You can run the **display xdsl mode** command in the privilege mode to query the ADSL mode.

Background Information

ONUs that support ADSL2+ access include MA5616.

Procedure

- **Configure the OLT.**

1. Create an SVLAN and configure its upstream port.

   On the OLT, each OLT, each slot of the OLT, or each PON port can be allocated with an SVLAN. In this example, an SVLAN is allocated to each slot. To precisely identify a user, stacking VLANs are used. This means to translate CVLANs on the OLT according to the planned VLAN IDs.

   Configure the SVLAN ID to 100, VLAN type to smart VLAN, and VLAN attribute to stacking. Add upstream port 0/19/0 to VLAN 100.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#vlan attrib 100 stacking
   huawei(config)#port vlan 100 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured to implement protection between ports and load sharing. For details, see **10.3 Configuring Upstream Link Aggregation**.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile,and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

   a. Configure a DBA profile.

      You can run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

      Configure the DBA profile name to PPPoE, type to Type4, and maximum bandwidth to 100 Mbit/s.

      ```
      huawei(config)#dba-profile add profile-name PPPoE type4 max 102400
      ```

   b. Configure an ONU line profile.

      Create GPON ONU line profile 10 and bind T-CONT 4 to DBA profile PPPoE. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

      ```
      huawei(config)#ont-lineprofile gpon profile-id 10
      huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name PPPoE
      ```

      NOTE

      The ID of the line profile to be created must not exist in the system. Please create proper ONU line profiles according to actual data plan. In this example, line profile 10 is used.

      Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting Internet traffic streams. Bind GEM port 0 and GEM port 1 to T-CONT 4. Set the QoS mode to priority-queue (default).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 4
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 4
```

NOTE

a. To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the **gem add** command to configure the ID of the traffic profile bound to the GEM port.

b. For the ONU V800R308, the QoS mode cannot be set to **gem-car** or **flow-car**. To implement QoS in the upstream and downstream directions, other modes are adopted. For example, bind a T-CONT to a DBA profile or bind a traffic profile when creating traffic streams.

c. When the QoS mode is PQ, the default queue priority is 0; when the QoS is **gem-car** or **flow-car**, traffic profile 6 is bound to the port by default (no rate limitation).

d. Before running the **multi-service-port** command to create service ports in batches, ensure that the number of GEM ports is the same as the number of CVLANs. Therefore, you must create GEM ports according to the number of CVLANs. If there are 24 CVLANs,, 24 GEM ports need to be created.

e. If you run the **service-port** command to create service ports one by one, note that one GEM port can be bound to up to eight service ports. Create sufficient GEM ports according to the number of service ports. If there are 24 CVLANs, at least three GEM ports need to be created. This example adopts this mode and only one GEM port is created. For different service ports within the same GEM port, you only need to replace the **mapping-index** and replace the mapped VLAN with the CVLAN.

Configure the mapping between the GEM port and the ONU-side service to the VLAN mapping mode (default), map the service port of management service port (the CVLAN ID is 8) to GEM port 0, and map the Internet service port (the CVLAN ID is 1001) to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 1001
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to configure an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

a. Add an ONU.

ONU 1 and ONU 2 are connected to GPON port 0/2/1 through an optical splitter. The IDs of ONU 1 and ONU 2 are 1 and 2 respectively. The SN of ONU 1 is 32303131B39FD641 and that of ONU 2 is 32303131B39FD642. The management mode is SNMP and the line profile 10 is bound.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.

- Automatically find an ONU: If the password or SN of an ONU is unknown, run the **port ont-auto-find** command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth
32303131B39FD641
snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 ontid 2 sn-auth
32303131B39FD642
snmp ont-lineprofile-id 10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1

------------------------------------------------------------------------
---
   Number              : 1
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD641
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

------------------------------------------------------------------------
---
   Number              : 2
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD642
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

------------------------------------------------------------------------
---
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth
32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 2 sn-auth
32303131B39FD642 snmp ont-lineprofile-id 10
```

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

After an alarm profile is configured, bind it to the ONT. In this example, bind the default alarm profile, namely alarm profile 1 to the ONU.

```
huawei(config-if-gpon-0/2)#ont alarm-profile 1 1 profile-id 1
huawei(config-if-gpon-0/2)#ont alarm-profile 1 2 profile-id 1
```

5. Confirm that the ONU goes online normally.

NOTE

In this step, query the status of ONU 1 as an example. The same method is applied for querying the status of ONU 2.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1

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

  F/S/P                :
0/2/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU already goes
online normally.
  Config state        : normal    //Indicates that the configuration status
of the ONU is normal.

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

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

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the **gem add** command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   a. Configure the inband management VLAN and IP address of the OLT.

      To telnet to the ONU from the OLT and then configure the ONU, you need to configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.1 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU 1 to 192.168.50.2/24, the static IP address of the ONU 2 to 192.168.50.3/24 , the gateway to 192.168.50.254 and the management VLAN ID to 8 (the same as that of the OLT) .

      ```
      huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address
      192.168.50.2
      mask 255.255.255.0 gateway 192.168.50.254 vlan 8
      huawei(config-if-gpon-0/2)#ont ipconfig 1 2 static ip-address
      192.168.50.3
      ```

```
mask 255.255.255.0 gateway 192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

c. Configure an inband management service port.

Configure the management service port index to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. On the OLT, the rate of the inband service port is not limited. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** and **ping** ***192.168.50.3*** command to check the connectivity to the ONU 1 and ONU 2. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** and **telnet** ***192.168.50.3*** command to telnet to the ONU 1 and ONU 2 and then configure the ONU.
8. Create service ports.

Create service port 101 connected to ONU 1 and service port 102 connected to ONU 2. Set the SVLAN ID to 100, GEM port ID to 1, and CVLAN ID to 1001. The traffic rate of upstream and downstream packets is limited on the ONU and not limited on the OLT. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

Assume the split ratio is 1:128. ONU 1 is connected to port 1 on the optical splitter by using optical fiber and ONU 2 is connected to port 2. The user PC is connected to ONU port 1. The inner VLAN IDs are 258 and 260 after they are calculated according to the formula.

```
huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 1 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 102 vlan 100 gpon 0/2/1 ont 2 gemport 1 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 260 rx-cttr 6 tx-cttr 6
```

NOTE

- The OLT's CVLAN must be the same as the upstream VLAN of the ONU.
- Run the **service-port** to create service ports one by one. In this example, only one service port is created as an example. When a service port is created, note that it must correspond to the GEM port configured with the ONU line-profile and the CVLAN.
- You can also run the **multi-service-port** command to create service ports in batches. In the case of GPON access, you must set **ontid**+**gemindex** to specify a service port. In addition, the number of GEM ports must be the same as the number of CVLANs.

9. Configure the queue scheduling mode.

Adopt the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode and their weights are 10, 10, 20, 20, and 40 respectively. Queues 5-7 adopt the PQ mode. The priority of the Internet access service is 1, adopting the WRR mode.

NOTE

- The queue scheduling mode is configured globally, and you need to configure it only once on the OLT. After the configuration is complete, the queue scheduling mode takes effect globally. When subsequent services are configured, you do not need to configure the queue scheduling mode again.
- For a board that supports only four queues, the default mapping between the 802.1p priorities and queue IDs are as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

Configure the mapping between the 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
```

10. Save the data.

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

- **Configure the ONU.**

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

2. Configure the traffic profile.

   You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

   Add traffic profile 8, and set the CIR to 4 Mbit/s. The priority for upstream packets is 1. The downstream priority policy is scheduled by the priority that the packets bear.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 1 priority-
policy
tag-In-Package
```

3. Create an SVLAN.

   Create SVLANs 1001-1032 in batches whose type is smart and attribute is common. Add SVLANs to upstream port 0/0/1.

   NOTE

   - The VLAN ID must be consistent with the CVLAN of the OLT.
   - An MA5616 (ONU) provides two upstream ports 0/0/0 and 0/0/1 and supports self-adaptation among three modes.

```
huawei(config)#vlan 1001-1032 smart
huawei(config)#port vlan 1001-1032 0/0 1
```

4. Configure the ADSL2+ line profile.
   - Run the **display adsl line-profile** command to query the existing ADSL2+ line profiles in the current system. A profile can be directly used if it meets the requirements.
   - If no ADSL2+ line profile in the system meets the requirements, you need to add an ADSL2+ line profile. Run the **adsl line-profile quickadd** command to add an ADSL2+ line profile.

   The parameters in the ADSL2+ line profile should be configured according to actual line conditions. In this example, add ADSL2+ line profile 4 by using default settings for the parameters.

```
huawei(config)#adsl line-profile quickadd 4
```

5. Configure the ADSL2+ channel profile.
   - Run the **display adsl channel-profile** command to query the existing ADSL2+ channel profiles in the current system. A profile can be directly used if it meets the requirements.
   - If no ADSL2+ channel profile in the system meets the requirements, you need to add an ADSL2+ channel profile. Run the **adsl channel-profile quickadd** command to add an ADSL2+ channel profile.

   The data in the ADSL2+ channel profile must be configured according to the actual channel conditions. In this example, the traffic profile is used to limit the user access rate; therefore, when the ADSL2+ channel profile is configured, the line rate parameters do not need to be configured.

   Add ADSL2+ channel profile 4 and use default settings for the parameters.

   ```
   huawei(config)#adsl channel-profile quickadd 4
   ```

6. Configure the ADSL2+ line template.
   - Run the **display adsl line-template** command to query the existing ADSL2+ line templates in the current system. A template can be directly used if it meets the requirements.
   - If no ADSL2+ line template in the system meets the requirements, you need to add an ADSL2+ line template. Run the **adsl line-template quickadd** command to add an ADSL2+ line template.

   Bind the ADSL2+ line profile configured in **Step 4** and the ADSL2+ channel profile configured in **Step 5** to form ADSL2+ line template 3. Set the downstream rate adaptation ratio to 100% and the upstream rate adaptation ratio to 100%.

   ```
   huawei(config)#adsl line-template quickadd 3 line 4 channel1 4 100 100
   ```

7. Activate the ADSL2+ port and bind the line template to the ADSL2+ port.

   Activate ADSL2+ port 0/1/1 and bind line template 3 to it.

   NOTE

   The other ADSL2+ ports can be activated similarly. If you want to activate all the ports of a board, use the command **activate all**.

   ```
   huawei(config)#interface adsl 0/1
   huawei(config-if-adsl-0/1)#deactivate 1
   huawei(config-if-adsl-0/1)#activate 1 template-index 3
   ```

8. (Optional) Bind the ADSL2+ alarm template to the port.

   Bind default ADSL2+ alarm template 1 to the port. To meet actual requirements, you can run the **adsl alarm-template quickadd** command to add an ADSL2+ alarm template.

   ```
   huawei(config-if-adsl-0/1)#alarm-config 1 1
   ```

9. Add a service port to the VLAN.

   An MA5616 configured with an ADL board provides 32-channel ADSL2+ access services. Use one of the service virtual ports as an example. The SVLAN is 1001, VPI 8, VCI 35, CVLAN untagged. The other service virtual ports can be added similarly by replacing the right SVLAN and the ADSL2+ port ID.

   ```
   huawei(config)#service-port 101 vlan 1001 adsl 0/1/1 vpi 8 vci 35 multi-
   service user-vlan untagged rx-cttr 8 tx-cttr 8
   ```

NOTE

In the case of batch service provisioning, run the **multi-service-port** command to add service ports in batches.

10. Save the data.

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

----End

Result

Users can enjoy the high-speed Internet service with PC by PPPoE.

After configuration is complete, use PCs to perform PPPoE. If the system displays "Error 678", troubleshoot the fault as follows:

1. Perform PPPoE dialup on a PC. On the ONU, run the **display mac-address all** command to check whether there is a MAC address of the PC. If there is a MAC address of the PC, the PC is connected properly to the ONU. Proceed to **2**. If there is not such a MAC address, check whether the ONU is configured properly as follows:
   a. In the corresponding xDSL mode, run the **display port state** command to check the related port status.
      - If the port is in the activating state, wait until the port is activated and then create a service port.
      - If the port is in the deactivated state, run the **activate** command to activate the xDSL port and then create a service port.
   b. Check the SVLAN of the service port created by running the **service-port** command and check whether the port connected to the PC is properly configured. Ensure that **user-vlan** is set to untagged.
2. On the OLT, run the **display mac-address all** command to check whether there is a MAC address of the ONU connected to the PC. If there is such a MAC address, capture packets and mirror packets on the upper-layer switch to locate faults. If there is not such a MAC address, check whether the OLT is configured properly.
   - Check whether ONUs connected to the OLT have conflict MAC addresses. If there are conflict MAC addresses, change the conflict MAC addresses.
   - Check the SVLAN of the service port created by running the **service-port** command and check whether the port connected to the PC is properly configured. Ensure that **user-vlan** is consistent with ONU's upstream VLAN configuration.

Configuration File

On the OLT side.

```
vlan 100 smart
vlan attrib 100 satcking
port vlan 100 0/19 0
dba-profile add profile-name PPPOE type4 max 102400
ont-lineprofile gpon profile-id 10
tcont 4 dba-profile-name PPPOE
gem add 0 eth tcont 4
gem add 1 eth tcont 4
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 1001
commit
quit
```

```
interface gpon 0/2
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
ont confirm 1 ontid 2 sn-auth 32303131B39FD642 snmp ont-lineprofile-id 10
ont alarm-profile 1 1 profile-id 1
ont alarm-profile 1 2 profile-id 1
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
interface gpon 0/2
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 gateway
192.168.50.254 vlan 8
ont ipconfig 1 2 static ip-address 192.168.50.3 mask 255.255.255.0 gateway
192.168.50.254 vlan 8
service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 1 multi-service
 user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-cttr 6
service-port 102 vlan 100 gpon 0/2/1 ont 2 gemport 1 multi-service
 user-vlan 1001 tag-transform translate-and-add inner-vlan 260 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

On the ONU side.

```
traffic table ip index 8 cir 4096 priority 1 priority-policy tag-In-Package
vlan 1001-1032 smart
port vlan 1001-1032 0/0 1
adsl line-profile quickadd 4
adsl channel-profile quickadd 4
adsl line-template quickadd 3
interface adsl 0/1
deactivate 1
activate 1 template-index 3
alarm-config 1 1
service-port 101 vlan 1001 adsl 0/1/1 vpi 8 vci 35 multi-service user-vlan
 untagged rx-cttr 8 tx-cttr 8
save
```

10.4.2 Configuring the FTTB and FTTC Internet Access Services (VDSL2 Access)

The OLT is connected to a remote ONU that support VDSL2 access by using the GPON port to provide users with the high-speed Internet access service.

Service Requirements

- VLANs are divided are isolated different user groups, preventing broadcast storms and facilitating O&M.
- Users perform PPPoE dialup on PCs to implement high-speed Internet access.
- Two VLAN tags are used to precisely identify services and users.
- The same QoS is used for the same type of services on the same type of ONUs, facilitating management.

Prerequisite

- Corresponding ONU version: V800R309C00. If another version is used, the configuration differs slightly. For details, see the configuration guide of the corresponding ONU version.

- The VDSL mode of ONU is Normal (namely TR129).

  NOTE

  You can run the **display xdsl mode** command in the privilege mode to query the VDSL mode.

Background Information

ONUs that support VDSL2 access include MA5616, MA5662.

Procedure

- **Configure the OLT.**

  1. Create an SVLAN and configure its upstream port.

     On the OLT, each OLT, each slot of the OLT, or each PON port can be allocated with an SVLAN. In this example, an SVLAN is allocated to each slot. To precisely identify a user, stacking VLANs are used. This means to translate CVLANs on the OLT according to the planned VLAN IDs.

     Configure the SVLAN ID to 100, VLAN type to smart VLAN, and VLAN attribute to stacking. Add upstream port 0/19/0 to VLAN 100.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#vlan attrib 100 stacking
     huawei(config)#port vlan 100 0/19 0
     ```

  2. (Optional) Configure upstream link aggregation.

     In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured to implement protection between ports and load sharing. For details, see **10.3 Configuring Upstream Link Aggregation**.

  3. Configure GPON ONU profiles.

     GPON ONU profiles include the DBA profile, line profile,and alarm profile.

     - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
     - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
     - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

     a. Configure a DBA profile.

        You can run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

        Configure the DBA profile name to PPPoE, type to Type4, and maximum bandwidth to 100 Mbit/s.

        ```
        huawei(config)#dba-profile add profile-name PPPoE type4 max 102400
        ```

     b. Configure an ONU line profile.

Create GPON ONU line profile 10 and bind T-CONT 4 to DBA profile PPPoE. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name PPPoE
```

NOTE

The ID of the line profile to be created must not exist in the system. Please create proper ONU line profiles according to actual data plan. In this example, line profile 10 is used.

Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting Internet traffic streams. Bind GEM port 0 and GEM port 1 to T-CONT 4. Set the QoS mode to priority-queue (default).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 4
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 4
```

NOTE

a. To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the **gem add** command to configure the ID of the traffic profile bound to the GEM port.

b. For the ONU V800R308, the QoS mode cannot be set to **gem-car** or **flow-car**. To implement QoS in the upstream and downstream directions, other modes are adopted. For example, bind a T-CONT to a DBA profile or bind a traffic profile when creating traffic streams.

c. When the QoS mode is PQ, the default queue priority is 0; when the QoS is **gem-car** or **flow-car**, traffic profile 6 is bound to the port by default (no rate limitation).

d. Before running the **multi-service-port** command to create service ports in batches, ensure that the number of GEM ports is the same as the number of CVLANs. Therefore, you must create GEM ports according to the number of CVLANs. If there are 24 CVLANs,, 24 GEM ports need to be created.

e. If you run the **service-port** command to create service ports one by one, note that one GEM port can be bound to up to eight service ports. Create sufficient GEM ports according to the number of service ports. If there are 24 CVLANs, at least three GEM ports need to be created. This example adopts this mode and only one GEM port is created. For different service ports within the same GEM port, you only need to replace the **mapping-index** and replace the mapped VLAN with the CVLAN.

Configure the mapping between the GEM port and the ONU-side service to the VLAN mapping mode (default), map the service port of management service port (the CVLAN ID is 8) to GEM port 0, and map the Internet service port (the CVLAN ID is 1001) to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 1001
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

- Run the **gpon alarm-profile add** command to configure an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

   a. Add an ONU.

   ONU 1 and ONU 2 are connected to GPON port 0/2/1 through an optical splitter. The IDs of ONU 1 and ONU 2 are 1 and 2 respectively. The SN of ONU 1 is 32303131B39FD641 and that of ONU 2 is 32303131B39FD642. The management mode is SNMP and the line profile 10 is bound.

   There are two ways to add an ONU. Select either of the two ways according to actual conditions.

   - Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
   - Automatically find an ONU: If the password or SN of an ONU is unknown, run the **port ont-auto-find** command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

   To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth
32303131B39FD641
snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 ontid 2 sn-auth
32303131B39FD642
snmp ont-lineprofile-id 10
```

   To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1

-------------------------------------------------------------------------
---
   Number              : 1
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD641
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

-------------------------------------------------------------------------
---
   Number              : 2
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD642
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

-------------------------------------------------------------------------
---
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth
```

```
32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 2 sn-auth
32303131B39FD642 snmp ont-lineprofile-id 10
```

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

After an alarm profile is configured, bind it to the ONT. In this example, bind the default alarm profile, namely alarm profile 1 to the ONU.

```
huawei(config-if-gpon-0/2)#ont alarm-profile 1 1 profile-id 1
huawei(config-if-gpon-0/2)#ont alarm-profile 1 2 profile-id 1
```

5. Confirm that the ONU goes online normally.

NOTE

In this step, query the status of ONU 1 as an example. The same method is applied for querying the status of ONU 2.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1

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

  F/S/P                 :
0/2/1
  ONT-ID                :
1
  Control flag          : active    //Indicates that the ONU is
activated.
  Run state             : online    //Indicates that the ONU already goes
online normally.
  Config state        : normal    //Indicates that the configuration status
of the ONU is normal.

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

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

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the **gem add** command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

a. Configure the inband management VLAN and IP address of the OLT.

To telnet to the ONU from the OLT and then configure the ONU, you need to configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

b. Configure the inband management VLAN and IP address of the ONU.

Configure the static IP address of the ONU 1 to 192.168.50.2/24, the static IP address of the ONU 2 to 192.168.50.3/24 , the gateway to 192.168.50.254 and the management VLAN ID to 8 (the same as that of the OLT) .

```
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address
192.168.50.2
mask 255.255.255.0 gateway 192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#ont ipconfig 1 2 static ip-address
192.168.50.3
mask 255.255.255.0 gateway 192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

c. Configure an inband management service port.

Configure the management service port index to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. On the OLT, the rate of the inband service port is not limited. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** and **ping** ***192.168.50.3*** command to check the connectivity to the ONU 1 and ONU 2. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** and **telnet** ***192.168.50.3*** command to telnet to the ONU 1 and ONU 2 and then configure the ONU.
8. Create service ports.

Create service port 101 connected to ONU 1 and service port 102 connected to ONU 2. Set the SVLAN ID to 100, GEM port ID to 1, and CVLAN ID to 1001. The traffic rate of upstream and downstream packets is limited on the ONU and not limited on the OLT. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

Assume the split ratio is 1:128. ONU 1 is connected to port 1 on the optical splitter by using optical fiber and ONU 2 is connected to port 2. The user PC is connected to ONU port 1. The inner VLAN IDs are 258 and 260 after they are calculated according to the formula.

```
huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 1 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-
cttr 6
huawei(config)#service-port 102 vlan 100 gpon 0/2/1 ont 2 gemport 1 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 260 rx-cttr 6 tx-
cttr 6
```

NOTE

- The OLT's CVLAN must be the same as the upstream VLAN of the ONU.
- Run the **service-port** to create service ports one by one. In this example, only one service port is created as an example. When a service port is created, note that it must correspond to the GEM port configured with the ONU line-profile and the CVLAN.
- You can also run the **multi-service-port** command to create service ports in batches. In the case of GPON access, you must set **ontid**+**gemindex** to specify a service port. In addition, the number of GEM ports must be the same as the number of CVLANs.

9. Configure the queue scheduling mode.

   Adopt the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode and their weights are 10, 10, 20, 20, and 40 respectively. Queues 5-7 adopt the PQ mode. The priority of the Internet access service is 1, adopting the WRR mode.

   NOTE

   - The queue scheduling mode is configured globally, and you need to configure it only once on the OLT. After the configuration is complete, the queue scheduling mode takes effect globally. When subsequent services are configured, you do not need to configure the queue scheduling mode again.
   - For a board that supports only four queues, the default mapping between the 802.1p priorities and queue IDs are as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between the 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
   ```

10. Save the data.

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

- **Configure the ONU.**

  NOTE

  The configuration on ONU 1 and ONU 2 is the same. Take configuration on ONU 1 for example.

  1. Log in to the ONU to perform the configuration.

     On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

  2. Configure the traffic profile.

     You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Add traffic profile 8, and set the CIR to 4 Mbit/s. The priority for upstream packets is 1. The downstream priority policy is scheduled by the priority that the packets bear.

     ```
     huawei(config)#traffic table ip index 8 cir 4096 priority 1 priority-
     policy
     tag-In-Package
     ```

  3. Create an SVLAN.

     Create SVLANs 1001-1024 in batches whose type is smart and attribute is common. Add SVLANs to upstream port 0/0/1.

NOTE

- The VLAN ID must be consistent with the CVLAN of the OLT.
- An MA5616 (ONU) provides two upstream ports 0/0/0 and 0/0/1 and supports self-adaptation among three modes.

```
huawei(config)#vlan 1001-1024 smart
huawei(config)#port vlan 1001-1024 0/0 1
```

4. Configure a VDSL2 line profile.
   - Run the **display vdsl line-profile** command to query the existing VDSL2 line profiles in the current system. A profile can be directly used if it meets the requirements.
   - If no VDSL2 line profile in the system meets the requirements, you need to add a VDSL2 line profile. Run the **vdsl line-profile quickadd** command to quickly add a VDSL2 line profile.

   The data in the VDSL2 line profile must be configured according to the actual line conditions. In this example, quickly add VDSL2 line profile 4 by using default settings for the parameters.

   ```
   huawei(config)#vdsl line-profile quickadd 4
   ```

5. Configure the VDSL2 channel profile.
   - Run the **display vdsl channel-profile** command to query the existing VDSL2 channel profiles in the current system. A profile can be directly used if it meets the requirements.
   - If no VDSL2 channel profile in the system meets the requirements, you need to add a VDSL2 channel profile. Run the **vdsl channel-profile quickadd** command to add a VDSL2 channel profile.

   NOTE

   The data in the VDSL2 channel profile must be configured according to the actual channel conditions. In this example, the traffic profile is used to limit the subscriber access rate; therefore, when the VDSL2 channel profile is configured, the line rate parameters do not need to be configured.

   Quickly add VDSL2 channel profile 4 and use default settings for the parameters.

   ```
   huawei(config)#vdsl channel-profile quickadd 4
   ```

6. Configure the VDSL2 line template.
   - Run the **display vdsl line-template** command to query the existing VDSL2 line templates in the current system. A template can be directly used if it meets the requirements.
   - If no VDSL2 line template in the system meets the requirements, you need to add a VDSL2 line template. Run the **vdsl line-template quickadd** command to add a VDSL2 line template.

   Bind the VDSL2 line profile configured in **Step 4** and the VDSL2 channel profile configured in **Step 5** Set the downstream rate adaptation ratio to 100% and the upstream rate adaptation ratio to 100%.

   ```
   huawei(config)#vdsl line-template quickadd 3 line 4 channel1 4 100 100
   ```

7. Activate VDSL2 port 0/1/0 and bind line template 3 to it.

   NOTE

   The other VDSL2 ports can be activated similarly. If you want to activate all the ports of a board, use the command **activate all**.

```
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#activate 0 template-index 3
```

8. Bind the VDSL2 alarm template.

   In this example, bind default VDSL2 alarm template 1. To meet actual requirements, you can run the **vdsl alarm-template add** command to add a VDSL2 alarm template.

   ```
   huawei(config-if-vdsl-0/1)#alarm-config 0 1
   ```

9. Add a service port to the VLAN.

   Consider one of service virtual ports 101 for example. The SVLAN is 1001, VDSL mode PTM, CVLAN untagged. The other service virtual ports can be added similarly by replacing the right SVLAN and the VDSL port ID.

   ```
   huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-
   service user-vlan untagged rx-cttr 8 tx-cttr 8
   ```

   NOTE

   In the case of batch service provisioning, run the **multi-service-port** command to add service ports in batches.

10. Save the data.

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

----End

Result

Users can enjoy the high-speed Internet service with PC by PPPoE.

After configuration is complete, use PCs to perform PPPoE. If the system displays "Error 678", troubleshoot the fault as follows:

1. Perform PPPoE dialup on a PC. On the ONU, run the **display mac-address all** command to check whether there is a MAC address of the PC. If there is a MAC address of the PC, the PC is connected properly to the ONU. Proceed to **2**. If there is not such a MAC address, check whether the ONU is configured properly as follows:
   a. In the corresponding xDSL mode, run the **display port state** command to check the related port status.
      - If the port is in the activating state, wait until the port is activated and then create a service port.
      - If the port is in the deactivated state, run the **activate** command to activate the xDSL port and then create a service port.
   b. Check the SVLAN of the service port created by running the **service-port** command and check whether the port connected to the PC is properly configured. Ensure that **user-vlan** is set to untagged.
2. On the OLT, run the **display mac-address all** command to check whether there is a MAC address of the ONU connected to the PC. If there is such a MAC address, capture packets and mirror packets on the upper-layer switch to locate faults. If there is not such a MAC address, check whether the OLT is configured properly.
   - Check whether ONUs connected to the OLT have conflict MAC addresses. If there are conflict MAC addresses, change the conflict MAC addresses.
   - Check the SVLAN of the service port created by running the **service-port** command and check whether the port connected to the PC is properly configured. Ensure that **user-vlan** is consistent with ONU's upstream VLAN configuration.

Configuration File

On the OLT side.

```
vlan 100 smart
vlan attrib 100 satcking
port vlan 100 0/19 0
dba-profile add profile-name PPPOE type4 max 102400
ont-lineprofile gpon profile-id 10
tcont 4 dba-profile-name PPPOE
gem add 0 eth tcont 4
gem add 1 eth tcont 4
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 1001
commit
quit
interface gpon 0/2
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
ont confirm 1 ontid 2 sn-auth 32303131B39FD642 snmp ont-lineprofile-id 10
ont alarm-profile 1 1 profile-id 1
ont alarm-profile 1 2 profile-id 1
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
interface gpon 0/2
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 gateway
192.168.50.254 vlan 8
ont ipconfig 1 2 static ip-address 192.168.50.3 mask 255.255.255.0 gateway
192.168.50.254 vlan 8
service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 1 multi-service
 user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-cttr 6
service-port 102 vlan 100 gpon 0/2/1 ont 2 gemport 1 multi-service
 user-vlan 1001 tag-transform translate-and-add inner-vlan 260 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

On the ONU side.

```
traffic table ip index 8 cir 4096 priority 0 priority-policy tag-In-Package
vlan 1001-1024 smart
port vlan 1001-1024 0/0 1
vdsl line-profile quickadd 4
vdsl channel-profile quickadd 4
vdsl line-template quickadd 3 line 4 channel1 4 100 100
interface vdsl 0/1
deactivate 0
activate 0 template-index 3
alarm-config 0 1
service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-
cttr 8 tx-cttr 8
save
```

10.4.3 Configuring the FTTB and FTTC VoIP Services (Based on the H.248 Protocol)

The OLT is connected to a remote ONU that supports H.248 by using the GPON port to provide users with the VoIP service.

Service Requirements

- Users directly uses the existing phone sets for the voice service and no additional investment is required.
- The voice data is carried over the IP network, which reduces the communication costs to a great extent without compromising the communication quality.
- Compared with traditional PSTN networks, IP-based networks provide more powerful service functions and richer user experience.
- The polarity-reversal accounting is supported.

Prerequisite

- The MGC interface data and the PSTN user data corresponding to the MG interface must be configured on the MGC.
- Run the **display board 0** command to make sure the **Status** of the voice board of ONU is **Normal**.

Background Information

ONUs that support SIP include the MA5616, MA5603T.

An ONU support either H.248 or SIP. To query the current voice protocol on an ONU, run the **display protocol support** command. To change the voice protocol to the other one, delete the MG interface and run the **protocol support** command. After the configuration is complete, save it and restart the system to make the configuration take effect.

WARNING

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

Procedure

- **Configure the OLT.**
  1. Create an SVLAN and add an upstream port to it.

     Create smart VLAN 200 and add upstream port 0/19/0 to it.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. (Optional) Configure upstream link aggregation.

     In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured to implement protection between ports and load sharing. For details, see **10.3 Configuring Upstream Link Aggregation**.

  3. Configure GPON ONU profiles.

     GPON ONU profiles include the DBA profile, line profile,and alarm profile.

     - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.

- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

a. Configure a DBA profile.

   You can run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

   Configure the DBA profile name to VoIP, type to Type4, assure bandwidth to 15 Mbit/s and maximum bandwidth to 30 Mbit/s.

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

b. Configure an ONU line profile.

   Create GPON ONU line profile 10 and bind T-CONT 2 to DBA profile VoIP. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

   NOTE

   The ID of the line profile to be created must not exist in the system. Please create proper line profiles according to actual data plan. In this example, line profile 10 is used.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 2 dba-profile-name VoIP
```

   Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting VoIP service streams. Bind GEM port 0 and GEM port 1 to T-CONT 2. Set the QoS mode to priority-queue (default).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 2
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 2
```

   NOTE

   a. To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the **gem add** command to configure the ID of the traffic profile bound to the GEM port.

   b. For the ONU V800R308, the QoS mode cannot be set to **gem-car** or **flow-car**. To implement QoS in the upstream and downstream directions, other modes are adopted. For example, bind a T-CONT to a DBA profile or bind a traffic profile when creating traffic streams.

   c. When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

   d. Before running the **multi-service-port** command to create service ports in batches, ensure that the number of GEM ports is the same as the number of CVLANs. Therefore, you must create GEM ports according to the number of CVLANs. In this example, 24 GEM ports need to be created.

   e. If you run the **service-port** command to create service ports one by one, note that one GEM port can be bound to up to eight service ports. Create sufficient GEM ports according to the number of service ports. In this example, three GEM ports need to be created. This example adopts this mode and only one GEM port is created. For different service ports within the same GEM port, you only need to replace the **mapping-index** and replace the mapped VLAN with the CVLAN.

Configure the mapping between the GEM port and the ONU-side service to the VLAN mapping mode (default), map the service port of management (the CVLAN ID is 8) to GEM port 0, and map the service port of VoIP service (the CVLAN ID is 200) to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 200
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to configure an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

a. Add an ONU.

ONU 1 and ONU 2 are connected to GPON port 0/2/1 through an optical splitter. The IDs of ONU 1 and ONU 2 are 1 and 2 respectively. The SN of ONU 1 is 32303131B39FD641 and that of ONU 2 is 32303131B39FD642. The management mode is SNMP and the line profile 10 is bound.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the **port ont-auto-find** command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth
32303131B39FD641
snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 ontid 2 sn-auth
32303131B39FD642
snmp ont-lineprofile-id 10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1

------------------------------------------------------------------------
---
   Number              : 1
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD641
   Password            :
   Loid                : 0000000000
```

```
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

-------------------------------------------------------------------------
---
   Number              : 2
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD642
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

-------------------------------------------------------------------------
---
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth
32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 2 sn-auth
32303131B39FD642 snmp ont-lineprofile-id 10
```

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

After an alarm profile is configured, bind it to the ONT. In this example, bind the default alarm profile, namely alarm profile 1 to the ONU.

```
huawei(config-if-gpon-0/2)#ont alarm-profile 1 1 profile-id 1
huawei(config-if-gpon-0/2)#ont alarm-profile 1 2 profile-id 1
```

5. Confirm that the ONU goes online normally.

NOTE

In this step, query the status of ONU 1 as an example. The same method is applied for querying the status of ONU 2.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1

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

  F/S/P               :
0/2/1
  ONT-ID              :
1
  Control flag        : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes
online normally.
  Config state        : normal    //Indicates that the configuration status
of the ONU is normal.

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

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

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.

- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the **gem add** command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   a. Configure the inband management VLAN and IP address of the OLT.

      To telnet to the ONU from the OLT and then configure the ONU, you need to configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.1 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU 1 to 192.168.50.2/24, the static IP address of the ONU 2 to 192.168.50.3/24 , the gateway to 192.168.50.254 and the management VLAN ID to 8 (the same as that of the OLT) .

      ```
      huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address
      192.168.50.2
      mask 255.255.255.0 gateway 192.168.50.254 vlan 8
      huawei(config-if-gpon-0/2)#ont ipconfig 1 2 static ip-address
      192.168.50.3
      mask 255.255.255.0 gateway 192.168.50.254 vlan 8
      huawei(config-if-gpon-0/2)#quit
      ```

   c. Configure an inband management service port.

      Configure the management service port index to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. On the OLT, the rate of the inband service port is not limited. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

      ```
      huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-
      service
      user-vlan 8 rx-cttr 6 tx-cttr 6
      huawei(config)#service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-
      service
      user-vlan 8 rx-cttr 6 tx-cttr 6
      ```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** and **ping** ***192.168.50.3*** command to check the connectivity to the ONU 1 and ONU 2. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** and **telnet** ***192.168.50.3*** command to telnet to the ONU 1 and ONU 2 and then configure the ONU.
8. Configure the traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 9, and no rate limitation on user packets. The priority is 6 and the priority policy is scheduled by the priority that the packets bear.

```
huawei(config)#traffic table ip index 9 cir off priority 6 priority-policy
tag-In-Package
```

9. Create a service port.

   Create service port 200 connected to ONU 1 and service port 201 connected to ONU 2. SVLAN ID to 200, GEM port ID to 1, bind traffic profile 9 and CVLAN ID to 200.

   NOTE

   The CVLAN must be consistent with the upstream VLAN of the ONU.

   ```
   huawei(config)#service-port 200 vlan 200 gpon 0/2/1 ont 1 gemport 1 multi-
   service user-vlan 200 rx-cttr 9 tx-cttr 9
   huawei(config)#service-port 201 vlan 200 gpon 0/2/1 ont 2 gemport 1 multi-
   service user-vlan 200 rx-cttr 9 tx-cttr 9
   ```

10. Configure the queue scheduling mode.

    Adopt the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode and their weights are 10, 10, 20, 20, and 40 respectively. Queues 5-7 adopt the PQ mode. The priority of the VoIP service is 6, adopting the PQ mode.

    NOTE

    - The queue scheduling mode is configured globally, and you need to configure it only once on the OLT. After the configuration is complete, the queue scheduling mode takes effect globally. When subsequent services are configured, you need not configure the queue scheduling mode again.
    - For a board that supports only four queues, the mapping between the 802.1p priorities and queue IDs are as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

    ```
    huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
    ```

    Configure the mapping between the 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
    ```

11. Save the data.

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

- **Configure the ONU.**

  NOTE

  The configuration on ONU 1 and ONU 2 is the same. Take configuration on ONU 1 for example.

  1. Log in to the ONU to perform the configuration.

     On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

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

     Create VLAN 200 and add upstream port 0/0/1 (0/9/0 for MA5603T) to the VLAN. Configure the IP address of the VLAN Layer 3 interface to 17.10.10.10 and subnet mask to 255.255.255.0,

NOTE

- The VLAN ID must be consistent with the CVLAN of the OLT.
- The VLAN ID of the default upstream Ethernet port is 1. Use the default VLAN if no specific VLAN is required for the upstream transmission.
- If you need to use another VLAN to transmit packets in the upstream direction, run the **port vlan** command to add the specified upstream port to the VLAN.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0 1  //for MA5616
huawei(config)#port vlan 200 0/9 0  //for MA5603T
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 17.10.10.10 24
huawei(config-if-vlanif200)#quit
```

3. Configure the media and signaling IP address pools.

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

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

NOTE

- You can configure the attributes of the MG interface only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The media IP address and the signaling IP address can be different. You can plan the IP addresses according to the actual network.

4. Configure the static route.

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

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

5. Add an MG interface.

   Add MG interface 0.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

6. Configure the attributes of the MG interface.
   - Signaling IP address: 17.10.10.10
   - Coding mode: text
   - Port number of the transport layer protocol: 2944
   - Transfer mode: UDP
   - IP address of the primary MGC: 200.200.200.200
   - Port number of the transport layer protocol of the primary MGC: 2944
   - Media IP address 1: 17.10.10.10
   - The beginning negotiation version of H248 protocol: V2

NOTE

You must confirm these as follows before configuring the MG interface.

- The enrollment type of the MG interface: IP address or the domain name. It must be the same strictly.
- The beginning negotiation version of H248 protocol: V1, V2 or V3 (default). Some softswitches do not support the V3 version, resulting in the MG interface cannot enroll.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 17.10.10.10 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-
```

```
port
 2944 mg-media-ip1 17.10.10.10
```

7. Reset the MG interface.

   NOTE

   - You must reset the MG interface after configuring and set the type to cold reset. Otherwise the MG interface is invalid.
   - Only the mgip, mgport, mgcip_1 (or mgc-domain-name1), mgcport_1, code, transfer, mg-media-ip parameters are set correctly, you can cold reset the MG interface.

   ```
   huawei(config-if-h248-0)#reset coldstart
     Are you sure to reset MG interface?(y/n)[n]:y
   huawei(config-if-h248-0)#quit
   ```

8. Configure the PSTN user data.

   Configure the telephone number of the user on port 0/2/0 to 0/2/23, telephone number of the user from 83110001 to 83110024, and terminal ID to 0.

   NOTE

   - This telephone number is used to self-exchange, means the communication of extension. The real telephone numbers are ranged by MGC.
   - The ONU configured with an ASRB board has 32 POTS ports and an MA5616 configured with an ASPB board has 64 POTS ports. Configuring 24 PSTN users is used as an example.
   - To configure the PSTN data of a single user, run the **mgpstnuser add** command.
   - To configure the PSTN data of multiple users in batches, run the **mgpstnuser batadd** command.
   - If the user of the MG interface is configured to support terminal layering, you need not configure the terminal ID and the system automatically allocates it. If the user of the MG interface does not support terminal layering, this parameter is mandatory. The terminal ID must be unique on one MG interface.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#mgpstnuser batadd 0/2/0 0/2/23 0 terminalid 0
   telno 83110001
   ```

9. Change the call priority of the PSTN user.

   Configure the call priority of the user on port 0/2/0 to Cat2 and the users of 0/2/1 to 0/2/23 to Cat3 (Default)

   ```
   huawei(config-esl-user)#mgpstnuser modify 0/2/0 priority cat2
   huawei(config-esl-user)#quit
   ```

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

    Modify the attributes of the PSTN port 0/2/0 to 0/2/23 so that the PSTN ports support the polarity reversal.

    ```
    huawei(config)#pstnport
    huawei(config-pstnport)#pstnport attribute batset 0/2/0 0/2/23 reverse-
    pole-pulse enable
    huawei(config-pstnport)#quit
    ```

11. Save the data.

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

----End

Result

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

- The caller can hear the dial tone after picking up the phone.

- When the caller dials the phone number of the callee, the phone of the callee can ring normally, and the caller can hear the ringback tone.
- The caller and the callee can communicate with each other successfully.
- After the callee hangs up the phone, the caller can hear the busy tone.

Configuration File

On the OLT side.

```
vlan 200 smart
port vlan 200 0/19 0
dba-profile add profile-name VoIP type3 assure 15360 max 30720
ont-lineprofile gpon profile-id 10
tcont 2 dba-profile-name VoIP
gem add 0 eth tcont 2
gem add 1 eth tcont 2
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 200
commit
quit
interface gpon 0/2
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
ont confirm 1 ontid 2 sn-auth 32303131B39FD642 snmp ont-lineprofile-id 10
ont alarm-profile 1 1 profile-id 1
ont alarm-profile 1 2 profile-id 1
quit
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
interface gpon 0/2
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont ipconfig 1 2 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
quit
traffic table ip index 9 cir off priority 6 priority-policy tag-In-Package
service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 200 vlan 200 gpon 0/2/1 ont 1 gemport 1 multi-service
 user-vlan 200 rx-cttr 9 tx-cttr 9
service-port 201 vlan 200 gpon 0/2/1 ont 2 gemport 1 multi-service
 user-vlan 200 rx-cttr 9 tx-cttr 9
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
```

On the ONU side.

```
vlan 200 smart
port vlan 200 0/0 1  //for MA5616
port vlan 200 0/9 0  //for MA5603T
interface vlanif 200
ip address 17.10.10.10 24
quit
voip
ip address media 17.10.10.10 17.10.10.1
ip address signaling 17.10.10.10
quit
ip route-static 200.200.200.0 24 17.10.10.1
interface h248 0
if-h248 attribute mgip 17.10.10.10 mgport 2944 code text transfer
 udp primary-mgc-ip1 200.200.200.200 primary-mgc-port 2944 mg-media-ip1
17.10.10.10
 start-negotiate-version 2
```

```
reset coldstart
quit
esl user
mgpstnuser batadd 0/2/0 0/2/23 0 terminalid 0 telno 83110001
mgpstnuser modify 0/2/0 priority cat2
quit
pstnport
pstnport attribute batset 0/2/0 0/2/23 reverse-pole-pulse enable
quit
save
```

10.4.4 Configuring the FTTB and FTTC VoIP Services (Based on the SIP Protocol)

The OLT is connected to a remote ONU that supports SIP by using the GPON port to provide users with the VoIP service.

Service Requirements

- Users directly uses the existing phone sets for the voice service and no additional investment is required.
- The voice data is carried over the IP network, which reduces the communication costs to a great extent without compromising the communication quality.
- Compared with traditional PSTN networks, IP-based networks provide more powerful service functions and richer user experience.
- The polarity-reversal accounting is supported.

Prerequisite

- The PSTN user data corresponding to the SIP interface must be configured on the IMS.
- Run the **display board 0** command to ensure that the **Status** of the voice board of ONU is **Normal**.

Background Information

ONUs that support SIP include the MA5616, MA5603T.

An ONU support either H.248 or SIP. To query the current voice protocol on an ONU, run the **display protocol support** command. To change the voice protocol to the other one, delete the MG interface and run the **protocol support** command. After the configuration is complete, save it and restart the system to make the configuration take effect.

WARNING

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

An ONU support either H.248 or SIP. To query the current voice protocol on an ONU, run the **display protocol support** command. To change the voice protocol to the other one, delete the MG interface and run the **protocol support** command. After the configuration is complete, save it and restart the system to make the configuration take effect. This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Procedure

- **Configure the OLT.**

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

     Create smart VLAN 200 and add upstream port 0/19/0 to it.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. (Optional) Configure upstream link aggregation.

     In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured to implement protection between ports and load sharing. For details, see **10.3 Configuring Upstream Link Aggregation**.

  3. Configure GPON ONU profiles.

     GPON ONU profiles include the DBA profile, line profile,and alarm profile.

     - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
     - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
     - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

     a. Configure a DBA profile.

        You can run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

        Configure the DBA profile name to VoIP, type to Type4, assure bandwidth to 15 Mbit/s and maximum bandwidth to 30 Mbit/s.

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

     b. Configure an ONU line profile.

        Create GPON ONU line profile 10 and bind T-CONT 2 to DBA profile VoIP. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

        NOTE

        The ID of the line profile to be created must not exist in the system. Please create proper line profiles according to actual data plan. In this example, line profile 10 is used.

        ```
        huawei(config)#ont-lineprofile gpon profile-id 10
        huawei(config-gpon-lineprofile-10)#tcont 2 dba-profile-name VoIP
        ```

        Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting VoIP service streams. Bind GEM port 0 and GEM port 1 to T-CONT 2. Set the QoS mode to priority-queue (default).

        ```
        huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 2
        huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 2
        ```

NOTE

a. To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the **gem add** command to configure the ID of the traffic profile bound to the GEM port.

b. For the ONU V800R308, the QoS mode cannot be set to **gem-car** or **flow-car**. To implement QoS in the upstream and downstream directions, other modes are adopted. For example, bind a T-CONT to a DBA profile or bind a traffic profile when creating traffic streams.

c. When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

d. Before running the **multi-service-port** command to create service ports in batches, ensure that the number of GEM ports is the same as the number of CVLANs. Therefore, you must create GEM ports according to the number of CVLANs. In this example, 24 GEM ports need to be created.

e. If you run the **service-port** command to create service ports one by one, note that one GEM port can be bound to up to eight service ports. Create sufficient GEM ports according to the number of service ports. In this example, three GEM ports need to be created. This example adopts this mode and only one GEM port is created. For different service ports within the same GEM port, you only need to replace the **mapping-index** and replace the mapped VLAN with the CVLAN.

Configure the mapping between the GEM port and the ONU-side service to the VLAN mapping mode (default), map the service port of management (the CVLAN ID is 8) to GEM port 0, and map the service port of VoIP service (the CVLAN ID is 200) to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 200
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to configure an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

a. Add an ONU.

ONU 1 and ONU 2 are connected to GPON port 0/2/1 through an optical splitter. The IDs of ONU 1 and ONU 2 are 1 and 2 respectively. The SN of ONU 1 is 32303131B39FD641 and that of ONU 2 is 32303131B39FD642. The management mode is SNMP and the line profile 10 is bound.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.

- Automatically find an ONU: If the password or SN of an ONU is unknown, run the **port ont-auto-find** command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth
32303131B39FD641
snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 ontid 2 sn-auth
32303131B39FD642
snmp ont-lineprofile-id 10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1

------------------------------------------------------------------------
---
   Number              : 1
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD641
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

------------------------------------------------------------------------
---
   Number              : 2
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD642
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

------------------------------------------------------------------------
---
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth
32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 2 sn-auth
32303131B39FD642 snmp ont-lineprofile-id 10
```

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

After an alarm profile is configured, bind it to the ONT. In this example, bind the default alarm profile, namely alarm profile 1 to the ONU.

```
huawei(config-if-gpon-0/2)#ont alarm-profile 1 1 profile-id 1
huawei(config-if-gpon-0/2)#ont alarm-profile 1 2 profile-id 1
```

5. Confirm that the ONU goes online normally.

NOTE

In this step, query the status of ONU 1 as an example. The same method is applied for querying the status of ONU 2.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1

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

  F/S/P                :
0/2/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU already goes
online normally.
  Config state        : normal    //Indicates that the configuration status
of the ONU is normal.

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

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

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the **gem add** command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   a. Configure the inband management VLAN and IP address of the OLT.

      To telnet to the ONU from the OLT and then configure the ONU, you need to configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.1 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU 1 to 192.168.50.2/24, the static IP address of the ONU 2 to 192.168.50.3/24 , the gateway to 192.168.50.254 and the management VLAN ID to 8 (the same as that of the OLT) .

      ```
      huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address
      192.168.50.2
      mask 255.255.255.0 gateway 192.168.50.254 vlan 8
      huawei(config-if-gpon-0/2)#ont ipconfig 1 2 static ip-address
      192.168.50.3
      ```

```
mask 255.255.255.0 gateway 192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

c. Configure an inband management service port.

Configure the management service port index to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. On the OLT, the rate of the inband service port is not limited. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** and **ping** ***192.168.50.3*** command to check the connectivity to the ONU 1 and ONU 2. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** and **telnet** ***192.168.50.3*** command to telnet to the ONU 1 and ONU 2 and then configure the ONU.
8. Configure the traffic profile.

   You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

   Add traffic profile 9, and no rate limitation on user packets. The priority is 6 and the priority policy is scheduled by the priority that the packets bear.

   ```
   huawei(config)#traffic table ip index 9 cir off priority 6 priority-policy
   tag-In-Package
   ```

9. Create a service port.

   Create service port 200 connected to ONU 1 and service port 201 connected to ONU 2. SVLAN ID to 200, GEM port ID to 1, bind traffic profile 9 and CVLAN ID to 200.

   NOTE

   The CVLAN must be consistent with the upstream VLAN of the ONU.

   ```
   huawei(config)#service-port 200 vlan 200 gpon 0/2/1 ont 1 gemport 1 multi-
   service user-vlan 200 rx-cttr 9 tx-cttr 9
   huawei(config)#service-port 201 vlan 200 gpon 0/2/1 ont 2 gemport 1 multi-
   service user-vlan 200 rx-cttr 9 tx-cttr 9
   ```

10. Configure the queue scheduling mode.

    Adopt the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode and their weights are 10, 10, 20, 20, and 40 respectively. Queues 5-7 adopt the PQ mode. The priority of the VoIP service is 6, adopting the PQ mode.

    NOTE

    - The queue scheduling mode is configured globally, and you need to configure it only once on the OLT. After the configuration is complete, the queue scheduling mode takes effect globally. When subsequent services are configured, you need not configure the queue scheduling mode again.
    - For a board that supports only four queues, the mapping between the 802.1p priorities and queue IDs are as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

Configure the mapping between the 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
```

11. Save the data.

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

- **Configure the ONU.**

NOTE

The configuration on ONU 1 and ONU 2 is the same. Take configuration on ONU 1 for example.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

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

   Create VLAN 200 and add upstream port 0/0/1 (0/9/0 for MA5603T) to the VLAN. Configure the IP address of the VLAN Layer 3 interface to 17.10.10.10 and subnet mask to 255.255.0.0.

   NOTE

   - The VLAN ID must be consistent with the CVLAN of the OLT.
   - The VLAN ID of the default upstream Ethernet port is 1. Use the default VLAN if no specific VLAN is required for the upstream transmission.
   - If you need to use another VLAN to transmit packets in the upstream direction, run the **port vlan** command to add the specified upstream port to the VLAN.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0 1  //for MA5616
huawei(config)#port vlan 200 0/9 0  //for MA5603T
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 17.10.10.10 24
huawei(config-if-vlanif200)#quit
```

3. Configure the media and signaling IP address pools.

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

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

   NOTE

   - You can configure the attributes of the 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.

4. Configure the static route.

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

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

5. Add an SIP interface.

   Add SIP interface 0.

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

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

   When the ONU is MA5616 with version of V800R306, run the command as follows:

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

   When the ONU is MA5603T, or MA5616 with a version newer than V800R306, run the command as follows:

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

7. Configure the optional attributes of the SIP interface.

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

8. Reset the SIP interface.

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

9. Configure the PSTN user data.

   Configure the telephone number of the user on port 0/2/0 to 0/2/23, telephone number of the user from 83110001 to 83110024, and terminal ID to 0.

   NOTE

   - The ONU configured with an ASRB board has 32 POTS ports and an MA5616 configured with an ASPB board has 64 POTS ports. Configuring 24 PSTN users is used as an example.
   - To configure the PSTN data of a single user, run the **sippstnuser add** command.
   - To configure the PSTN data of multiple users in batches, run the **sippstnuser batadd** command.

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/2/0 0/2/23 0 telno 83110001
```

10. Change the call priority of the PSTN user.

    Configure the call priority of the user on port 0/2/0 to Cat2 and the users of 0/2/1 to 0/2/23 to Cat3 (Default)

```
huawei(config-esl-user)#sippstnuser attribute set 0/2/0 priority cat2
huawei(config-esl-user)#quit
```

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

Modify the attributes of the PSTN port 0/2/0 to 0/2/23 so that the PSTN ports support the polarity reversal.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/2/0 0/2/23 reverse-pole-pulse enable
huawei(config-pstnport)#quit
```

12. Save the data.

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

----End

Result

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

- The caller can hear the dial tone after picking up the phone.
- When the caller dials the phone number of the callee, the phone of the callee can ring normally, and the caller can hear the ringback tone.
- The caller and the callee can communicate with each other successfully.
- After the callee hangs up the phone, the caller can hear the busy tone.

Configuration File

On the OLT side.

```
vlan 200 smart
port vlan 200 0/19 0
dba-profile add profile-name VoIP type3 assure 15360 max 30720
ont-lineprofile gpon profile-id 10
tcont 2 dba-profile-name VoIP
gem add 0 eth tcont 2
gem add 1 eth tcont 2
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 200
commit
quit
interface gpon 0/2
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
ont confirm 1 ontid 2 sn-auth 32303131B39FD642 snmp ont-lineprofile-id 10
ont alarm-profile 1 1 profile-id 1
ont alarm-profile 1 2 profile-id 1
quit
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
interface gpon 0/2
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont ipconfig 1 2 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
quit
traffic table ip index 9 cir off priority 6 priority-policy tag-In-Package
service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 200 vlan 200 gpon 0/2/1 ont 1 gemport 1 multi-service
 user-vlan 200 rx-cttr 9 tx-cttr 9
service-port 201 vlan 200 gpon 0/2/1 ont 2 gemport 1 multi-service
 user-vlan 200 rx-cttr 9 tx-cttr 9
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
```

On the ONU side.

```
vlan 200 smart
port vlan 200 0/0 1  //for MA5616
port vlan 200 0/9 0  //for MA5603T
interface vlanif 200
ip address 17.10.10.10 24
quit
voip
ip address media 17.10.10.10 17.10.10.1
ip address signaling 17.10.10.10
quit
ip route-static 200.200.200.0 24 17.10.10.1
interface sip 0

if-sip attribute basic media-ip 17.10.10.10 signal-ip 17.10.10.10
 signal-port 5060 transfer udp primary-proxy-ip1 200.200.200.200
 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
//When the ONU is MA5616 with version of V800R306

if-sip attribute basic media-ip 17.10.10.10
 signal-ip 17.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1
200.200.200.200 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
//When the ONU is MA5603T, or MA5616 with a version newer than V800R306

reset
quit
esl user
sippstnuser batadd 0/2/0 0/2/23 0 telno 83110001
sippstnuser attribute set 0/2/0 priority cat2
quit
pstnport
pstnport attribute batset 0/2/0 0/2/23 reverse-pole-pulse enable
quit
save
```

10.4.5 Configuring the FTTB and FTTC IPTV Multicast Services

The OLT is connected to a remote ONU through the GPON port to provide users with the high-speed Internet access service. This topic considers the MA5620 as an example, and uses the GPBC board on the OLT.

Service Requirements

- The user set-top box (STB) is connected to the ONU 1 and ONU 2 through FE port, and the ONU 1 and ONU 2 are connected to the OLT and then to the upper-layer network through GPON, implementing the IPTV service.
- The DBA of the IPTV service adopts the maximum bandwidth mode, and no rate limitation is performed on the upstream and downstream traffic.
- The OLT adopts IGMP proxy and the ONU adopts IGMP snooping.
- Multicast programs are configured statically.
- Multicast logs are reported to the log server in the CDR format.

Prerequisite

The license for the multicast program or the multicast user must already be requested and installed.

Procedure

- **Configure the OLT.**

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

     Create smart VLAN 1000 and add upstream port 0/19/0 to it.

     ```
     huawei(config)#vlan 1000 smart
     huawei(config)#port vlan 1000 0/19 0
     ```

  2. (Optional) Configure upstream link aggregation.

     In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured to implement protection between ports and load sharing. For details, see **10.3 Configuring Upstream Link Aggregation**.

  3. Configure GPON ONU profiles.

     GPON ONU profiles include the DBA profile, line profile,and alarm profile.

     - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
     - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
     - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

     a. Configure a DBA profile.

        You can run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

        Configure the DBA profile name to IPTV, type to Type4, and upstream bandwidth to 100 Mbit/s.

        ```
        huawei(config)#dba-profile add profile-name IPTV type4 max 102400
        ```

     b. Add an ONU line profile.

        Add GPON ONU line profile 10 and bind T-CONT 3 to DBA profile named IPTV. In this way, the T-CONT can flexibly provide DBA solutions based on different configurations in the DBA profile.

        NOTE

        The ONU line profile to be created must not exist in the system. Please create proper ONU line profile according to actual data plan. This topic considers creating the ONU line profile 10 for example.

        ```
        huawei(config)#ont-lineprofile gpon profile-id 10
        huawei(config-gpon-lineprofile-10)#tcont 3 dba-profile-name IPTV
        ```

        Add GEM port 0 for carrying management traffic streams and GEM port 1 for carrying traffic streams of the IPTV service. Bind GEM port 0 and GEM port 1 to T-CONT 3. Configure the QoS mode to priority-queue (default).

        ```
        huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 3 cascade on
        huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 3 cascade on
        ```

NOTE

a. To change the default QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the **gem add** command to configure the index of the traffic profile to which the GEM port is bound.

b. For the ONU V800R308, the QoS mode cannot be set to gem-car or flow-car. To implement QoS in the upstream and downstream directions, other modes are adopted. For example, bind a T-CONT to a DBA profile or bind a traffic profile when creating traffic streams.

c. When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound by default (no rate limitation).

d. Before running the **multi-service-port** command to create service ports in batches, ensure that the number of GEM ports is the same as the number of CVLANs. Therefore, you must create GEM ports according to the number of CVLANs. In this example, 24 GEM ports need to be created.

e. If you run the **service-port** command to create service ports one by one, note that one GEM port can be bound to up to eight service ports. Create sufficient GEM ports according to the number of service ports. In this example, three GEM ports need to be created. This example adopts this mode and only one GEM port is created. For different service ports within the same GEM port, you only need to replace the **mapping-index** and replace the mapped VLAN with the CVLAN.

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management (CVLAN 8) to GEM port 0, and map the service port of IPTV service port (CVLAN 1000) to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 1000
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to configure an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

a. Add an ONU.

ONU 1 and ONU 2 are connected to GPON port 0/2/1 through an optical splitter. The IDs of ONU 1 and ONU 2 are 1 and 2 respectively. The SN of ONU 1 is 32303131B39FD641 and that of ONU 2 is 32303131B39FD642. The management mode is SNMP and the line profile 10 is bound.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the **port ont-auto-find** command in the GPON mode to enable the ONU

auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth
32303131B39FD641
snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont add 1 ontid 2 sn-auth
32303131B39FD642
snmp ont-lineprofile-id 10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1

-------------------------------------------------------------------------
---
   Number              : 1
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD641
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

-------------------------------------------------------------------------
---
   Number              : 2
   F/S/P               : 0/2/1
   Ont SN              : 32303131B39FD642
   Password            :
   Loid                : 0000000000
   Checkcode           :
   VenderID            : HWTC
   Ont Version         : MA5616 VER.B
   Ont SoftwareVersion : V8R309 C00
   Ont EquipmentID     : SmartAX MA5616
   Ont autofind time   : 2011-05-10 10:06:00+08:00

-------------------------------------------------------------------------
---
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth
32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 2 sn-auth
32303131B39FD642 snmp ont-lineprofile-id 10
```

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

After an alarm profile is configured, bind it to the ONT. In this example, bind the default alarm profile, namely alarm profile 1 to the ONU.

```
huawei(config-if-gpon-0/2)#ont alarm-profile 1 1 profile-id 1
huawei(config-if-gpon-0/2)#ont alarm-profile 1 2 profile-id 1
```

5. Confirm that the ONU goes online normally.

NOTE

In this step, query the status of ONU 1 as an example. The same method is applied for querying the status of ONU 2.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1

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

  F/S/P                :
0/2/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU already goes
online normally.
  Config state        : normal    //Indicates that the configuration status
of the ONU is normal.

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

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

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the **gem add** command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   a. Configure the inband management VLAN and IP address of the OLT.

      To telnet to the ONU from the OLT and then configure the ONU, you need to configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.1 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU 1 to 192.168.50.2/24, the static IP address of the ONU 2 to 192.168.50.3/24 , the gateway to 192.168.50.254 and the management VLAN ID to 8 (the same as that of the OLT) .

      ```
      huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address
      192.168.50.2
      mask 255.255.255.0 gateway 192.168.50.254 vlan 8
      huawei(config-if-gpon-0/2)#ont ipconfig 1 2 static ip-address
      192.168.50.3
      mask 255.255.255.0 gateway 192.168.50.254 vlan 8
      huawei(config-if-gpon-0/2)#quit
      ```

   c. Configure an inband management service port.

      Configure the management service port index to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. On the OLT, the rate of the inband

service port is not limited. Therefore, use default traffic profile 6. To limit the rate of a service port, run the **traffic table ip** command to create a traffic profile and then bind the profile to the service port.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** and **ping** ***192.168.50.3*** command to check the connectivity to the ONU 1 and ONU 2. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** and **telnet** ***192.168.50.3*** command to telnet to the ONU 1 and ONU 2 and then configure the ONU.
8. Create a service port.

   Create service port 1000 connected to ONU 1 and service port 1001 connected to ONU 2. SVLAN ID to 1000, GEM port ID to 1, and CVLAN ID to 1001. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

   NOTE

   The CVLAN must be consistent with the upstream VLAN of the ONU.

```
huawei(config)#service-port 1000 vlan 1000 gpon 0/2/1 ont 1 gemport 1
multi-service user-vlan 1000 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 1001 vlan 1000 gpon 0/2/1 ont 2 gemport 1
multi-service user-vlan 1000 rx-cttr 6 tx-cttr 6
```

9. Configure the queue scheduling mode.

   Adopt the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode and their weights are 10, 10, 20, 20, and 40 respectively. Queues 5-7 adopt the PQ mode. The priority of the IPTV service is 4, adopting the WRR mode.

   NOTE

   - The queue scheduling mode is configured globally, and you need to configure it only once on the OLT. After the configuration is complete, the queue scheduling mode takes effect globally. When subsequent services are configured, you do not need to configure the queue scheduling mode again.
   - For a board that supports only four queues, the mapping between the 802.1p priorities and queue IDs are as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

   Configure the mapping between the 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
```

10. Configure a multicast subtending port.

    Configure port 0/2/1 connected to the ONU as a multicast subtending port.

```
huawei(config)#btv
huawei(config-btv)#igmp cascade-port 0/2/1 ontid 1 gemport 1
huawei(config-btv)#igmp cascade-port 0/2/1 ontid 2 gemport 1
```

NOTE

If no multicast subtending port is configured and multicast users are directly configured, the maximum number of multicast users that each multicast user can demand is limited. If multicast users are directly configured:

- To set authentication of a multicast user, run the **igmp profile add** command to create a right profile, run the **igmp profile** command to modify right parameters in the profile, and then run the **igmp user bind-profile** command to bind the right profile to the multicast user.
- To authenticate a multicast user, remove parameter **no-auth** when adding the multicast user.

The corresponding procedure is as follows:

```
huawei(config-btv)#igmp user add service-port 1000 no-auth
huawei(config-btv)#igmp user add service-port 1001 no-auth
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1001
```

11. Set the IGMP version.

    Use IGMP V3.

    ```
    huawei(config)#multicast-vlan 1000
    huawei(config-mvlan10000)#igmp version v3
    ```

12. Select the IGMP mode.

    Select the IGMP proxy mode.

    ```
    huawei(config-mvlan10000)#igmp mode proxy
      Are you sure to change IGMP mode?(y/n)[n]:y
    ```

13. Configure the 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-mvlan10000)#igmp uplink-port 0/19/0
    ```

14. Set the multicast global parameters.

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

15. Configure the program library.

    The multicast IP address of the program is 224.1.1.10 and the IP address of the program source is 10.10.10.10

    ```
    huawei(config-mvlan10000)#igmp program add name program1 ip 224.1.1.10
    sourceip 10.10.10.10
    ```

16. Configure a log server.

    Enable CDR log reporting, and configure the IP address of the active server to 10.10.10.20.

    ```
    huawei(config-mvlan10000)#btv
    huawei(config-btv)#igmp cdr enable
    huawei(config-btv)#quit
    huawei(config)#file-server auto-backup cdr primary 10.10.10.20 tftp
    ```

17. Save the data.

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

- **Configure the ONU.**

  1. Log in to the ONU to perform the configuration.

     On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

  2. Configure the traffic profile.

     You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 10, and no rate limitation on user packets. The priority is 4, bind the traffic profile 8 and the priority policy is scheduled by the priority that the packets bear.

```
huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy tag-In-Package
```

3. Configure a VLAN and add an upstream port to the VLAN.

   Create S-VLAN 1000 and add upstream port 0/0/1 to S-VLAN 1000.

   NOTE

   The CVLAN must be consistent with the upstream VLAN of the ONU.

   ```
   huawei(config)#vlan 1000
   huawei(config)#port vlan 1000 0/0 1
   ```

4. Configure a service port.

   We use the ADSL2+ port 0/3/1 as an example, add service port 100, configure CVLAN to untagged, and bind VLAN 1000 and traffic profile 10 to it.

   NOTE

   - Because the same version of ONUs with different types have different access modes and the slots for their service boards are different, the methods for creating service ports are different. MA5616s are used as an example to describe how to create service ports. For details about how to create service ports on other types of ONUs, see the related configuration guide.
   - In xDSL access mode, xDSL ports must be activated before service ports are created.
   - The SVLAN must be the same as the CVLAN on the OLT.

   ```
   huawei(config)#service-port 100 vlan 1000 adsl 0/3/1 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
   ```

5. Configure the multicast mode and multicast protocol version.

   Configure the multicast mode to IGMP snooping and adopt IGMP V3.

   ```
   huawei(config)#multicast-vlan 1000
   huawei(config-mvlan1000)#igmp version v3
   huawei(config-mvlan1000)#igmp mode snooping
   ```

6. Configure a multicast upstream port and a multicast program.

   Configure upstream port 0/0/1 as the upstream multicast port, and configure the IP address of the multicast to 224.1.1.10 and the source IP address to 10.10.10.10.

   ```
   huawei(config-mvlan1000)#igmp uplink-port 0/0/1
   huawei(config-mvlan1000)#igmp program add ip 224.1.1.10 sourceip 10.10.10.10
   ```

7. Configure a multicast user and add the user to the multicast VLAN.

   Configure service port 1000 as a multicast user, add the user to VLAN 1000, and adopt the no-auth mode for the multicast user.

   NOTE

   - If set users to be authenticated, you can run the command **igmp profile add** to add a multicast authority profile, and then use the command **igmp profile** to modify the authority parameters. At last, use the **igmp user bind-profile** command to bind this profile to the user need to be authenticated.
   - If set users to be authenticated, delete the **no-auth** parameter.

   ```
   huawei(config-mvlan1000)#btv
   huawei(config-btv)#igmp user add service-port 1000 no-auth
   huawei(config-btv)#multicast-vlan 1000
   huawei(config-mvlan1000)#igmp multicast-vlan member service-port 100
   huawei(config-mvlan1000)#quit
   ```

8. Save the configuration.

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

----End

Result

The user can watch program 1 on the TV.

Configuration File

On the OLT side.

```
vlan 1000 smart
port vlan 1000 0/19 0
dba-profile add profile-name IPTV type4 max 61440
ont-lineprofile gpon profile-id 10
tcont 3 dba-profile-name IPTV
gem add 0 eth tcont 3 cascade on
gem add 1 eth tcont 3 cascade on
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 1000
commit
quit
interface gpon 0/2
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
ont confirm 1 ontid 2 sn-auth 32303131B39FD642 snmp ont-lineprofile-id 10
ont alarm-profile 1 1 profile-id 1
ont alarm-profile 1 2 profile-id 1
quit
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 gateway
192.168.50.254 vlan 8
ont ipconfig 1 2 static ip-address 192.168.50.3 mask 255.255.255.0 gateway
192.168.50.254 vlan 8
service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 2 vlan 8 gpon 0/2/1 ont 2 gemport 0 multi-service
 user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1000 vlan 100 gpon 0/2/1 ont 1 gemport 1 multi-service
 user-vlan 1000 rx-cttr 6 tx-cttr 6
service-port 1001 vlan 100 gpon 0/2/1 ont 2 gemport 1 multi-service
 user-vlan 1000 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
btv
igmp cascade-port 0/2/1 ontid 1 gemport 1
igmp cascade-port 0/2/1 ontid 2 gemport 1
multicast-vlan 1000
igmp version v3
igmp mode proxy
igmp uplink-port 0/19/0
igmp program add name program1 ip 224.1.1.10 sourceip 10.10.10.10
btv
igmp cdr enable
quit
file-server auto-backup cdr primary 10.10.10.20 tftp
save
```

On the ONU side.

```
vlan 1000 smart
port vlan 1000 0/0 1
traffic table ip index 10 cir off priority 4 priority-policy tag-In-Package
service-port 100 vlan 1000 adsl 0/3/1 vpi 0 vci 35 rx-cttr
 10 tx-cttr 10
multicast-vlan 1000
igmp version v3
```

```
igmp mode proxy
igmp uplink-port 0/0/1
igmp program add name program1 ip 224.1.1.10 sourceip 10.10.10.10
btv
igmp user add service-port 100 no-auth
multicast-vlan 1000
igmp multicast-vlan member service-port 100
save
```

A Acronyms and Abbreviations

A

ADSL	Asymmetrical Digital Subscriber Line
AG	Access Gateway

B

BRAS	Broadband Remote Access Server
BTV	Broadband TV

C

CAR	Committed Access Rate
CIR	Committed Information Rate
CLI	Command Line Interface

D

DHCP	Dynamic Host Configuration Protocol
DHCP option82	DHCP relay agent option 82

E

EPON	Ethernet Passive Optical Network

F

FoIP	Fax over Internet Protocol

FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
GEM	GPON Encapsulation Method
GPON	Gigabit-capable Passive Optical Networks
I	
IP	Internet Protocol
IPoA	Internet Protocol Over ATM
IPoE	IP over Ethernet
L	
LAN	Local Area Network
M	
MAC	Medium Access Control
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MoIP	Modem over Internet Protocol
MTU	Maximum Transmission Unit
N	
NGN	Next Generation Network
NMS	Network Management System
O	
OLT	Optical Line Terminal
ONT	Optical Network Terminal
ONU	Optical Network Unit

P

PITP	Policy Information Transfer Protocol
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PPPoA	Point-to-Point Protocol Over ATM
PPPoE	Point-to-Point Protocol Over Ethernet
PSTN	Public Switched Telephone Network

Q

QoS	Quality of Service

R

RFC	Remote Feature Control

S

SNMP	Simple Network Management Protocol
SSH	Secure Shell
STB	Set Top Box
STP	Spanning Tree Protocol

T

T-CONT	Transmission Container
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol

U

UDP	User Datagram Protocol

V

VLAN	Virtual LAN
VOD	Video On Demand
VoIP	Voice over Internet Protocol