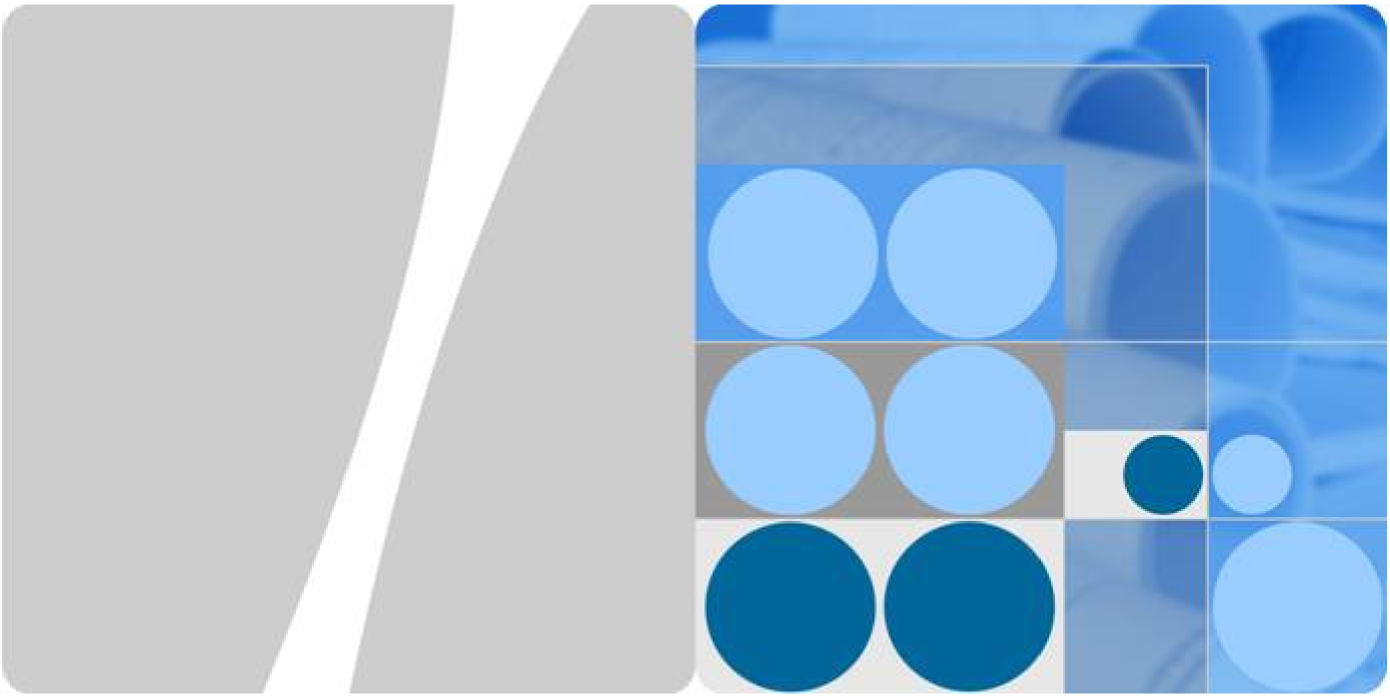


SmartAX MA5621 Multi-service Access Module V800R309C00

Configuration Guide

Issue 02

Date 2011-07-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute 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 MA5621. 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 MA5621.

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 02 (2011-07-20)

Based on issue 01 (2011-05-28), the document is updated as follows:

The following information is modified:

- **3.2 Configuring the U2000**
- **9.3 Configuration Example of Transmitting Power Distribution Site Information by Using the Ethernet Access**

Issue 01 (2011-05-28)

This is the first release.

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 MA5621.	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 MA5621.	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.

Prerequisite

- 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.

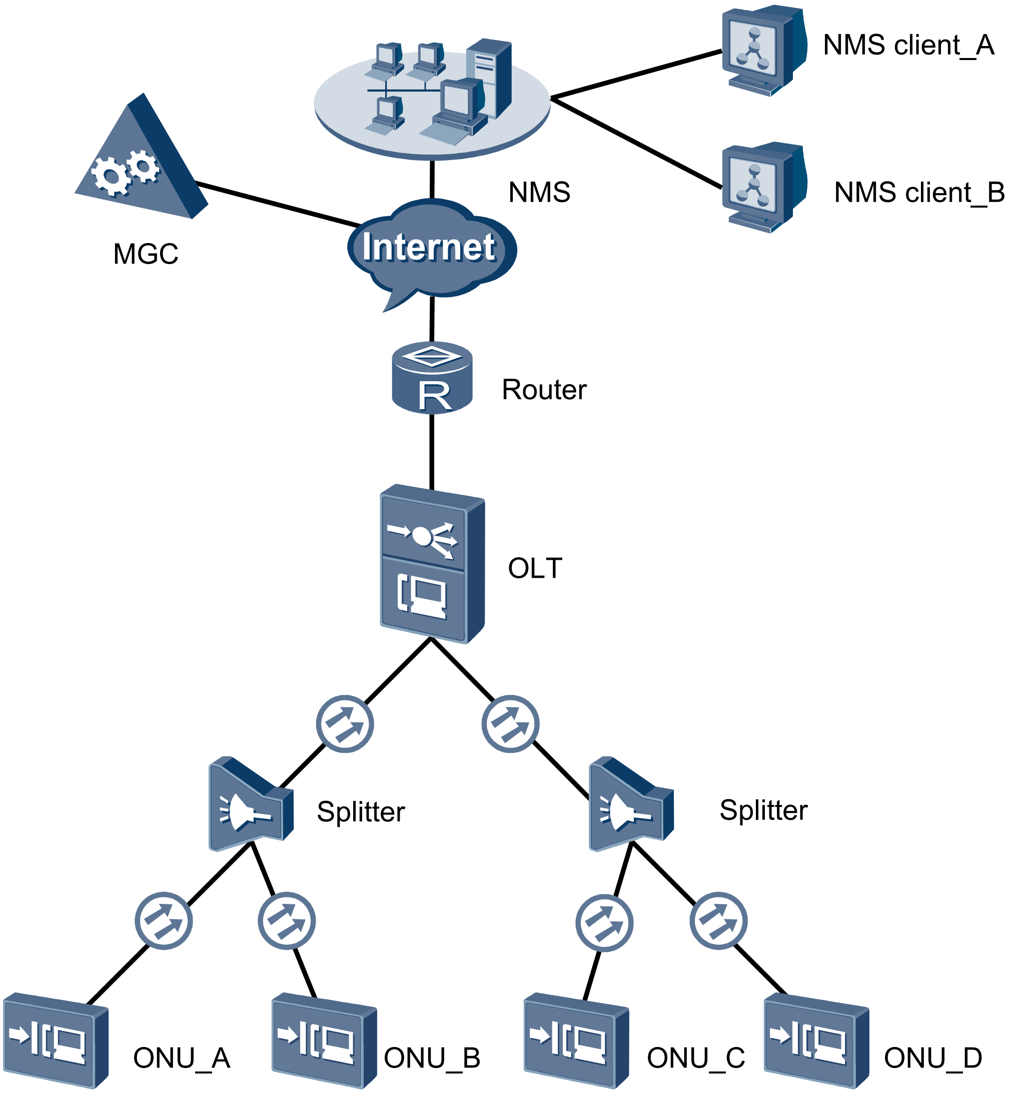
Context

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.

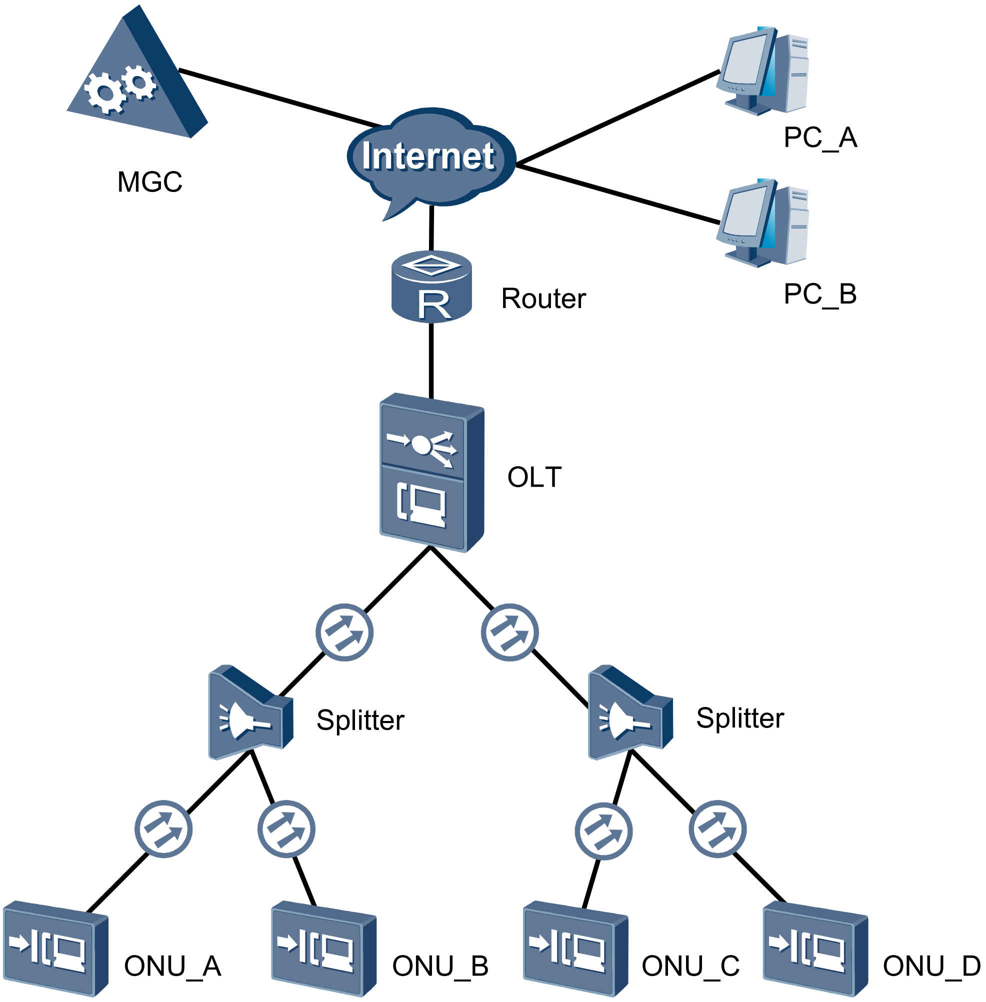
5. After confirming that the ONU works in the normal state (the Link LED is on and the Auth LED blinks), the hardware installation engineer records the ONU SN and reports the SN to the commissioning engineer.
6. The commissioning engineer maps the ONU SN, the management IP address of the ONU, and the 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 MA5621 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.

Prerequisite

You must be logged in to the MA5621. 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 MA5621 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 MA5621 to be queried. Then, click **Search**.
  3. In the search result, select the desired MA5621. 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 *MA5621 Upgrade guide*.

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.

3.1 Configuring the Maintenance Terminal
This topic describes three modes of managing the MA5621 from the maintenance terminal.

3.2 Configuring the U2000
The MA5621 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 MA5621 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.

3.3 Configuring the Attributes of the Upstream Port
The MA5621 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.

3.4 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.

3.5 Configuring a VLAN Service Profile
Integrate VLAN-related configurations into the VLAN service profile so that all attributes take effect immediately after the VLAN service profile is bound to the VLAN. This increases the configuration efficiency.

3.6 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.

3.7 Configuring the User Security
Configuring the security mechanism can protect operation users and access users against user account theft and roaming or from the attacks from malicious users.

This topic describes how to configure the network security and protection measures of the system to protect the system from malicious attacks.

This topic describes how to configure the AAA on the MA5621, including configuring the MA5621 as the local and remote AAA servers.

This topic describes the type, rule, and configuration of the ACL on the MA5621.

This topic describes how to configure quality of service (QoS) on the MA5621 to provide end-to-end quality assurance for user services.

You can monitor the environment status of the MA5621 through its built-in virtual EMU H831VESC. This topic describes how to configure the H831VESC.

3.1 Configuring the Maintenance Terminal

This topic describes three modes of managing the MA5621 from the maintenance terminal.

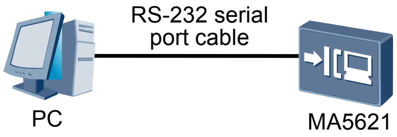
3.1.1 Configuring Management Through a Local Serial Port

This topic describes how to connect the maintenance terminal to the MA5621 through a local serial port, log in to the MA5621, and then manage the MA5621 from the maintenance terminal.

Networking

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

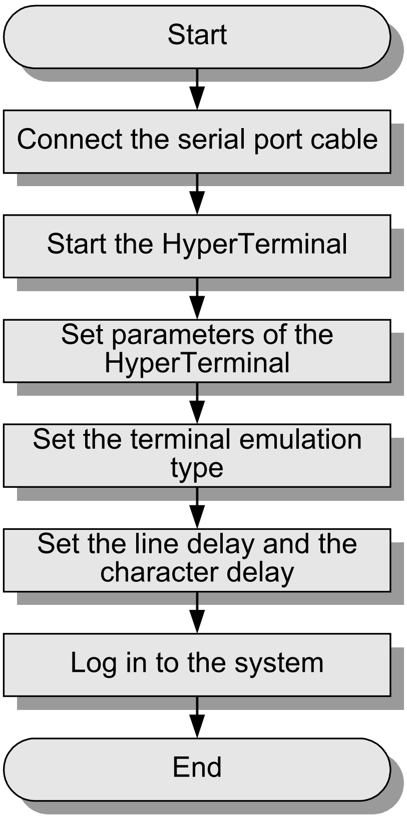
Figure 3-1 Example network for configuring management through a local serial port



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


Start
Connect the serial port cable
Start the HyperTerminal
Set parameters of the HyperTerminal
Set the terminal emulation type
Set the line delay and the character delay
Log in to the system
End

NOTE

This topic uses Windows XP operating system as an example.

Procedure

Step 1 Connect the serial port cable.

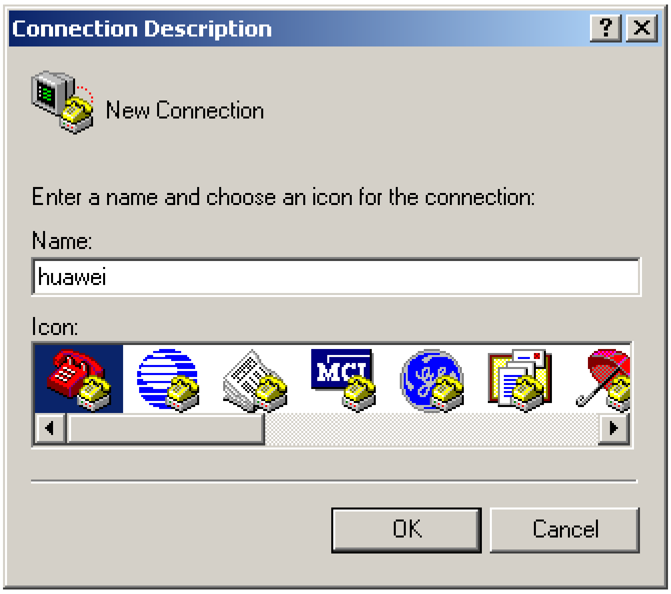
Use a standard RS-232 serial port cable to connect the serial port of the PC to the CONSOLE port (maintenance serial port) on the control board of the MA5621, as shown in **Figure 3-1**.

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



Connection Description

New Connection

Enter a name and choose an icon for the connection:

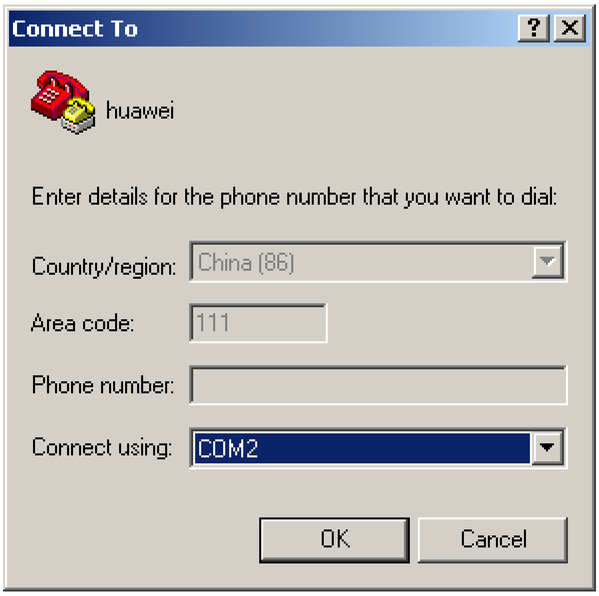
Name: huawei

Icon:

2. Set the serial port.

   On the PC that is connected to the MA5621, select the number of the 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



Connect To

huawei

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

Country/region: China (86)

Area code: 111

Phone number:

Connect using: COM2

Step 3 Set the communication parameters of the HyperTerminal.

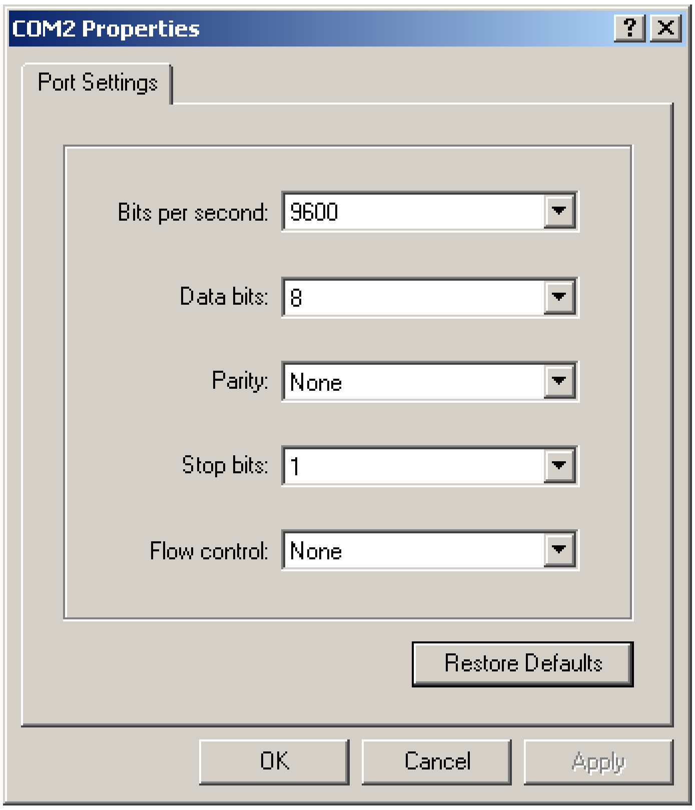
Set the parameters in the **COM2 Properties** dialog box, as shown in **Figure 3-5**. The parameters are as follows:

- 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 MA5621. By default, the baud rate of the serial port on the MA5621 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 MA5621 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



COM2 Properties

Port Settings

Bits per second: 9600

Data bits: 8

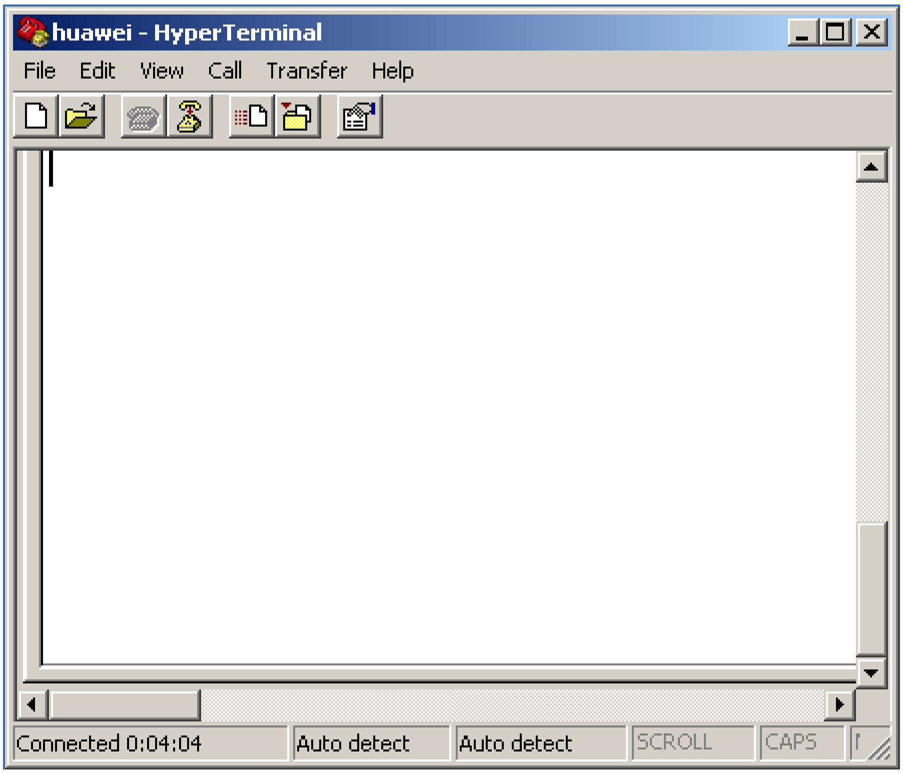
Parity: None

Stop bits: 1

Flow control: None

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

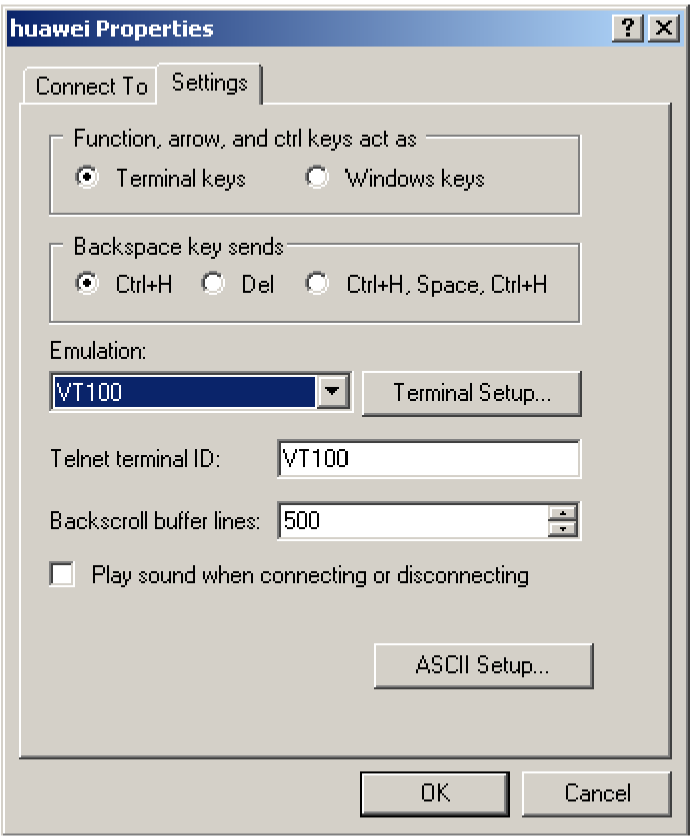
Figure 3-6 HyperTerminal interface



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



huawei Properties

Connect To | Settings

Function, arrow, and ctrl keys act as

● Terminal keys ○ Windows keys

Backspace key sends

● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

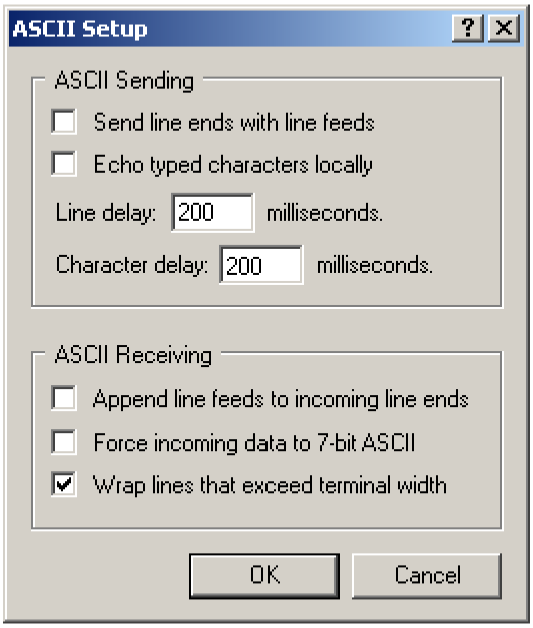
Step 5 Set the line delay and the character delay.

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



ASCII Setup

ASCII Sending

□ Send line ends with line feeds

□ Echo typed characters locally

Line delay: 200 milliseconds.

Character delay: 200 milliseconds.

ASCII Receiving

□ Append line feeds to incoming line ends

□ Force incoming data to 7-bit ASCII

☑ Wrap lines that exceed terminal width

----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 MA5621 to the maintenance terminal through an outband management port, log in to the MA5621, and then manage the MA5621.

Prerequisite

- 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.

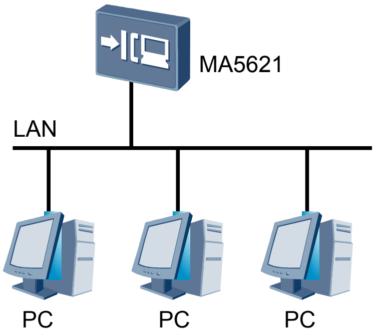
NOTE

In the following operations, the configurations of the MA5621 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 MA5621 and the IP address of the maintenance terminal are in the same network segment. You can also manage the MA5621 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 MA5621.

Data Plan - LAN

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

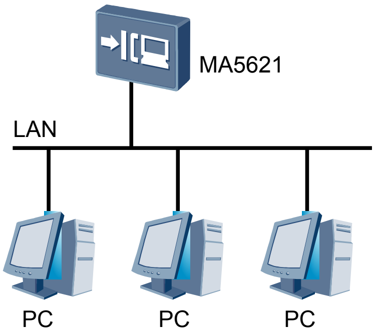
Table 3-1 Data plan for configuring outband management over a LAN in the telnet mode

Item	Data
Maintenance Ethernet port of the MA5621	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 MA5621 is connected to the WAN through the maintenance Ethernet port. You can manage the MA5621 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.

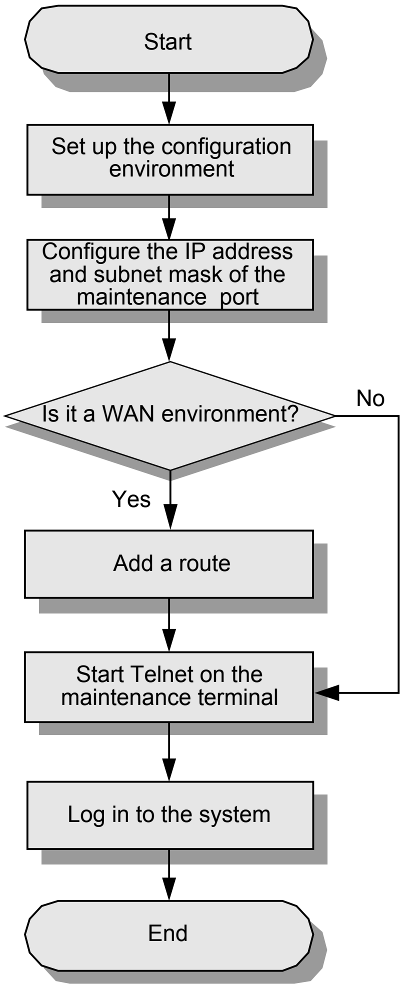
Table 3-2 Data plan for configuring outband management over a WAN in the telnet mode

Item	Data
Maintenance Ethernet port of the MA5621	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 MA5621	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


Start
Set up the configuration environment
Configure the IP address and subnet mask of the maintenance port
Is it a WAN environment?
No
Yes
Add a route
Start Telnet on the maintenance terminal
Log in to the system
End

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 MA5621.

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.

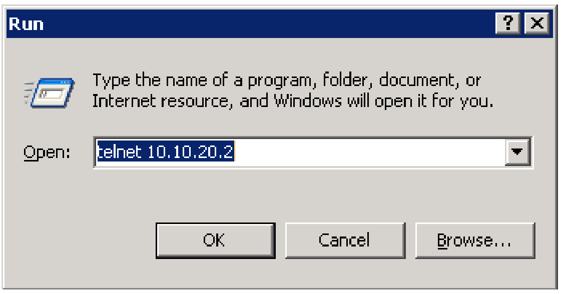
- If the remote WAN management environment is set up as shown in **Figure 3-10**, run the **ip route-static** command to add a route to the next hop.

```
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 MA5621), 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



Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
telnet 10.10.20.2
OK
Cancel
Browse...

Step 5 Log in to the MA5621.

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 (MA5621).

  Copyright(C) Huawei Technologies Co., Ltd. 2002-2011. All rights reserved.
```

----End

Result

After logging in to the MA5621, you can manage the MA5621. For instructions on CLI, see CLI Operation Characteristics.

3.1.3 Configuring Inband Management (GPON Upstream)

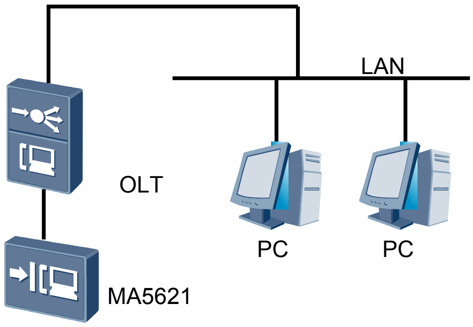
This topic describes how to log in to the MA5621 through an OLT from the maintenance terminal to manage the MA5621.

Prerequisite

- The physical connection between the MA5621 and the OLT must be normal.
- The IP address of the maintenance terminal must be properly configured.

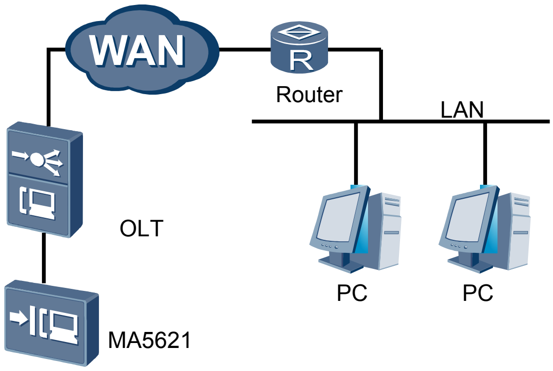
Networking - LAN

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



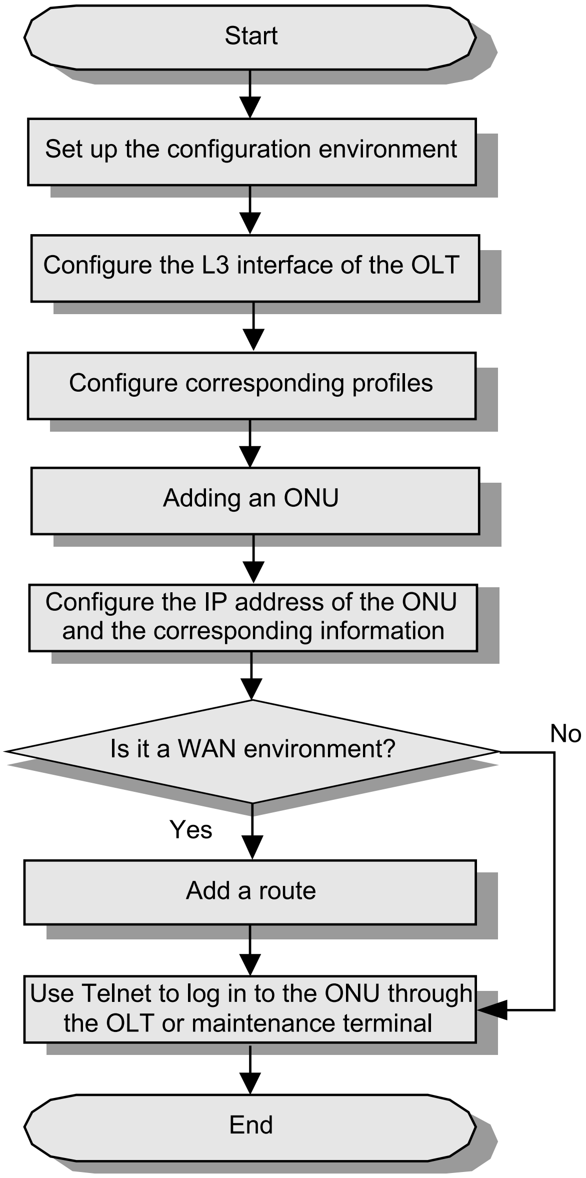
Configuration Flowchart

Figure 3-15 shows the flowchart for managing the MA5621 through an inband channel in the GPON upstream mode.

NOTE

In the GPON upstream mode, the MA5621 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


Start
Set up the configuration environment
Configure the L3 interface of the OLT
Configure corresponding profiles
Adding an ONU
Configure the IP address of the ONU and the corresponding information
Is it a WAN environment?
No
Yes
Add a route
Use Telnet to log in to the ONU through the OLT or maintenance terminal
End

Result

After logging in to the MA5621 through the OLT or maintenance terminal, you can configure the MA5621. 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 MA5621 through an upstream port (inband management port) of the MA5621 for inband management.

Prerequisite

- 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.

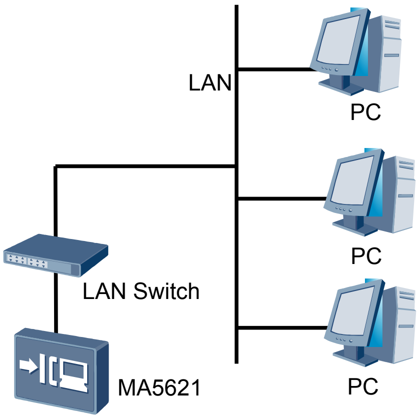
NOTE

In the following operations, the configurations of the MA5621 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.

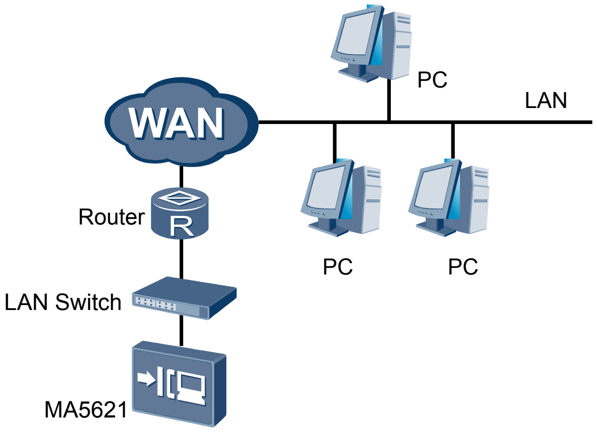
Table 3-3 Data plan for configuring inband management over a LAN in the telnet mode

Item	Data
Upstream port of the MA5621	● 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.

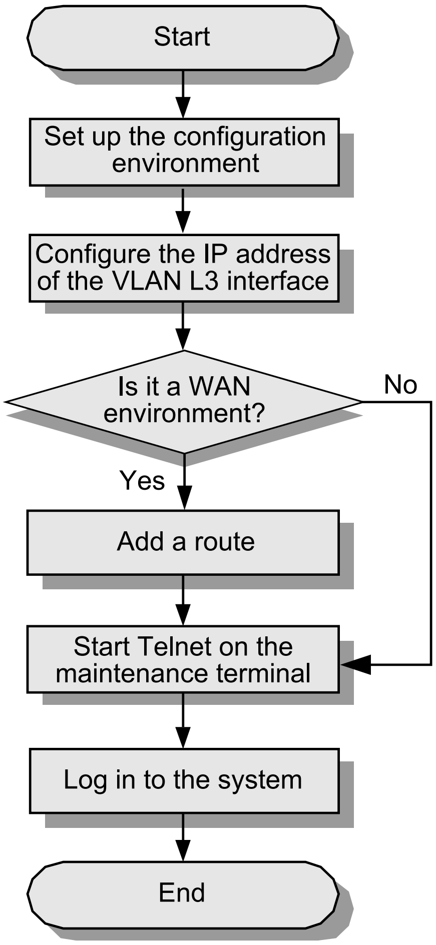
Table 3-4 Data plan for configuring inband management over a WAN in the telnet mode

Item	Data
Upstream port of the MA5621	● 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


Start
Set up the configuration environment
Configure the IP address of the VLAN L3 interface
Is it a WAN environment?
No
Yes
Add a route
Start Telnet on the maintenance terminal
Log in to the system
End

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 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 3 Add a route.

- If the configuration environment is set up as shown in **Figure 3-16**, you need not add a route.

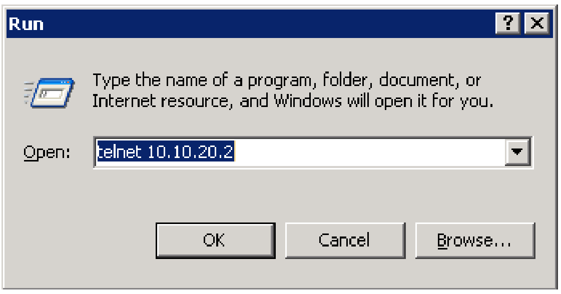
- If the remote WAN management environment is set up as shown in **Figure 3-17**, run the **ip route-static** command to add a route to the next hop.

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

Step 4 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 MA5621), 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



Run

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

Open: telnet 10.10.20.2

Step 5 Log in to the MA5621.

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 (MA5621).

  Copyright(C) Huawei Technologies Co., Ltd. 2002-2011. All rights reserved.
```

----End

Result

After logging in to the MA5621, you can manage the MA5621. For instructions on CLI, see CLI Operation Characteristics.

3.2 Configuring the U2000

The MA5621 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 MA5621 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 MA5621 can be interconnected with the U2000 in inband or outband networking mode.

Prerequisite

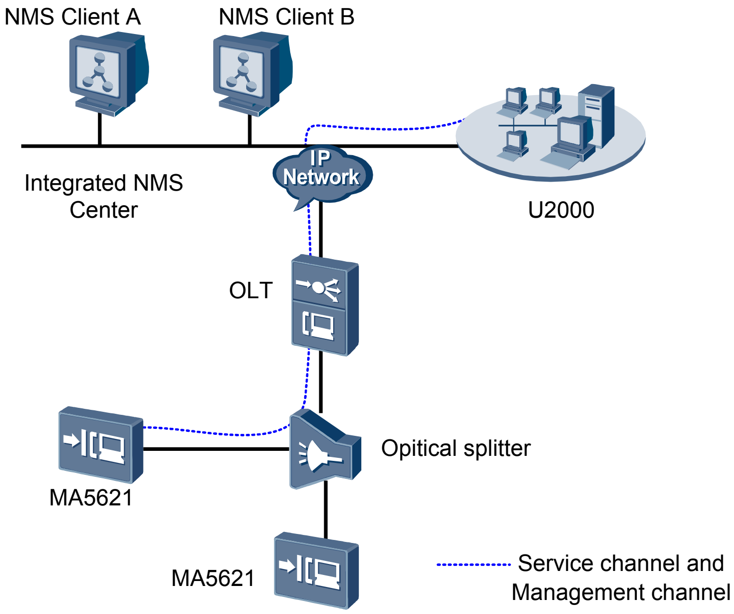
- If the device is interconnected with the NMS in outband networking mode, the communication port (maintenance network port) must be configured. For detailed procedure, see **3.1.2 Configuring Outband Management**.
- If the device is interconnected with the NMS through the GPON upstream port in inband networking mode, the communication port (GPON 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 MA5621 supports the GPON/GE upstream port.
- A static route is used between the MA5621 and the U2000.

Figure 3-20 Inband networking

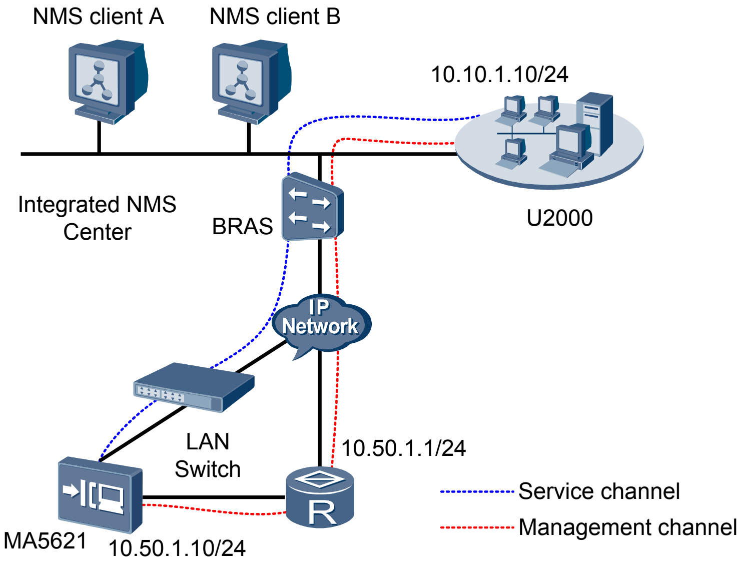


Networking - Outband Networking Mode

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.

- A static route is used between the MA5621 and the U2000.

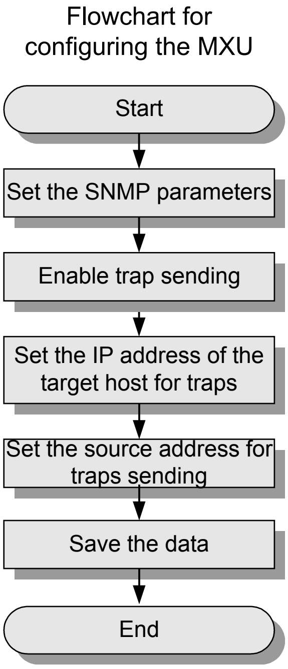
Figure 3-21 Outband networking



Configuration Flowchart

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

Figure 3-22 Flowchart for configuring the NMS


Flowchart for configuring the MXU
Start
Set the SNMP parameters
Enable trap sending
Set the IP address of the target host for traps
Set the source address for traps sending
Save the data
End

Procedure

- Configuration procedure on the device
  1. Configure the SNMP parameters.

     (1) 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
     ```

     (2) (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
     ```

     (3) 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 to enable the function of sending traps to the NMS. After the function is enabled, the device reports abnormal events to the NMS server.

   ```
   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 trap-hostname***hostname***address***ip-addr* [**udp-port***udp-portid*] **trap-paramsname***paramsname* 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
   ```

   NOTE

   udp-port: is the destination host port ID of traps. The default value (162) takes effect if you do not specify a value. The default values on the NMS and device are both 162 and are recommended.

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 MA5621. This step can be omitted because the MA5621 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.

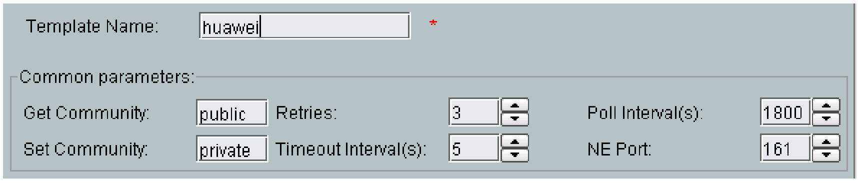
NOTE

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:

(1) Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.

(2) In **Default Access Protocol Parameters**, click the **SNMPv1 Parameters** tab, and then click **Add**.

(3) Set the profile name, and then set other parameters according to the plan.



Template Name: huawei *

Common parameters:

Get Community: public

Retries: 3

Poll Interval(s): 1800

Set Community: private

Timeout Interval(s): 5

NE Port: 161

NOTE

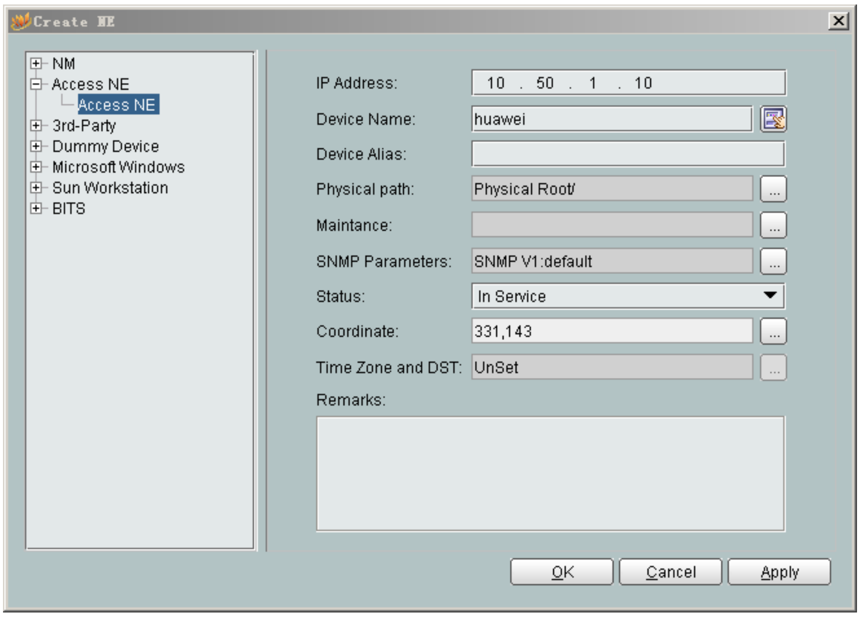
NE Port: is the management port ID. The default values on the NMS and the device are both 161 and are recommended.

(4) Click **OK**. Then, the SNMP parameters are configured.

4. Add a device.

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

(2) In the dialog box that is displayed, set relevant parameters.



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V1:default
Status: In Service
Coordinate: 331,143
Time Zone and DST: UnSet
Remarks:

NOTE

- The IP address is the management IP address of the MA5621.
- 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.

(3) 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 MA5621 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 MA5621 can be interconnected with the U2000 in inband or outband networking mode.

Prerequisite

- 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 GPON upstream port in inband networking mode, the communication port (GPON 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 MA5621 supports GPON/GE upstream port.
- A static route is used between the MA5621 and the U2000.

Networking - Outband 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 management channel. Service packets and management packets are transmitted through different channels. The outband NMS management is implemented through the maintenance network port.

- A static route is used between the MA5621 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.
     (1) 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
```

(2) (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 XA_China
```

(3) 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 to enable the function of sending traps to the NMS. After the function is enabled, the device reports abnormal events to the NMS server.

```
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 trap-hostname***hostname***address***ip-addr* [**udp-port***udp-portid*] **trap-paramsname***paramsname* 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
```

NOTE

udp-port: is the destination host port ID of traps. The default value (162) takes effect if you do not specify a value. The default values on the NMS and device are both 162 and are recommended.

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 MA5621. This step can be omitted because the MA5621 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.

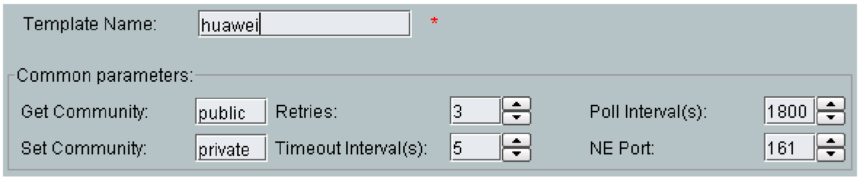
   NOTE

   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:

   (1) Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.

   (2) In **Default Access Protocol Parameters**, click the **SNMPv2 Parameters** tab, and then click **Add**.

   (3) Set the profile name, and then set other parameters according to the plan.



Template Name: huawei *

Common parameters:

Get Community: public
Retries: 3
Poll Interval(s): 1800
Set Community: private
Timeout Interval(s): 5
NE Port: 161

NOTE

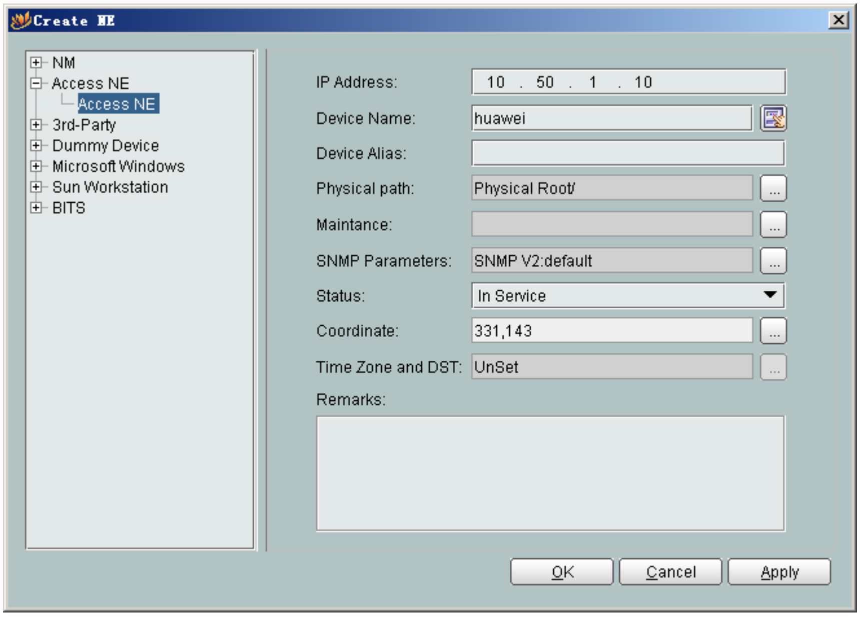
NE Port: is the management port ID. The default values on the NMS and the device are both 161 and are recommended.

(4) Click **OK**. Then, the SNMP parameters are configured.

4. Add a device.

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

(2) In the dialog box that is displayed, set relevant parameters.



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V2:default
Status: In Service
Coordinate: 331,143
Time Zone and DST: UnSet
Remarks:

NOTE

- The IP address is the management IP address of the MA5621.
- Select the SNMP parameters based on the selected SNMP version. This section considers the SNMP V2 default profile as an example. You can select the profile corresponds to the actual planning.

(3) 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 MA5621 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 MA5621 can be interconnected with the U2000 in inband or outband networking mode.

Prerequisite

- 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 GPON upstream port in inband networking mode, the communication port (GPON 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 MA5621 supports GPON/GE upstream port.
- A static route is used between the MA5621 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.

- A static route is used between the MA5621 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.

     (1) 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 authk
     ey123 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
     ```

     (2) (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
     ```

     (3) (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
     ```

     (4) 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 to enable the function of sending traps to the NMS. After the function is enabled, the device reports abnormal events to the NMS server.

     ```
     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 trap-hostname***hostname***address***ip-addr* [**udp-port***udp-portid*] **trap-paramsname***paramsname* 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
```

NOTE

udp-port: is the destination host port ID of traps. The default value (162) takes effect if you do not specify a value. The default values on the NMS and device are both 162 and are recommended.

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.

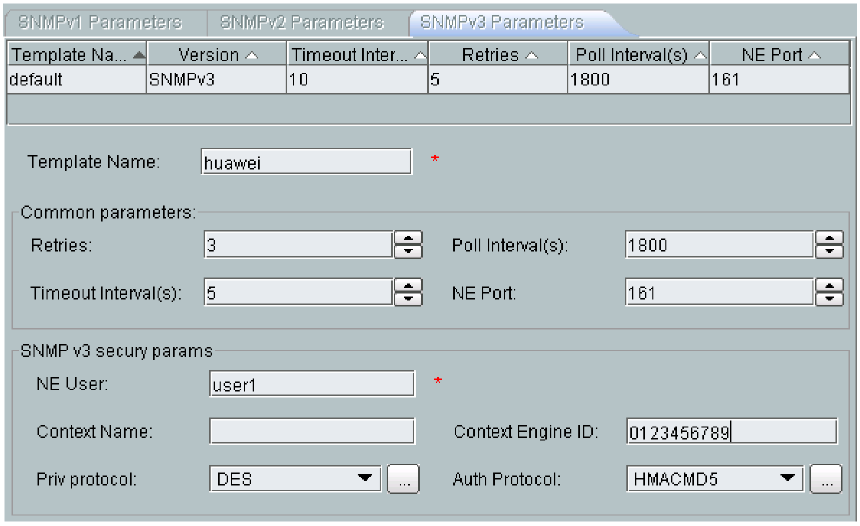
2. Log in to the U2000.

3. Configure the SNMP parameters.

   (1) Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.

   (2) In **Default Access Protocol Parameters**, click the **SNMPv3 Parameters** tab, and then click **Add**.

   (3) Set the profile name, and then set other parameters according to the plan.



Template Na...	Version	Timeout Inter...	Retries	Poll Interval(s)	NE Port
default	SNMPv3	10	5	1800	161

Template Name: huawei *

Common parameters:

Retries: 3 Poll Interval(s): 1800

Timeout Interval(s): 5 NE Port: 161

SNMP v3 secury params

NE User: user1 *

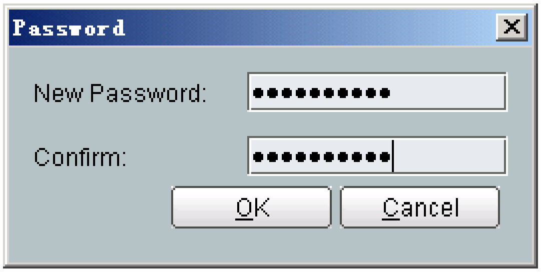
Context Name: Context Engine ID: 0123456789

Priv protocol: DES ... Auth Protocol: HMACMD5 ...

NOTE

NE Port: is the management port ID. The default values on the NMS and the device are both 161 and are recommended.

   (4) 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**.


Password

New Password: ●●●●●●●●●●●

Confirm: ●●●●●●●●●●●

NOTE

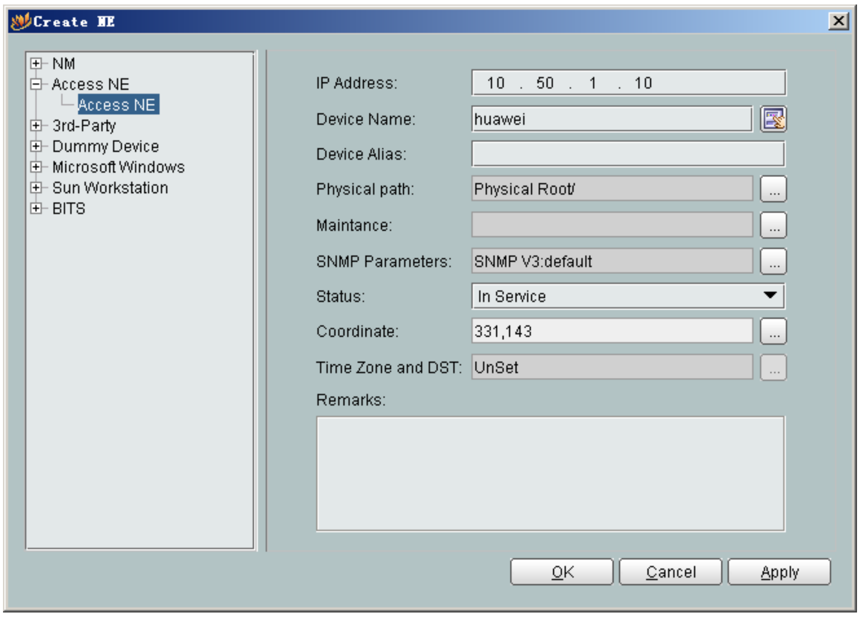
NE User, **Context Engine ID**, **Priv Protocol** and the password, and **Auth Protocol** and the password must be the same as those configured on the MA5621. The **display snmp-agent usm-user** command is used to query the device user, data encryption protocol, and authentication protocol configured on the MA5621. The **display snmp-agent local-engineid** command is used to query the environment engine ID configured on the MA5621.

   (5) Click **OK**. Then, the SNMP parameters are configured.

4. Add a device.

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

   (2) In the dialog box that is displayed, set relevant parameters.



IP Address: 10 . 50 . 1 . 10
Device Name: huawei
Device Alias:
Physical path: Physical Root/
Maintance:
SNMP Parameters: SNMP V3:default
Status: In Service
Coordinate: 331,143
Time Zone and DST: UnSet
Remarks:

NOTE

- The IP address is the management IP address of the MA5621.
- 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.

(3) 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 MA5621 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 MA5621 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 (Optional) Configuring an Uplink Ethernet Port

This topic describes how to configure a specified Ethernet port so that the system can use it to communicate with an upper-layer device.

Prerequisite

If you configure the MA5621 in offline mode, the port mode is configured using the **port mode** command.

Context

The MA5621 must be interconnected with an upper-layer device through Ethernet ports. Therefore, ensure that the attributes of the Ethernet ports connecting the two devices are the same.

Default Settings

Table 3-5 lists the default settings of Ethernet port attributes.

Table 3-5 Default settings of Ethernet port attributes

Parameter	Default Setting (Optical Port)
Auto negotiation mode	Enabled
Rate	Auto negotiation
Duplex mode	Auto negotiation
Network cable adaptation mode	Not supported
Flow control	Disabled

Procedure

- Configure the physical attributes of an Ethernet port.
  1. 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.
     - After the auto negotiation mode is disabled, the rate and working mode of the port are in the forced mode (the two attributes use default values or are set using command line interface (CLI).
  2. 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 preset rate. When setting the rate, ensure that:

     - The rate of the Ethernet port is the same as that of the interconnected port on the peer device. This prevents communication failures.
     - The auto negotiation mode of the Ethernet port is disabled.
  3. 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. When setting the duplex mode, ensure that:

     - The ports of two interconnected devices work in the same duplex mode. This prevents communication failures.
     - The auto negotiation mode is disabled.
  4. 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 classified into:

     - **normal**: The straight-through cable is used as the network cable. In this mode, the network cable connecting to the Ethernet port must be a straight-through cable.
     - **across**: The crossover cable is used as the network cable. In this mode, the network cable connecting to the Ethernet port must be a crossover cable.
     - **auto**: The network cable is selected in auto negotiation mode. In this mode, the network cable can be a straight-through or crossover cable.

     When configuring the network cable adaptation mode, pay attention to the following points:

     - The Ethernet optical port does not support the network cable adaptation mode.
     - If an Ethernet electrical port works in forced mode (the auto negotiation mode is disabled), the network cable adaptation mode of the port cannot be configured to **auto**.
- 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 an Ethernet port on the 0/0/1 has the following attributes:

- Optical/Electrical adaptation mode: optical
- Rate: 1000 Mbit/s
- Duplex mode: full-duplex
- Flow control: enabled
- Auto negotiation mode: not enabled

To configure the Ethernet port, 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 Uplink GPON 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 uplink GPON port.

Prerequisite

If you configure the MA5621 in offline mode, the port attribute can be configured only after the port mode is configured through the **port mode** command.

Procedure

- Set the password for registering with the OLT.

  Run the **password** (in the GPONNNI mode) command to set the registration password of the current device that functions as a GPON ONU.

  NOTE

  When dual GPON ports are used for upstream transmission, only 0/0/1 port can be set. After the setting, the parameters of port 0/0/1 are the same as those of port 0/0/0.

- Set the alarm thresholds for the receive optical power of the optical transceiver.

  Run the **optical-module threshold** (in 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 uplink GPON port.

  Run the **laser** (in GPONNNI mode) command to set the optical transceiver to active, always active, or disabled.

  - To ensure normal running of the optical transceiver of the uplink GPON port, you need to set the optical transceiver to work normally.
  - When disabling the optical transceiver of the uplink PON port, ensure that the uplink GPON port is not carrying any services.
  - After setting the optical transceiver of the uplink GPON 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 uplink PON port to **auto**, do as follows:

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

  Command:
          password huawei
huawei(config-if-gponnni-0/0/0)#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-0/0/0)#laser auto
```

3.4 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.

Prerequisite

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 3-6**.

Table 3-6 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

User Type	Application Scenario	VLAN Planning
	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 VLAN+MAC or 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 3-7 lists the default parameter settings of VLAN.

Table 3-7 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 3-8 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the **vlan** ***vlanid*** **standard** command.	Standard VLAN. 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 service access. For example, Smart VLANs can be used in residential users.
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 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 3-9 VLAN attributes and application scenarios

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
Common	The default attribute for a new VLAN is "common".	The VLAN with this attribute can be a standard VLAN, smart VLAN, 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.
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 MA5621. 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 MA5621. 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 MA5621. 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 stacking VLAN with ID of 50 is to be configured for extension of the VLAN. A service port is added to VLAN 50. The outer VLAN tag 50 of the stacking VLAN identifies the access device and the inner VLAN tag 10 identifies the user with access to the device. For the VLAN, description needs to be configured for easy maintenance. To configure such a VLAN, do as follows:

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#service-port vlan 50 eth 0/1/3 multi-service user-encap pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#stacking label vlan 50 baselabel 10
huawei(config)#vlan desc 50 description stackingvlan/label10
```

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
```

3.5 Configuring a VLAN Service Profile

Integrate VLAN-related configurations into the VLAN service profile so that all attributes take effect immediately after the VLAN service profile is bound to the VLAN. This increases the configuration efficiency.

Prerequisite

The VLAN to which the VLAN service profile is bound must be created.

Procedure

Step 1 Create a VLAN service profile.

Run the **vlan service-profile** command to create a VLAN service profile or enter the configuration mode of the VLAN service profile. When the profile does not exist, running this command means to create a VLAN service profile and enter the configuration mode of the service profile. If the profile exists, running this command means to directly enter the configuration mode of this service profile.

Step 2 Configure parameters of the VLAN service profile.

The VLAN service profile contains VLAN-related configurations. You can select them according to your requirements.

- Run the **forwarding** command to configure the VLAN forwarding mode. The MA5621 supports two forwarding modes: VLAN+MAC address (vlan-mac) and S+C (vlan-connect). The system forwarding policy differs according to different VLAN forwarding modes.
- Run the **packet-policy** command to configure the forwarding policy for the unknown multicast packets in the VLAN. Two policies namely forward and discard are supported.
- Run the **bpdu tunnel** command to configure the BPDU transparent transmission switch. After transparent transmission is enabled, the Layer 2 BPDUs of the private network can be transmitted transparently over the public network.
- Run the **rip tunnel** command to configure the RIP Layer 2 transparent transmission switch. After the transparent transmission switch is enabled, RIP packets can be transparently transmitted at Layer 2 based on VLAN on the MA5621 without running the RIP protocol.
- Run the **ospf tunnel** command to configure the OSPF Layer 2 transparent transmission switch. After the transparent transmission switch is enabled, OSPF packets can be transparently transmitted at Layer 2 based on VLAN on the MA5621 without running the OSPF protocol.
- Run the **user-bridging** command to configure the bridging function of the VLAN service profile. After the bridging function is enabled, two users in the same VLAN can directly communicate with each other at Layer 2.
- Run the **vtp-cdp tunnel** command to configure the VTP/CDP packet transparent transmission switch. After the switch is enabled, VTP/CDP packets are transparently transmitted based on the VLAN.
- Run the **commit** command to commit the current parameter configuration of the VLAN service profile.

NOTE

After the configuration is completed, you must run the **commit** command to make the configuration take effect.

Step 3 Bind the VLAN service profile to the VLAN.

Run the **vlan bind service-profile** command to bind the configured VLAN service profile to a specified VLAN.

----End

Example

Add VLAN service profile 3 and bind it to VLAN 100. The profile parameters are planned as follows:

- VLAN forwarding mode VLAN+MAC address (vlan-mac)
- BPDU transparent transmission: enabled
- Unknown multicast packet: discarded

Adopt the default values for other parameters.

```
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#forwarding vlan-mac
huawei(config-vlan-srvprof-3)#bpdu tunnel enable
huawei(config-vlan-srvprof-3)#packet-policy multicast discard
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
huawei(config)#vlan bind service-profile 100 profile-id 3
```

3.6 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 MA5621 supports all these modes.

Default Configuration

Table 3-10 provides the default configuration for NTP.

Table 3-10 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

3.6.1 (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.

Prerequisite

Before configuring the NTP authentication, make sure that the network interface and the routing protocol of the MA5621 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
```

3.6.2 Configuring the NTP Broadcast Mode

This topic describes how to configure the MA5621 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.

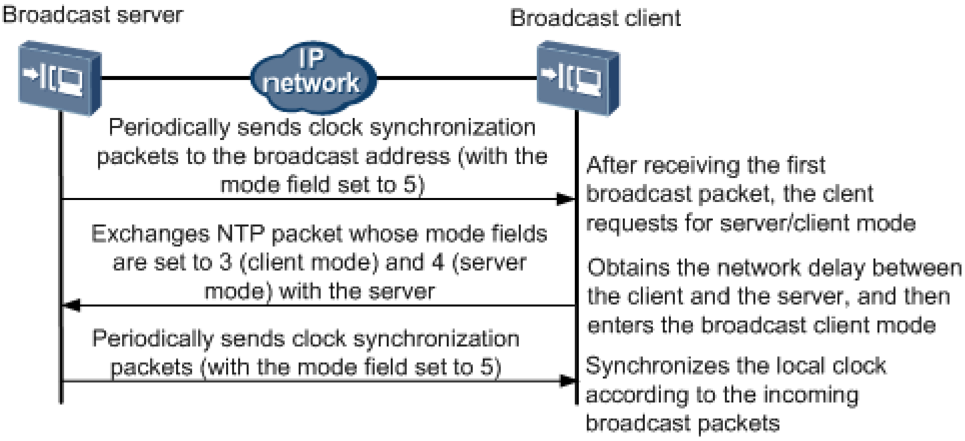
Prerequisite

Before configuring the NTP broadcast mode, make sure that the network interface and the routing protocol of the MA5621 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 3-23**.

Figure 3-23 NTP broadcast mode


Broadcast server
Broadcast client
IP network
Periodically sends clock synchronization packets to the broadcast address (with the mode field set to 5)
Exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server
Periodically sends clock synchronization packets (with the mode field set to 5)
After receiving the first broadcast packet, the clent requests for server/client mode
Obtains the network delay between the client and the server, and then enters the broadcast client mode
Synchronizes the local clock according to the incoming broadcast packets

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.

     (1) Run the **ntp-service authentication enable** command to enable NTP authentication.

     (2) Run the **ntp-service authentication-keyid** command to set an NTP authentication key.

     (3) Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
  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.

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

----End

Example

Assume the following configurations: MA5621 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
```

3.6.3 Configuring the NTP Multicast Mode

This topic describes how to configure the MA5621 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.

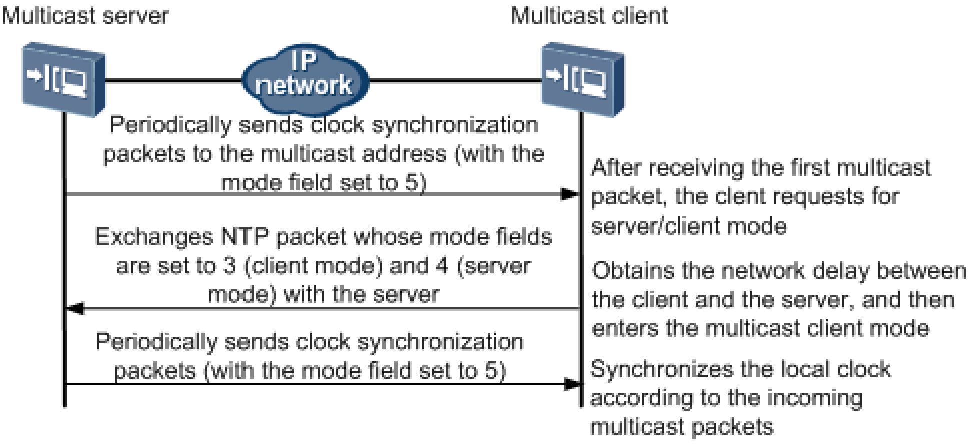
Prerequisite

Before configuring the NTP multicast mode, make sure that the network interface and the routing protocol of the MA5621 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 3-24**.

Figure 3-24 NTP multicast mode


Multicast server
Multicast client
IP network
Periodically sends clock synchronization packets to the multicast address (with the mode field set to 5)
After receiving the first multicast packet, the clent requests for server/client mode
Exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server
Obtains the network delay between the client and the server, and then enters the multicast client mode
Periodically sends clock synchronization packets (with the mode field set to 5)
Synchronizes the local clock according to the incoming multicast packets

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.

     (1) Run the **ntp-service authentication enable** command to enable NTP authentication.

     (2) Run the **ntp-service authentication-keyid** command to set an NTP authentication key.

     (3) Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
  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.

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

----End

Example

Assume the following configurations: MA5621 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
```

3.6.4 Configuring the NTP Unicast Server Mode

This topic describes how to configure the MA5621 as the NTP client to synchronize with the NTP server in the network.

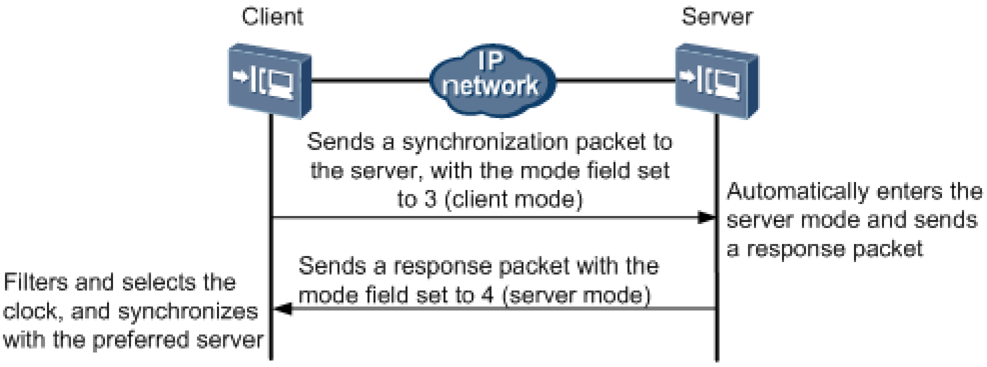
Prerequisite

Before configuring the NTP client/server mode, make sure that the network interface and the routing protocol of the MA5621 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 3-25**.

Figure 3-25 NTP client/server mode


Client
Server
IP network
Sends a synchronization packet to the server, with the mode field set to 3 (client mode)
Automatically enters the server mode and sends a response packet
Sends a response packet with the mode field set to 4 (server mode)
Filters and selects the clock, and synchronizes with the preferred server

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, MA5621 (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:

```
uawei(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
```

3.6.5 Configuring the NTP Peer Mode

This topic describes how to configure the MA5621 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.

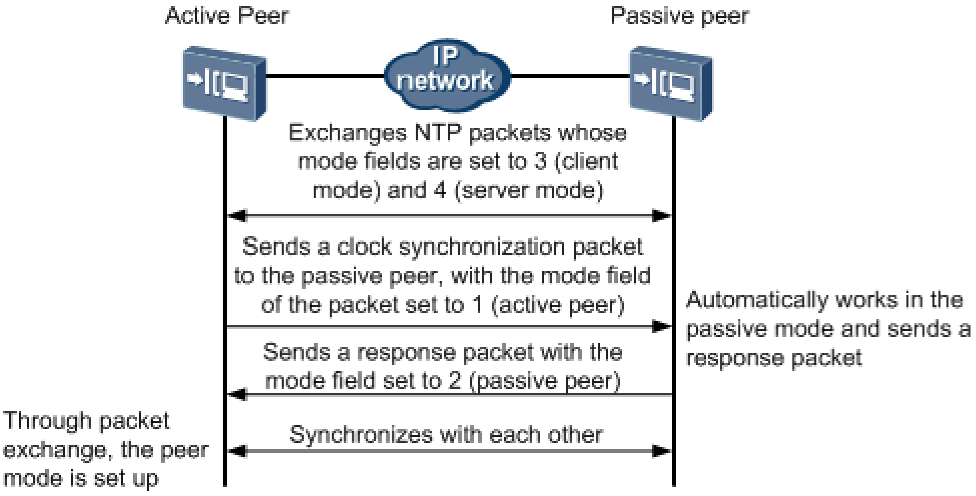
Prerequisite

Before configuring the NTP peer mode, make sure that the network interface and the routing protocol of the MA5621 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 3-26**.

Figure 3-26 NTP peer mode


Active Peer
Passive peer
IP network
Exchanges NTP packets whose mode fields are set to 3 (client mode) and 4 (server mode)
Sends a clock synchronization packet to the passive peer, with the mode field of the packet set to 1 (active peer)
Automatically works in the passive mode and sends a response packet
Sends a response packet with the mode field set to 2 (passive peer)
Through packet exchange, the peer mode is set up
Synchronizes with each other

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 MA5621 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 MA5621 (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
```

3.7 Configuring the User Security

Configuring the security mechanism can protect operation users and access users against user account theft and roaming or from the attacks from malicious users.

Context

The user security mechanism includes:

- 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.

3.7.1 Configuring the Anti-IP Address Attack

This topic describes how to configure IP address binding to prevent malicious users from attacking the device or authorized users by forging the IP addresses of authorized users.

Prerequisite

The service port to be bound to an IP address is created.

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.

Procedure

- Configure the IP address binding.

  Run the **bind ip** command to bind an IP address to a service port.

  To permit only the users of certain IP addresses to access the system so that illegal users cannot access the system by using the IP addresses of legal users, configure the IP address binding.

----End

Example

To bind IP address 10.10.10.20 to service port 2, that is, service port 2 permits only the packet whose source IP address is 10.10.10.20, do as follows:

```
huawei(config)#bind ip service-port 2 10.10.10.20
```

3.7.2 Configuring the Anti-MAC Address Attack

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

Context

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 MA5621 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.

The anti-MAC-duplicate function does not allow dynamic MAC addresses to be duplicated before they are aged. In this way, when MAC address conflicts occur between different users, the user that goes online first will not be affected.

Procedure

- Configure the MAC address binding.
  1. Run the **mac-address static** command to add a static MAC address.
  2. Run the **mac-address max-mac-count** command to set the maximum number of learnable MAC addresses to 0.

     This parameter is to limit the maximum number of the MAC addresses that can be learned through one account, that is, to limit the maximum number of the PCs that can access the Internet through one account.
- Configure the 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 bind static MAC address 1010-1010-1010 to service port 1, and set the maximum number of learnable MAC addresses to 0, that is, service port 1 permits only the packet whose source MAC address is 1010-1010-1010, do as follows:

```
huawei(config)#mac-address static service-port 1 1010-1010-1010
huawei(config)#mac-address max-mac-count service-port 1 0
```

To enable anti-MAC 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-dos function             : disable
   Anti-ipattack function        : disable
   Anti-icmpattack function      : disable
   Source-route filter function  : disable
   Anti-macduplicate function    : enable
   Anti-dos safegard time  (min) : 5
```

3.8 Configuring System Security

This topic describes how to configure the network security and protection measures of the system to protect the system from malicious attacks.

Context

With the system security feature, the MA5621 can be protected against the attacks from the network side or user side, and therefore the MA5621 can run stably in the network. System security includes the following items:

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

The following common inappropriate configurations affect the system security:

- Use a public network address to manage the device. The access rights are not strictly limited when the ACL is configured. Therefore, the network may be attacked.

  Preventive methods or measures:

  - Use a private network address to manage the device.
  - When configuring the ACL, apply the minimum authorization principle.
  - Configure the permitted IP address segment, and add only the necessary management IP address segment. IP addresses other than have been specified are not permitted to access the device through the management port.
- Packets accessing the management interface of the device are not controlled. When a device is attacked by packets, the system is busy and the services cannot be provided in the normal state.

  Preventive methods or measures: Run the **firewall packet-filter** command to apply the firewall packet filtering rule on the interface to filter packets received on the interface and prevent packet attacks.

Table 3-11 lists the default settings of system security.

Table 3-11 Default settings of system security

Parameter	Default Setting
Firewall blacklist	Disabled
Anti-DoS attack	Disabled
Anti-ICMP attack	Disabled
Anti-IP attack	Disabled
Source route filtering	Disabled
User-side ring network detection	Disabled

3.8.1 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 MA5621, 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 **interface meth** command to enter the METH mode to configure the firewall packet filtering rules for an METH interface; run the **interface vlanif** command to

enter the VLANIF mode configure the firewall packet filtering rules for a VLAN interface.

6. Run the **firewall packet-filter** command to apply firewall packet filtering rules to an interface.

----End

Example

To add IP address 10.10.10.18 to the firewall blacklist with the aging time of 100 min, do as follows:

```
huawei(config)#firewall blacklist item 10.10.10.18 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 10.10.11.0 to access the maintenance Ethernet port with IP address 10.10.11.28 on the device, do as follows:

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)#rule 5 deny icmp source 10.10.11.0 0.0.0.255 destin
ation 10.10.11.28 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
```

3.8.2 Configuring Anti-Attack

Enabling anti-DoS attack and anti-ICMP/IP attack, and configuring the source route filtering and source MAC address filtering functions can prevent malicious users' attack on the system, so as to improve system security.

Context

The MA5621 supports the following measures to prevent malicious users' attack on the system. Choose measures according to actual requirements.

- Anti-DoS attack: indicates the defensive measures taken by the system to receive only a certain number of control packets sent from a user.
- Anti-ICMP attack: indicates the defensive measures taken by the system to drop the ICMP packets sent from the user-side device to the MA5621. This is to prevent the user-side device from pinging the VLAN interface of the MA5621.
- Anti-IP attack: indicates the defensive measures taken by the system to drop the IP packets sent from the user-side device to the MA5621.
- Source route filtering: indicates the defensive measures taken by the system to filter the IP packets that are sent by the user and carry the routing option field.

- Source MAC address filtering: indicates the defensive measures taken by the system to filter the packets that are sent by the user and carry certain source MAC addresses.
- User-side ring network check: indicates the defensive measures taken by the system to check user-side ring networks. In this way, the system can process ring networks to prevent ring networks from affecting services.

Procedure

- Configure anti-DoS attack.

  Run the **security anti-dos enable** command to enable global anti-DoS attack. With global anti-DoS attack enabled, when the system receives attack packets from a user port, the system adds the user port to the blacklist. When global anti-DoS attack is disabled, the system deletes the blacklist.

  Application scenario: Two PCs (PC1 and PC2) are connected to the network through the MA5621. If a malicious user (PC1) sends a large number of protocol control packets to attack the CPU of the MA5621, the CPU usage of the MA5621 will be over high, and then the MA5621 is unable to process the services of another user (PC2). To implement anti-DoS attack, shield the attack port or suppress the protocol packet sending to protect the MA5621 from being attacked.
- Configure anti-ICMP attack.

  Run the **security anti-icmpattack enable** command to enable anti-ICMP attack. Anti-ICMP attack is mainly used to prevent the user-side device from pinging the VLAN interface of the MA5621.

  Application scenario: Two PCs (PC1 and PC2) are connected to the network through the MA5621. When PC2 sends a large number of ICMP packets to the VLAN interface, the services of the user (PC1) that obtains the upper-layer DHCP information through the same VLAN interface will be abnormal. To implement anti-ICMP attack, directly drop the user-side ICMP packets if the IP address of the VLAN interface on the MA5621 is its destination IP address.
- Enable anti-IP attack.

  Run the **security anti-ipattack enable** command to enable anti-IP attack. The anti-IP attack is used to prevent user-side IP packets from attacking the Layer 3 interface of the device or to prevent illegal users from logging in to the device through telnet.

  Application scenario: When a PC sends the packets with the address of VLAN x as the destination IP address to VLANIF x, it may send a large number of packets to attack the device, causing the device to fail to process normal services; when a user knows the address of VLAN x, or the user name and password for logging in to the device, the user may log in to the device through telnet to randomly change the configurations of the device. To prevent the two preceding cases, the device needs to implement anti-IP attack. With this feature, the device drops the packets with the address of the device interface as the destination IP address to prevent the user from attacking the device.
- Enable the source route filtering function.

  Run the **security source-route enable** command to enable the source route filtering function. This function is mainly used to filter the packets that carry the routing information and are reported to the Layer 3 switch.

  Application scenario: In general, routes are dynamic and application does not control route selection. The sender can add the routing information to IP packets through the source route to perform route selection. In this case, packets go along a specific route in the network according to the intention of the sender. To prevent the preceding cases, enable the source route filtering function. Then the MA5621 performs validity check on IP packets and drops the packets that match the source route options.

- Configure the MAC address filtering function.

  Run the **security mac-filter** command to enable the MAC address filtering function.

  The MAC addresses that are dynamically learned by the host and the source MAC addresses that are statically configured by running the **security mac-filter source** command share the four entries for source MAC addresses on the board. The entries for the statically configured MAC addresses are of a higher priority than that of the dynamically learned MAC addresses.

  Application scenario: To prevent users from forging the MAC address of the network-side device, or forging certain renowned MAC addresses, set the MAC address of the network-side as the MAC address to be filtered.

- Configure the function of checking user-side ring networks.

  Run the **ring check enable** command to enable the function of checking user-side ring networks. By default, the function of checking user-side ring networks is disabled.

  CAUTION

  To ensure device security, it is recommended that you enable this function.

----End

Example

To enable the global anti-DoS attack function, enable anti-IP attack function, and the function of checking user-side ring networks, do as follows:

```
huawei(config)#security anti-dos enable
huawei(config)#security anti-ipattack enable
huawei(config)#ring check enable
```

3.8.3 Preventing the Access of Illegal Users

Only the users of the permitted IP address segment can access the device, and the users of the denied IP address segment cannot access the device. This prevents the users of illegal IP address segments from logging in to the system, safeguarding the system.

Context

- Each firewall can be configured with up to 10 address segments.
- When adding an address segment, ensure that the start address does not repeat an existing start address.
- To delete an address segment, you only need to enter the start address of the address segment.

CAUTION

- To ensure the device security, apply the minimum authorization principles. That is, configure the permitted IP address segment, and add only the necessary management IP address segment. IP addresses other than have been specified are not permitted to access the device through the management port.
- It is recommended that the permitted IP address segment and the denied IP address segment should not overlap, and only the user whose IP address is in the permitted address segment and is not in the denied address segment can access the device.

Procedure

- Configure the permitted/denied IP address segment for the access through Telnet.
  1. Run the **sysman ip-access telnet** command to configure the IP address segment that is permitted to access the device through Telnet.
  2. Run the **sysman ip-refuse telnet** command to configure the IP address segment that is forbidden to access the device through Telnet.
  3. Run the **sysman firewall telnet enable** command to enable the firewall function for the access through Telnet. By default, the firewall function of the system is disabled.
- Configure the permitted/denied IP address segment for the access through SSH.
  1. Run the **sysman ip-access ssh** command to configure the IP address segment that is permitted to access the device through SSH.
  2. Run the **sysman ip-refuse ssh** command to configure the IP address segment that is forbidden to access the device through SSH.
  3. Run the **sysman firewall ssh enable** command to enable the firewall function for the access through SSH. By default, the firewall function of the system is disabled.
- Configure the permitted/denied IP address segment for the access through SNMP (NMS).
  1. Run the **sysman ip-access snmp** command to configure the IP address segment that is permitted to access the device through SNMP.
  2. Run the **sysman ip-refuse snmp** command to configure the IP address segment that is forbidden to access the device through SNMP.
  3. Run the **sysman firewall snmp enable** command to enable the firewall function for the access through SNMP. By default, the firewall function of the system is disabled.

----End

Example

To enable the firewall function for the access through Telnet, and permit only the users of the IP address segment 10.10.5.1-10.10.5.254 to log in to the device through Telnet, do as follows:

```
huawei(config)#sysman ip-access telnet 10.10.5.1 10.10.5.254
huawei(config)#sysman firewall telnet enable
```

To enable the firewall function for the access through SSH, and permit only the users of the IP address segment 10.10.20.1-10.10.20.254 to log in to the device through SSH, do as follows:

```
huawei(config)#sysman ip-access ssh 10.10.20.1 10.10.20.254
huawei(config)#sysman firewall ssh enable
```

To enable the firewall function for the access through SNMP, and permit only the users of the IP address segment 10.10.20.1-10.10.20.254 to log in to the device through SNMP, do as follows:

```
huawei(config)#sysman ip-refuse snmp 10.10.20.1 10.10.20.254
huawei(config)#sysman firewall snmp enable
```

3.9 Configuring AAA

This topic describes how to configure the AAA on the MA5621, including configuring the MA5621 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

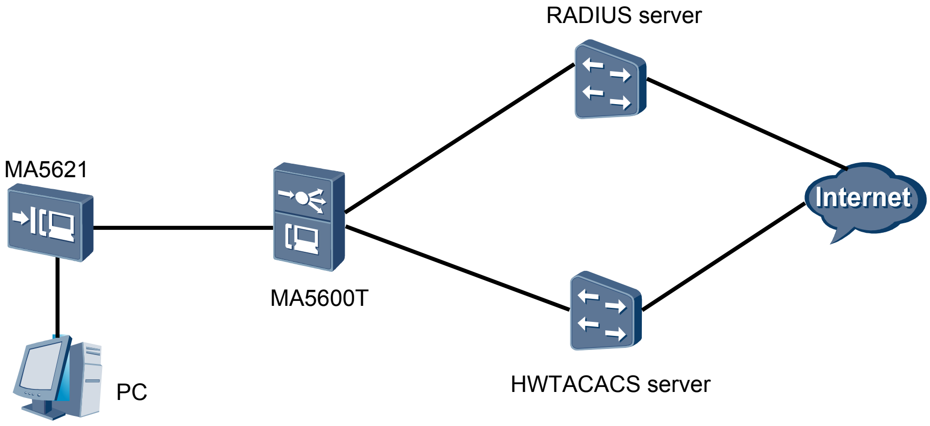
AAA is generally applied to the users that access the Internet in the PPPoA, PPPoE, VLAN, WLAN, or Admin Telnet (associating the user name and the password with the domain name) mode.

NOTE

In the existing network, Admin Telnet correspond to the local AAA, that is, the MA5621 functions as a local AAA server; PPPoE corresponds to the remote AAA, that is, the MA5621 functions as the client of a remote AAA server.

Figure 3-27 shows an example network of the AAA application.

Figure 3-27 Example network of the AAA application



The preceding figure shows that the AAA function can be implemented on the MA5621 in the following three ways:

- The MA5621 functions as a local AAA server. In this case, the local AAA needs to be configured. The local AAA does not support accounting.
- The MA5621 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 MA5621 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 3-12 lists the differences between HWTACACS and RADIUS.

Table 3-12 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.

3.9.1 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
```

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

The MA5621 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 MA5621, 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 MA5621 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 MA5621 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 MA5621 is in the normal state.
   - Make sure that the configuration of the RADIUS service port of the MA5621 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 (MA5621) 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 MA5621 sends the request packets to the RADIUS server. If the RADIUS server does not respond within the response timeout time, the MA5621 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 MA5621 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 MA5621 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
```

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

The MA5621 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 (MA5621) 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 MA5621 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 MA5621 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 MA5621 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 MA5621 is in the normal state.
- Make sure that the HWTACACS server port of the MA5621 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 (MA5621) 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 MA5621 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 MA5621 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
```

3.9.4 Configuration Example of the Authentication Based on the RADIUS Protocol

The MA5621 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.

Prerequisite

- The route from the MA5621 to the RADIUS server must be configured.
- The management user information (user name@domain and password) must be configured on the RADIUS server.

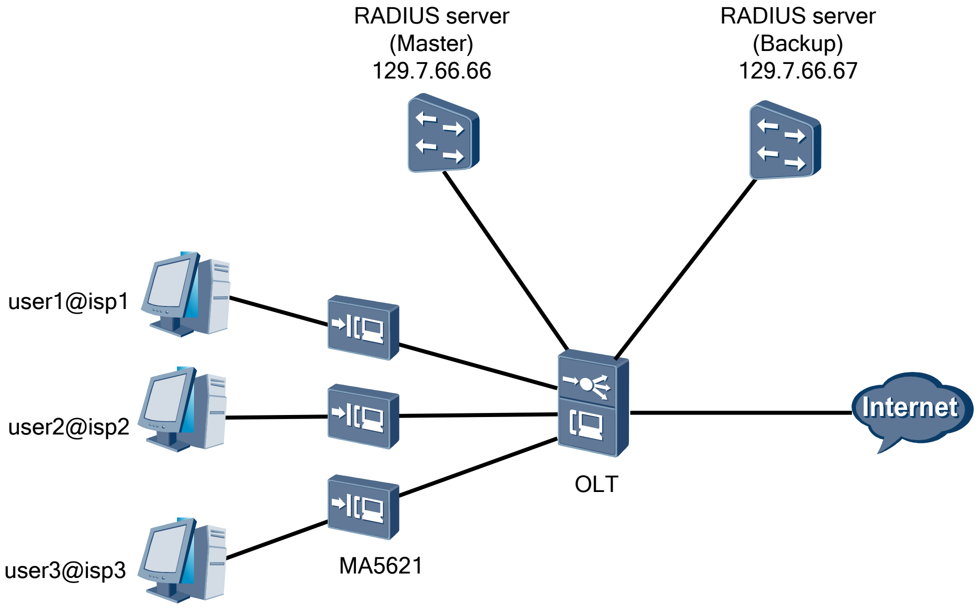
Service Requirements

- 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 3-28 shows the example network of RADIUS authentication.

Figure 3-28 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
huawei(config-aaa)#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>):test01
  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:
  Error choice or the input level higher than owns
     1. Common User  2. Operator  3. Administrator:3
  Permitted Reenter Number(0--4):1
  User's Appended Info(<=30 chars):
  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 MA5621 through Telnet. After entering the user name and password specified on the RADIUS server, the management user can successfully log in to the MA5621.
- 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 MA5621 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 MA5621 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>):
```

3.9.5 Configuration Example of the Authentication Based on the HWTACACS Protocol

The MA5621 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.

Prerequisite

- The route from the MA5621 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

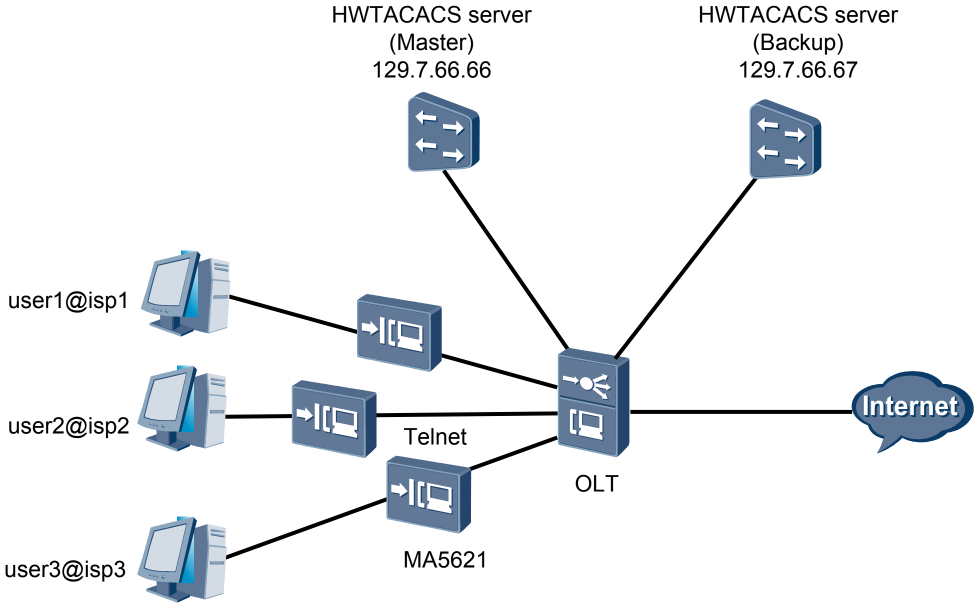
- Prefer the HWTACACS server to authenticate management user of domain **isp1**.
- Local authentication can be used when the HWTACACS server is unreachable.
- The user logs in to the server carrying the domain name.

- 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 3-29 shows the example network of HWTACACS authentication.

Figure 3-29 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)#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
huawei(config-aaa-domain-isp1)#quit
huawei(config-aaa)#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 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 MA5621 through Telnet. After entering the user name and password specified on the HWTACACS server, the management user can successfully log in to the MA5621.
- 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 MA5621 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 MA5621 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>):
```

3.10 Configuring the ACL for Packet Filtering

This topic describes the type, rule, and configuration of the ACL on the MA5621.

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 3-13 lists the ACL types.

Table 3-13 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 an arrival traffic stream matches two or more ACL rules, the matching sequence is as follows:

- An ACL rule is valid only when it is within the period of *time-range-name*.
- If the rules are all user-defined rules or non-user-defined rules, and are issued to the physical port:
  - If the rules of an ACL are activated at the same time, the rule with larger *rule-id* has a higher priority.
  - If the rules of an ACL are activated one by one, the rule activated later has higher priority over the one activated earlier.
  - If the rules are issued to the port from different ACLs, the rule activated later has higher priority over the one activated earlier.
- If the rules are issued to the routing interface or firewall, the rule with smaller *rule-id* has a higher priority. It is irrelative to the activation sequence. The rules are used to match the packets based on **rule-id** in an ascending order. Once the rule with a smaller **rule-id** matches the packets, its subsequent rules are not used. That is, the rules with a larger **rule-id** are invalid.

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.

3.10.1 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 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 deny time-range time1
huawei(config-acl-basic-2000)#rule permit source 2.2.2.2 0.0.0.0 time-range time1
huawei(config-acl-basic-2000)#quit
huawei(config)#packet-filter inbound ip-group 2000 port 0/1/1
huawei(config)#save
```

3.10.2 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

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 **3.11.4 Configuring Traffic Management Based on ACL Rules**.

----End

Example

Assume that the service board of the MA5621 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
```

3.10.3 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 **3.11.4 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)#packet-filter inbound link-group 4001 port 0/1/1
huawei(config)#save
```

3.11 Configuring QoS

This topic describes how to configure quality of service (QoS) on the MA5621 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 MA5621, 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 MA5621 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 **3.10 Configuring the ACL for Packet Filtering**), and then QoS can be implemented for traffic streams.

3.11.1 Configuring Traffic Management

This topic describes how to configure traffic management on the MA5621.

Overview

The MA5621 supports traffic management for the inbound and outbound traffic streams of the system.

NOTE

For details on configuring traffic classification, see **4.4 Creating the Ethernet Access Service Port**.

In addition, the MA5621 supports rate limit on the Ethernet port and traffic suppression on inbound broadcast packets and unknown (multicast or unicast) packets.

3.11.1.1 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 3-14 lists the traffic parameters defined in the IP traffic profiles.

Table 3-14 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 3-14**.

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

3.11.1.2 Configuring Rate Limitation on an Ethernet Port

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

Prerequisite

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 0/0/0 to 6400 kbit/s, do as follows:

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

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

3.11.1.3 Configuring Rate Limitation by User

When the rate is limited based on user, two services: (a) site information about the electric system and (b) goose packets share a total user bandwidth. When either of the two services carries no traffic, the other service can occupy the total user bandwidth. In this way, the total user bandwidth can be managed in a unified manner.

Context

During the automatic transmission of site information about the electric system, the site information about the electric system and goose packets share a total user bandwidth. The traffic with a high 802.1p priority is transmitted in precedence over the traffic with a low 802.1p priority.

Procedure

Step 1 Run the **traffic table ip** command to create an IP traffic profile and set the class of service (CoS) priority, committed information rate (CIR), and peak information rate (PIR) for each service. PIR is equal to the total user bandwidth. When either of the two services carries no traffic, the other service can occupy the total user bandwidth.

The 802.1p priority of goose packets is higher than that of the site information about the electric system.

Step 2 Run the **service-port** command to create traffic that references the IP traffic profile created in **Step 1**.

Step 3 Run the **queue-scheduler strict-priority** command to set the queue scheduling mode to strict priority queue (PQ).

----End

Example

On Ethernet port 0/1/1, set the following parameters for traffic of the site information about the electric system and goose packet:

- Set the total user bandwidth to 10 Mbit/s, that is, set the maximum downstream rate in the channel profile to 10 Mbit/s. When either of the two services carries no traffic, the other service can occupy the total user bandwidth.
- Set the traffic ID of the site information about the electric system to 100, referenced traffic profile ID to 10, CIR to 2 Mbit/s, and 802.1p priority to 3.
- Set the traffic ID of goose packets to 102, referenced traffic profile ID to 12, and 802.1p priority to 5, without limiting the packet rate.

```
huawei(config)#traffic table ip index 10 cir 2048 pir 10240 priority 3 priority-
policy local-Setting
huawei(config)#service-port 100 vlan 2 eth 0/1/1 multi-service untagged rx-cttr 10
tx-cttr 10
huawei(config)#traffic table ip index 12 cir off priority 5 priority-policy local-
Setting
huawei(config)#service-port 102 vlan 2 eth 0/1/1 multi-service user-vlan 40 rx-cttr
12 tx-cttr 12
huawei(config)#queue-scheduler strict-priority
```

3.11.1.4 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 board in slot 0/1, do as follows:

```
huawei(config)#interface eth 0/1
huawei(config-if-eth-0/1)#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       :  7
  Current traffic suppression index of multicast       :  7
  Current traffic suppression index of unknown unicast :  7
  ---------------------------------------------------------------------
huawei(config-if-eth-0/1)#traffic-suppress all broadcast value 8
huawei(config-if-eth-0/1)#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
  ---------------------------------------------------------------------
```

3.11.2 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.

3.11.2.1 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 MA5621 supports 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 for resource acquisition. In the WRR scheduling mode, the queues are scheduled in turn, which ensures that each queue can be scheduled.

  Table 3-15 lists the mapping between the queue weights and the actual queues.

Table 3-15 Mapping between the queue weights and the actual queues

Queue Number	Configured Weight	Actual Queue Weight (Port Supporting Eight Queues)
7	W7	W7

Queue Number	Configured Weight	Actual Queue Weight (Port Supporting Eight Queues)
6	W6	W6
5	W5	W5
4	W4	W4
3	W3	W3
2	W2	W2
1	W1	W1
0	W0	W0

Wn: Indicates the weight of queue n. The weight sum of the queues must be equal to 0 or 100, where 0 indicates that the strict PQ scheduling mode is 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 WRR 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 (0 to 5) 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                      --
  ---------------------------------
```

3.11.2.2 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 3-16**.

Table 3-16 Mapping between the queue and the 802.1p priority

Queue Number	Actual Queue Number (Port Supporting Eight Queues)	802.1p Priority
7	7	7
6	6	6
5	5	5
4	4	4
3	3	3
2	2	2
1	1	1
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
  ------------------------
```

3.11.3 Configuring Early Drop

This topic describes how to configure early drop, which is applicable to the dropping policy settings for the packets in the queue. The MA5621 supports early drop by color.

Context

Early drop means that the system drops the packets that wait to enter the queue when congestion occurs. This process occurs after traffic management.

The MA5621 supports early drop by color according to the parameters in the IP traffic profile. The system drops the yellow packets that wait to enter the queue when congestion occurs.

Procedure

Step 1 Add the weighted random early detection (WRED) profile.

Run the **wred-profile** command to add the WRED profile.

Step 2 (Optional) Query the information about the WRED profile.

Run the **display wred-profile** command to verify that the WRED profile information is correct.

Step 3 Bind a queue with a WRED profile.

Run the **queue-wred** command to bind a queue with a WRED profile.

----End

Example

Assume the following configurations: The WRED profile ID is 0; the green packets are not dropped; the lower threshold of dropping the yellow packets is 50; the upper threshold of dropping the yellow packets is 80; the packet drop rate is 100. To bind such a WRED profile with queue 0, do as follows:

```
huawei(config)#wred-profile index 0 green low-limit 100 high-limit 100 discard-
probability 0 yellow low-limit 50 high-limit 80 discard-probability 100
huawei(config)#display wred-profile all
  Command:
          display wred-profile all
 -----------------------------------------------------------------
  WRED profile index: 0
            Low-limit(%)   High-limit(%)   Discard-probability(%)
  Green:             100             100                        0
  Yellow:             50              80                      100
  Queue ID: -
 -----------------------------------------------------------------
huawei(config)#queue-wred queue0 0
```

3.11.4 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.

3.11.4.1 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 0/1/1 to 512 kbit/s, do as follows:

```
huawei(config)#traffic-limit inbound ip-group 2001 512 port 0/1/1
huawei(config)#display qos-info traffic-limit port 0/1/1
traffic-limit:
port 0/1/1:
 Inbound:
   Matches: Acl 2001 rule 5     running
```

```
          Target rate: 512 Kbps
          Exceed action: drop
```

3.11.4.2 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 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 0/1/1, and the local priority of the traffic is 0 , do as follows:

```
huawei(config)#traffic-priority inbound ip-group 2001 local-precedence 0 port 0/1/1
huawei(config)#display qos-info traffic-priority port 0/1/1

traffic-priority:
port 0/1/1:
 Inbound:
   Matches: Acl 2001 rule 5  running
     Priority action: local-precedence 0
```

3.11.4.3 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 0/0/0, do as follows:

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

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

3.11.4.4 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 0/1/1 to port 0/0/0, do as follows:

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

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

3.12 Configuring the Monitoring Through the H831VESC

You can monitor the environment status of the MA5621 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 MA5621, and the ALARM port on the control board is connected to the external sensor through 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 subnode ID is 1.
- The H831VESC supports four digital parameters, all of which can be defined by users. Among the four digital parameters,
  - Digital parameter 0: Indicates the smoke 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 wiring 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. Ensure that it is running properly.

Step 2 Configure the digital parameters.

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

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 MA5621. When the actual level of a monitored digital parameter is different from the valid level preset in the system, the MA5621 reports an alarm.

Example

Table 3-17 shows the parameter plan for configuring the H831VESC.

Table 3-17 Data plan for configuring the H831VESC

Item	Data	Remarks
Digital parameters	Digital parameter ID: 0	-
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the MA5621 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: 6	When the temperature in the cabinet is between 67°C and 73°C, the MA5621 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: UPS 6: digital user-defined alarm
	Digital parameter ID: 1	-
	Valid level of digital parameter 1: high level	When the high level represents the valid level, the MA5621 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 MA5621 reports an alarm.
	Digital parameter ID: 2	-
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the MA5621 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 MA5621 reports an alarm.
	Digital parameter ID: 3	-
	Valid level of digital parameter 3: low level	When the low level represents the valid level, the MA5621 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: 6	When the fan is faulty, the MA5621 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    : RS232
  ----------------------------------------------------------------------------
huawei(config)#interface emu 0
huawei(config-if-h831vesc-0)#esc digital 0 available-level low-level digital-alarm
6 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
6 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
```

4 Configuring the Ethernet Access Service

About This Chapter

This topic describes the features and specifications of the Ethernet access service and how to configure the Ethernet access service on the MA5621.

1. 4.1 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. 4.2 Configuring the Upstream Port
   This topic describes how to add the upstream port to a certain VLAN so that the user packets carrying the VLAN ID can be transmitted to the upper-layer device through the upstream port.
3. 4.3 (Optional) Configuring the Attributes of the Ethernet Port
   This topic describes how to configure the attributes of a specified Ethernet port so that the system communicates with the user access device in the normal state. If the attributes of a specified Ethernet port do not meet the requirements in the actual application, configure the attributes.
4. 4.4 Creating the Ethernet Access Service Port
   The service port is used to connect the user side to the network side. To provision services, the service port must be created.

4.1 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.

Prerequisite

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 4-1**.

Table 4-1 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 VLAN+MAC or 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 4-2 lists the default parameter settings of VLAN.

Table 4-2 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 4-3 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 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 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 4-4 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 MA5621. 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 MA5621. 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 MA5621. 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 stacking VLAN with ID of 50 is to be configured for extension of the VLAN. A service port is added to VLAN 50. The outer VLAN tag 50 of the stacking VLAN identifies the access device and the inner VLAN tag 10 identifies the user with access to the device. For the VLAN, description needs to be configured for easy maintenance. To configure such a VLAN, do as follows:

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#service-port vlan 50 eth 0/1/3 multi-service user-encap pppoe
rx-cttr 6 tx-cttr 6
huawei(config)#stacking label vlan 50 baselabel 10
huawei(config)#vlan desc 50 description stackingvlan/label10
```

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
```

4.2 Configuring the Upstream Port

This topic describes how to add the upstream port to a certain VLAN so that the user packets carrying the VLAN ID can be transmitted to the upper-layer device through the upstream port.

Prerequisite

- The MA5621 must be interconnected with the OLT.
- The VLAN must be configured on the MA5621. For detailed procedure, see **Configuring A VLAN**.

Procedure

Step 1 Add the upstream port to the VLAN.

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

Step 2 (Optioal) Configure the attributes of the upstream port.

If the default attributes of the upstream port fail to meet the requirement for interconnecting the upstream port with the upper-layer device, you need to configure the attributes of the upstream port. For detailed procedure, see **3.3 Configuring the Attributes of the Upstream Port**.

Step 3 (Optional) Configure redundancy backup for the upstream link.

To ensure reliability of the upstream GE link, you can configure the redundancy backup of the upstream port in two upstream-transmission modes. For detailed procedure, see **7.2 Configuring the Link Aggregation of Uplink Ethernet Port** .

----End

Example

To add upstream port 0/0/0 to VLAN 100, do as follows:

```
huawei(config)#port vlan
{ vlan-list<S><Length 1-256>|vlanid<U><1,4093> }:100
{ frame/slot<S><Length 1-15>|to<K> }:0/0
{ portlist<S><Length 1-256> }:0

  Command:
          port vlan 100 0/0 0
```

4.3 (Optional) Configuring the Attributes of the Ethernet Port

This topic describes how to configure the attributes of a specified Ethernet port so that the system communicates with the user access device in the normal state. If the attributes of a specified Ethernet port do not meet the requirements in the actual application, configure the attributes.

Context

The MA5621 need to be interconnected with the user access device through the Ethernet port. Therefore, pay attention to the consistency of port attributes.

Default configuration

Table 4-5 lists the default settings of the attributes of an Ethernet port.

Table 4-5 Default settings of the attributes of an Ethernet port

Parameter	Default Setting (Electrical Port)
Auto-negotiation mode of the port	Enabled
Port rate	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the port rate.
Duplex mode	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the duplex mode.
Network cable adaptation mode	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the network cable adaptation mode.

Procedure

Step 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).

Step 2 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:

- Ensure 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.

Step 3 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:

- Ensure that the ports of two interconnected devices work in the same duplex mode. This prevents communication failure.
- The auto-negotiation mode needs to be disabled.

Step 4 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.

----End

Example

Assume that:

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

To configure the Ethernet port 0/1/1, do as follows:

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

4.4 Creating the Ethernet Access Service Port

The service port is used to connect the user side to the network side. To provision services, the service port must be created.

Context

A service port can carry a single service or multiple services. When a service port on the MA5621 carries multiple services, the service streams can be classified as follows:

- By user-side VLAN
- By user-side service encapsulation mode
- By user-side packet priority

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.

Step 2 Create the service port.

You can 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.
  - Multi-service service port based on the user-side VLAN:

    Select **multi-service user-vlan** { **other-all** | **priority-tagged** | **untagged** | *user-vlanid* }.
    - **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* is 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 of transparent LAN service (TLS) are created and are mainly used in the QinQ transparent transmission service for enterprises. All the services except known service in the system is carried on this service port.
  - By user-side packet priority (802.1p)

    Select **multi-service user-8021p** *user-8021p*.
  - By user-side service encapsulation mode

    Select **multi-service 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. Thus, the configuration of service ports is simplified. During the creation of a service port, *index* indicates the index of the service port and it is optional. If you do not specify the index, the system automatically adopts the smallest idle index.
  - **vlan** indicates the S-VLAN. An S-VLAN can only be a MUX VLAN or smart VLAN.
  - **rx-cttr** is the same as **outbound** in terms of meanings and functions. Either of them indicates the index of the traffic profile from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meanings and functions. Either of them indicates the index of the traffic profile from the user side to the network side.
- Run the **multi-service-port** command to create service ports in batches.

Step 3 (Optional) Configure the attributes of the service port.

Run the **service-port desc** command to configure the description of the service port. To facilitate maintenance, you can add information such as the function of the service port.

----End

Example

Assume that the access service port is 0/1/1, the user-side VLAN is 2, and the upstream VLAN is 100; the traffic profile 8 is used, the specified profile name is huawei, the CIR is 10240; the upstream priority is specified to 0, and packet priority policy is based on the traffic profile that is scheduled according to the local priority setting. To configure a service port for Internet access service in Ethernet access mode, do as follows:

```
huawei(config)#traffic table ip
{ cir<K>|index<K>|modify<K>|name<K> }:index
{ row-index<U><0,63> }:8
{ cir<K>|name<K> }:name
{ name<S><Length 1-32> }:huawei
{ cir<K> }:cir
{ cir<U><64,1024000>|off<K> }:10240
{ cbs<K>|color-mode<K>|pbs<K>|pir<K>|priority<K> }:priority
{ prival<U><0,7>|user-cos<K>|user-inner-cos<K>|user-tos<K> }:0
{ inner-priority<K>|priority-policy<K> }:priority-policy
{ priority-policy<E><Local-Setting,Tag-In-Package> }:local-Setting

  Command:
          traffic table ip index 8 name net cir 10240 priority 0 priority-policy
 local-setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 8
  TD Name              : net
  Priority             : 0
  Copy Priority        : -
  CTAG Mapping Priority: -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                  : 10240 kbps
  CBS                  : 329680 bytes
  PIR                  : 20480 kbps
  PBS                  : 657360 bytes
  Color Mode           : color-blind
  Referenced Status    : not used
  ------------------------------------------------

huawei(config)#service-port
{ desc<K>|index<U><0,511>|remote-desc<K>|vlan<K> }:1
{ adminstatus<K>|inbound<K>|outbound<K>|vlan<K> }:vlan
{ transparent<K>|vlanid<U><1,4093> }:100
{ eth<K> }:eth
{ frameid/slotid/portid<S><Length 1-15> }:0/1/1
{ multi-service<K> }:multi-service
{ user-8021p<K>|user-encap<K>|user-vlan<K> }:user-vlan
{ other-all<K>|priority-tagged<K>|untagged<K>|user-vlanid<U><1,4095> }:2
{ bundle<K>|inbound<K>|rx-cttr<K>|user-encap<K> }:rx-cttr
{ rx-index<U><0,63> }:8
{ tx-cttr<K> }:tx-cttr
{ tx-index<U><0,63> }:8

  Command:
          service-port 1 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-cttr 8 tx-
cttr 8
```

5 Configuring the Serial Port Data Service

About This Chapter

The MA5621 provides the serial port data service using the TCP/IP protocol stack. This service, when coupled with the intelligent power distribution solution of the electrical power network, achieves intelligent power distribution and centralized metering.

1. 5.1 Configuring the Serial Port Working Mode
   The MA5621 supports two serial port working modes, RS-232 and RS-485. After the serial port working mode is configured, the MA5621 can communicate with terminal units.
2. 5.2 (Optional) Configuring Serial Port Attributes
   Serial port attributes include the baud rate, data bit, parity check, and stop bit. After the serial port attributes are configured, the MA5621 can communicate with terminal units.
3. 5.3 Configuring the Serial Port Connection
   After the serial port connection is configured, the serial port data can be carried using Socket. This helps a master station server and terminal units transmit serial port data over the serial port line and the Ethernet network.

5.1 Configuring the Serial Port Working Mode

The MA5621 supports two serial port working modes, RS-232 and RS-485. After the serial port working mode is configured, the MA5621 can communicate with terminal units.

Procedure

Step 1 Run the **interface serial** command to enter SERIAL mode.

Step 2 Run the **port mode** command to configure the serial port working mode.

Ports 0 and 1 default to RS-485 and ports 2 and 3 default to RS-232.

Step 3 Run the **display port state** command to query the serial port working mode.

Step 4 Run the **save** command to save the data.

----End

Example

Assume that the serial port working mode of the terminal unit connected to the MA5621 is RS-485. To configure the serial port working mode of the MA5621 to the same as that of the terminal unit, do as follows:

```
huawei(config)#interface serial 0/2
huawei(config-if-serial-0/2)#port mode 0 rs485
huawei(config-if-serial-0/2)#display port state 0
  Mode      : RS485
  Baud-Rate : 9600
  Data-Bit  : 8
  Parity    : EVEN
  Stop-Bit  : 1
  Flow-Ctrl : NONE
huawei(config-if-serial-0/2)#quit
huawei(config)#save
```

5.2 (Optional) Configuring Serial Port Attributes

Serial port attributes include the baud rate, data bit, parity check, and stop bit. After the serial port attributes are configured, the MA5621 can communicate with terminal units.

Default Settings

Table 5-1 lists the default serial port attributes of the MA5621.

Table 5-1 Default serial port attributes of the MA5621

Item	Default Setting
Baud rate	9600 bit/s
Data bit	8
Parity check	even

Item	Default Setting
Stop bit	1

Procedure

Step 1 Run the **interface serial** command to enter SERIAL mode.

Step 2 Run the **port config** command to configure the serial port attributes.

The data bit, stop bit, parity check and baud rate of the MA5621 must be the same as that of terminal units. You can use their default values or specify a value based on site requirements.

Step 3 Run the **display port state** command to query the serial port attributes.

Step 4 Run the **save** command to save the data.

----End

Example

Assume that the baud rate of the terminal unit connected to the MA5621 is 19200 bit/s. To configure the baud rate of the MA5621 to the same as that of the terminal unit, do as follows:

```
huawei(config)#interface serial 0/2
huawei(config-if-serial-0/2)#port config 0 baudrate 19200
huawei(config-if-serial-0/2)#display port state 0
  Mode      : RS485
  Baud-Rate : 19200
  Data-Bit  : 8
  Parity    : EVEN
  Stop-Bit  : 1
  Flow-Ctrl : NONE
huawei(config-if-serial-0/2)#quit
huawei(config)#save
```

5.3 Configuring the Serial Port Connection

After the serial port connection is configured, the serial port data can be carried using Socket. This helps a master station server and terminal units transmit serial port data over the serial port line and the Ethernet network.

Prerequisite

A reachable route is available between the VLAN Layer 3 interface of the MA5621 and the interface of a master station server.

Procedure

Step 1 Configure the VLAN Layer 3 interface.

1. Run the **vlan** command to create a VLAN.
2. Run the **port vlan** command to add an uplink port to the VLAN.
3. Run the **interface vlanif** command to enter VLANIF mode.

4. Run the **ip address** command to set the IP address of the VLAN Layer 3 interface.
5. Run the **quit** command to quit VLANIF mode.

Step 2 Run the **serialop-connection** command to create a serial port connection.

- Each serial port supports one serial port connection.
- **local-address**: indicates the IP address of the VLAN Layer 3 interface.
- **local-port/peer-port**: indicates the local port/peer port. Ports used for certain services cannot be used as the local port/peer port and the local port/peer port must be unique.
- **peer-address**: indicates the IP address of the interface of a master station server.
- **frame-type**: indicates the serial port frame types supported by the MA5621, including FT1.2, DL645, DL698, user-defined, and none. Generally, the default value is used and you can change the settings based on site requirements.

Step 3 Run the **display serialop-connection** command to query the serial port connection.

Step 4 Run the **save** command to save the data.

----End

Example

Assume that the MA5621 has the following parameters to obtain the serial port data of a terminal unit through a serial port identified by port ID, encapsulate the serial port data into Transmission Control Protocol (TCP) packets, and transmit the packets upstream to a master station server over the IP network:

- VLAN ID: 30
- IP address of the VLAN Layer 3 interface: 10.1.1.3
- Working mode: tcp-server
- Local port ID: 3000
- Remote IP address: 10.10.1.10
- Remote port ID: 3000

To configure these parameters, do as follows:

```
huawei(config)#vlan 30 standard
huawei(config)#port vlan 30 0/0 0
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.1.1.3 24
huawei(config-if-vlanif30)#quit
huawei(config)#serialop-connection 1 port 0/2/0 working-mode tcp-server local-
address
 10.1.1.3 local-port 3000 peer-address 10.10.1.10 peer-port 3000 frame-type ft1.2
huawei(config)#display serialop-connection all
  -------------------------------------------------------------------------
   ConnectID F/S/P   mode Local Address   Local Peer Address      Peer Frame
                                          Port                    Port Type
  -------------------------------------------------------------------------
           1 0/2/0   TCPS 10.1.1.3         3000 10.10.1.10        3000 ft1.2
  -------------------------------------------------------------------------
  Total :  1
huawei(config)#save
```

6 Configuring the Ethernet OAM

About This Chapter

Operation, administration, and maintenance (OAM) refers to a method of monitoring and diagnosing network faults. The Ethernet OAM feature includes two sub-features, namely, Ethernet CFM OAM and Ethernet EFM OAM.

6.1 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.

Prerequisite

- 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.

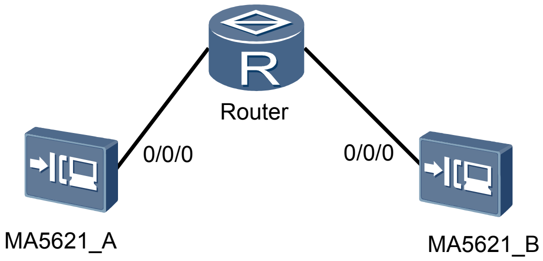
Ethernet is a widely used local area network (LAN) technology. It provides rich bandwidth, features low cost, and supports plug-and-play and multipoint operations. As the Ethernet technology is developing from carriers' networks to metropolitan area networks (MANs) and wide area networks (WANs), the 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 6-1 shows the example network of the Ethernet CFM OAM function.

Figure 6-1 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***mdindex***name-format** { **no-name** | **dns-name***dns-name* | **mac-integer***mac-address* | **string***string* } **level***level* [**mhf-creation**{ **no-mhf** | **default-mhf** | **explicit-mhf** }] 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:

- MA5621_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.
- MA5621_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 *MA5621_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 *MA5621_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
```

6.2 Configuring the Ethernet EFM OAM

Ethernet in the First Mile (EFM) OAM is defined in IEEE 802.3ah to make the Ethernet physical-layer specifications in respect of the user access part and the Ethernet OAM in respect of the access part. Ethernet EFM OAM is used for the link detection of the last mile and it is the link-level OAM.

Prerequisite

- Network devices and lines must be in the normal state.
- The OLT must support the Ethernet EFM OAM function.

Context

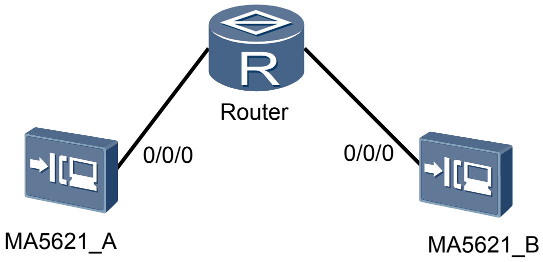
OAM is a key method of reducing network maintenance cost.

Ethernet EFM OAM is defined in IEEE 802.3ah Clause 57 and it is a key component of Ethernet OAM. Ethernet EFM OAM provides a mechanism for monitoring links, such as remote defect indication (RDI) and remote loopback control. It is an L2 mechanism, as a complement to the higher layer applications.

Networking

Figure 6-2 shows the example network of the Ethernet EFM OAM function.

Figure 6-2 Example network of the Ethernet EFM OAM function



Procedure

Step 1 Run the **efm oam mode** command to configure the Ethernet EFM OAM mode of the port.

- The default Ethernet EFM OAM mode of the port is the active mode.
- After the Ethernet EFM OAM function is enabled on the port, the mode of the port cannot be changed.
- When the Ethernet EFM OAM mode of both the local and peer devices is the passive mode, the Ethernet EFM OAM function cannot be enabled. The Ethernet EFM OAM function can be enabled only when the Ethernet EFM OAM mode of the device at one end is the active mode.

Step 2 Run the **efm oam** { *frameid/slotid* | *frameid/slotid/portid* } **enable** command to enable the Ethernet EFM OAM function on the port.

By default, the Ethernet EFM OAM function on the port is disabled.

Step 3 (Optional) Run the **efm loopback** command to configure the start, end, and control parameters for the Ethernet EFM OAM loopback on the port.

- By default, the Ethernet EFM OAM loopback is not performed.
- After the Ethernet EFM OAM loopback is started, all the services are interrupted.

Step 4 Run the **efm error-frame** command to set error frame parameters and the status of the error frame alarm function. In this manner, the link signals and data quality can be monitored.

Step 5 Query the configuration information about the Ethernet EFM OAM function.

- Run the **display efm oam status** command to query the status of the Ethernet EFM OAM function.
- Run the **display efm oam event config** command to query the parameters of the Ethernet EFM OAM event.

----End

Example

- MA5621_A: The Ethernet EFM OAM function is enabled; the Ethernet EFM OAM mode is in the active mode; the error frame alarm function is enabled; the local error frame window is 1; the error frame threshold is 1.
- MA5621_B: The Ethernet EFM OAM function is enabled; the Ethernet EFM OAM mode is in the passive mode; the error frame alarm function is enabled; the local error frame window is 1; the error frame threshold is 1.

Configure MA5621_A:

```
huawei(config)#efm oam mode 0/0/0 active
huawei(config)#efm oam 0/0/0 enable
huawei(config)#efm error-frame 0/0/0 notification enable
huawei(config)#efm error-frame 0/0/0 period 1
huawei(config)#efm error-frame 0/0/0 threshold 1
```

*Run the **display efm oam status** command to query the status of the Ethernet EFM OAM function.*

```
huawei(config)#display efm oam status
{ frameid/slotid/portid<S><Length 1-15> }:0/0/0
{ local<K>|remote<K> }:local

  Command:
          display efm oam status 0/0/0 local
  Admin Status                   : Enable
  Operation Status               : LinkFault
  OAM Mode                       : Active  //The local Ethernet OAM mode is the 
active mode.
  Max OAM PDU Size               : 1514
  Stable & Evaluation            : 1
  Configuration Revision         : 0
  Multiplexer Action             : Forward
  Parser Action                  : Forward
  Unidirectional Support         : No
  Loopback Support               : Yes
  Event Support                  : Yes
  Variable Support               : No
```

*Run the **display efm oam event config** command to query the parameters of the Ethernet EFM OAM event.*

```
huawei(config)#display efm oam event config
{ frameid/slotid/portid<S><Length 1-15> }:0/0/0

  Command:
          display efm oam event config 0/0/0
  Errored Symbol Period Event                     :Disable
  Errored Symbol Period Event Window              :-
  Errored Symbol Period Event Threshold           :-
  Errored Frame Event                             :Enable  //The error frame alarm 
function is enabled.
  Errored Frame Event Window                      :1       //The error frame window 
is 1.
  Errored Frame Event Threshold                 :1       //The error frame threshold 
is 1.
  Errored Frame Period Event                      :Disable
  Errored Frame Period Event Window               :-
  Errored Frame Period Event Threshold            :-
  Errored Frame Seconds Summary Event             :Disable
  Errored Frame Seconds Summary Event Window      :-
  Errored Frame Seconds Summary Event Threshold   :-
  Link Fault Event                                :Enable
  Dying Gasp Event                                :Disable
  Critical Link Event                             :Disable
```

Configure MA5621_B:

```
huawei(config)#efm oam  mode 0/0/0 passive
huawei(config)#efm oam 0/0/0 enable
huawei(config)#efm error-frame 0/0/0 notification enable
huawei(config)#efm error-frame 0/0/0 period 1
huawei(config)#efm error-frame 0/0/0 threshold 1
```

*Run the **display efm oam status** command to query the status of the Ethernet EFM OAM function.*

```
huawei#display efm oam status
{ frameid/slotid/portid<S><Length 1-15> }:0/0/0
{ local<K>|remote<K> }:local    //Query the local Ethernet OAM status. If you need 
to query the remote Ethernet OAM status, select remote.

  Command:
          display efm oam status 0/0/0 local
  Admin Status                   : Enable   //The Ethernet OAM function is 
enabled.
  Operation Status               : Operational
  OAM Mode                       : Passive  //The local Ethernet OAM mode is the 
passive mode.
  Max OAM PDU Size               : 1514
  Stable & Evaluation            : 2
  Configuration Revision         : 0
  Multiplexer Action             : Forward
  Parser Action                  : Forward
  Unidirectional Support         : No
  Loopback Support               : No
  Event Support                     : Yes
  Variable Support                  : No
```

Run the ***display efm oam event config*** *command to query the parameters of the Ethernet EFM OAM event.*

```
huawei(config)#display efm oam event config 0/0/0
  Errored Symbol Period Event                       :Disable
  Errored Symbol Period Event Window                :-
  Errored Symbol Period Event Threshold             :-
  Errored Frame Event                               :Enable  //The error frame alarm
function is enabled.
  Errored Frame Event Window                        :1       //The error frame window
is 1.
  Errored Frame Event Threshold                   :1       //The error frame threshold
is 1.
  Errored Frame Period Event                        :Disable
  Errored Frame Period Event Window                 :-
  Errored Frame Period Event Threshold              :-
  Errored Frame Seconds Summary Event               :Disable
  Errored Frame Seconds Summary Event Window        :-
  Errored Frame Seconds Summary Event Threshold     :-
  Link Fault Event                                  :Enable
  Dying Gasp Event                                  :Disable
  Critical Link Event                               :Disable
```

7 Configuring Network Protection

About This Chapter

The MA5621 provides a network protection mechanism to improve the system reliability. The mechanism maximally secures the network and services of carriers and minimizes loss if an exception occurs.

7.1 Configuring the MSTP

This topic describes how to configure MSTP on the MA5621.

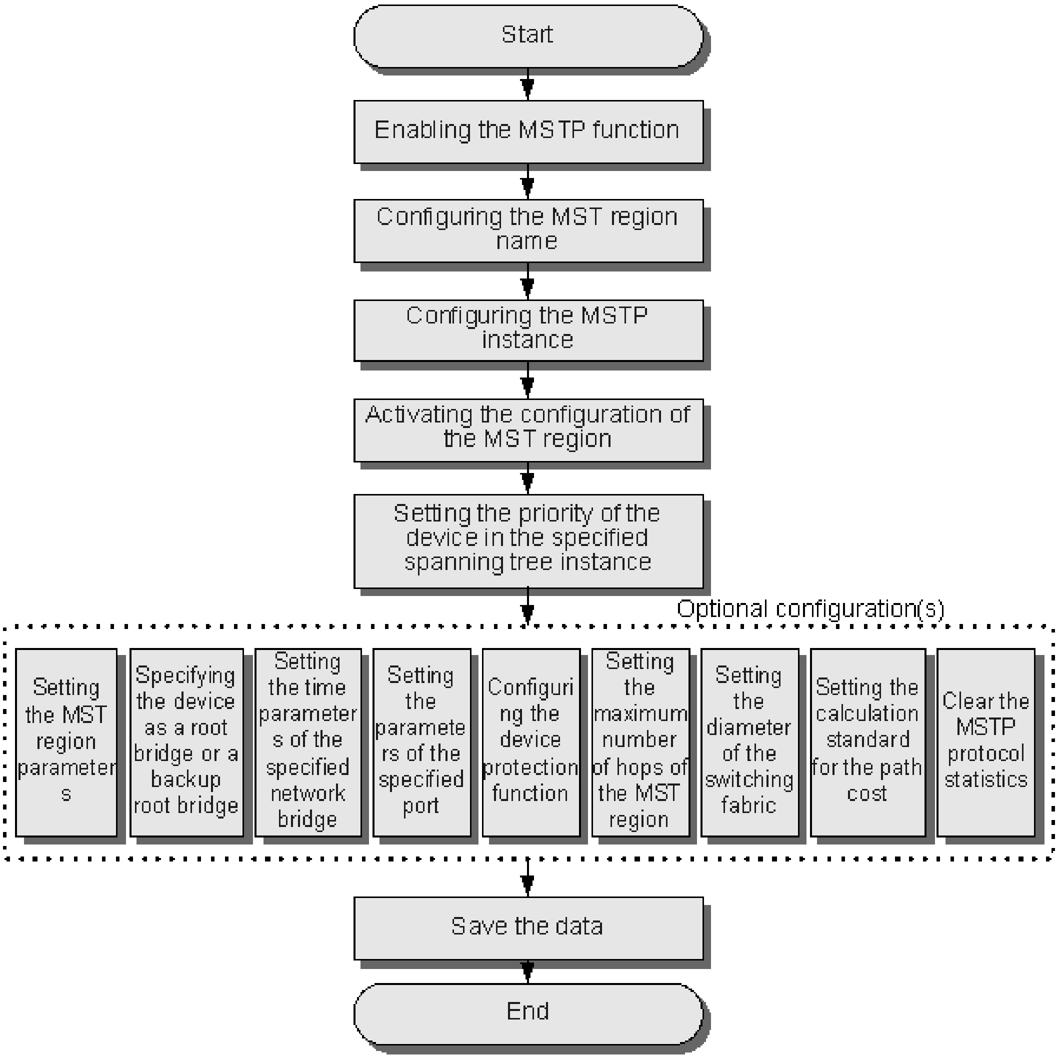
Context

- MSTP applies to a redundant network. It makes up for the drawback of STP and RSTP. MSTP makes the network converge fast and the traffic of different VLANs distributed along their respective paths, which provides a better load-sharing mechanism.
- MSTP trims a loop network into a loop-free tree network. It prevents the proliferation and infinite cycling of the packets in the loop network. In addition, MSTP provides multiple redundant paths for VLAN data transmission to achieve the load-sharing purpose.

Configuration Flowchart

Figure 7-1 shows the flowchart for configuring the MSTP.

Figure 7-1 Flowchart for configuring the MSTP


Start
Enabling the MSTP function
Configuring the MST region name
Configuring the MSTP instance
Activating the configuration of the MST region
Setting the priority of the device in the specified spanning tree instance
Optional configuration(s)
Setting the MST region parameters
Specifying the device as a root bridge or a backup root bridge
Setting the time parameters of the specified network bridge
Setting the parameters of the specified port
Configuring the device protection function
Setting the maximum number of hops of the MST region
Setting the diameter of the switching fabric
Setting the calculation standard for the path cost
Clear the MSTP protocol statistics
Save the data
End

Procedure

Step 1 Enabling the MSTP function.

- By default, the MSTP function is disabled.
- After the MSTP function is enabled, the device determines whether it works in STP compatible mode or MSTP mode based on the configured protocol.
- After the MSTP function is enabled, MSTP maintains dynamically the spanning tree of the VLAN based on the received BPDU packets. After the MSTP function is disabled, if the transparent transmission of BPDU packets is disabled, the MSTP device becomes a transparent bridge and does not maintain the spanning tree.

1. Run the **stp enable** command or the **stp port** ***frameid/slotid/portid*** **enable** command to enable the MSTP function of the bridge or the port.
2. Run the **display stp** command or the **display stp port** command to query the MPLS state of the bridge or the port.

Step 2 Configuring the MST region name.

1. Run the **stp region-configuration** command to enter MST region mode.
2. Run the **region-name** command to configure the name of the MST region.
3. Run the **check region-configuration** command to query the parameters of the current MST region.

Step 3 Configuring the MSTP instance.

The MSTP protocol configures the VLAN mapping table (mapping between the VLAN and the spanning tree), which maps the VLAN to the spanning tree.

- By default, all VLANs are mapped to CIST, that is, instance 0.
- One VLAN can be mapped to only one instance. If you re-map a VLAN to another instance, the original mapping is disabled.
- A maximum of 10 VLAN sections can be configured for an MSTP instance.

1. Run the **instance** ***instance-id*** **vlan** command to map the specified VLAN to the specified MSTP instance.
2. Run the **check region-configuration** command to query the parameters of the current MST region.

Step 4 Activating the configuration of the MST region.

1. Run the **active region-configuration** command to activate the configuration of the MST region.
2. Run the **display stp region-configuration** command to query the effective configuration of the MST region.
3. Run the **quit** command to quit MST region mode.

Step 5 Other optional configurations.

- Setting the priority of the device in the specified spanning tree instance.
  - Run the **stp priority** command to set the priority of the device in the specified spanning tree instance.
  - Run the **display stp** command to query the MSTP configuration of the device.

- Setting the MST region parameters.
  - Run the **stp md5-key** command to set the MD5-Key for the MD5 encryption algorithm configured on the MST region.
  - In the MSTP region mode, run the **vlan-mapping module** command to map all VLANs to the MSTP instances by modular arithmetic.
  - In the MSTP region mode, run the **revision-level** command to set the MSTP revision level of the device.
  - Run the **reset stp region-configuration** command to restore the default settings to all parameters of the MST region.
- Specifying the device as a root bridge or a backup root bridge.
  - Run the **stp root** command to specify the device as a root bridge or a backup root bridge.
- Setting the time parameters of the specified network bridge.
  - Run the **stp timer forward-delay** command to set the Forward Delay of the specified network bridge.
  - Run the **stp timer hello** command to set the Hello Time of the specified network bridge.
  - Run the **stp timer max-age** command to set the Max Age of the specified network bridge.
  - Run the **stp time-factor** command to set the timeout time factor of the specified network bridge.
- Setting the parameters of the specified port.
  - Run the **stp port** ***frameid/slotid/portid*** **transmit-limit** command to set the number of packets transmitted by the port within the Hello Time.
  - Run the **stp port** ***frameid/slotid/portid*** **edged-port enable** command to set the port as an edge port.
  - Run the **stp port** ***frameid/slotid/portid*** **cost** command to set the path cost of a specified port.
  - Run the **stp port** ***frameid/slotid/portid*** **port-priority** command to set the priority of the specified port.
  - Run the **stp port point-to-point** command to set whether the link that is connected to the port is a point-to-point link.
- Configuring the device protection function.
  - Run the **stp bpdu-protection enable** command to enable the BPDU protection function of the device.
  - Run the **stp port** ***frameid/slotid/portid*** **loop-protection enable** command to enable the loop protection function of the port.
  - Run the **stp port** ***frameid/slotid/portid*** **root-protection enable** command to enable the root protection function of the port.
- Setting the maximum number of hops of the MST region.
  - Run the **stp max-hops** command to set the maximum number of hops of the MST region.
- Setting the diameter of the switching fabric.
  - Run the **stp bridge-diameter** command to set the diameter of the switching fabric.
- Setting the calculation standard for the path cost.
  - Run the **stp pathcost-standard** command to set the calculation standard for the path cost.
- Clear the MSTP protocol statistics.

- Run the **reset stp statistics** command to clear the MSTP protocol statistics.

----End

Example

Assume that:

- MSTP function: enabled
- MST region name: hwrg1
- VLAN 2-VLAN 10 and VLAN 12-VLAN 16 are mapped to MSTP instance 1.
- Priority of the device in a specified spanning tree instance: 0.
- Maximum number of hops in the MST region: 10
- Diameter of the switching network: 6
- BPDU protection function: enabled

To configure the MSTP with these parameters, do as follows:

```
huawei(config)#stp enable
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg1
huawei(stp-region-configuration)#instance 1 vlan 2 to 10 12 to 16
huawei(stp-region-configuration)#active region-configuration
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 1 priority 0
huawei(config)#stp max-hops 10
huawei(config)#stp bridge-diameter 6
huawei(config)#stp bpdu-protection enable
```

7.2 Configuring the Link Aggregation of Uplink Ethernet Port

Port aggregation means aggregating the two uplink GE ports on the MA5621 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.

Prerequisite

- The network device and the line must be normal.
- The VLAN of the interface on the upper-layer device of the MA5621 must be consistent with the VLAN configured for the uplink port on the MA5621.

Context

- Ensure that the configurations of the Ethernet port attributes on two aggregation ports are 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.

If the aggregation group is a static Link Aggregation Control Protocol (LACP) group, run the **display lacp link-aggregation port***frame/slot/port* command to query the type, role, and status of an aggregated port.

----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 uplink ports 0/0/0 and 0/0/1 of the MA5621 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)
```

8 Configuration Examples of MA5621 Services

About This Chapter

This topic describes how to configure the Ethernet access service and serial port access service on the MA5621 in various scenarios.

8.1 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 MA5621.

8.1.1 Configuration Example of the VLAN Stacking Wholesale Service

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.

Prerequisite

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

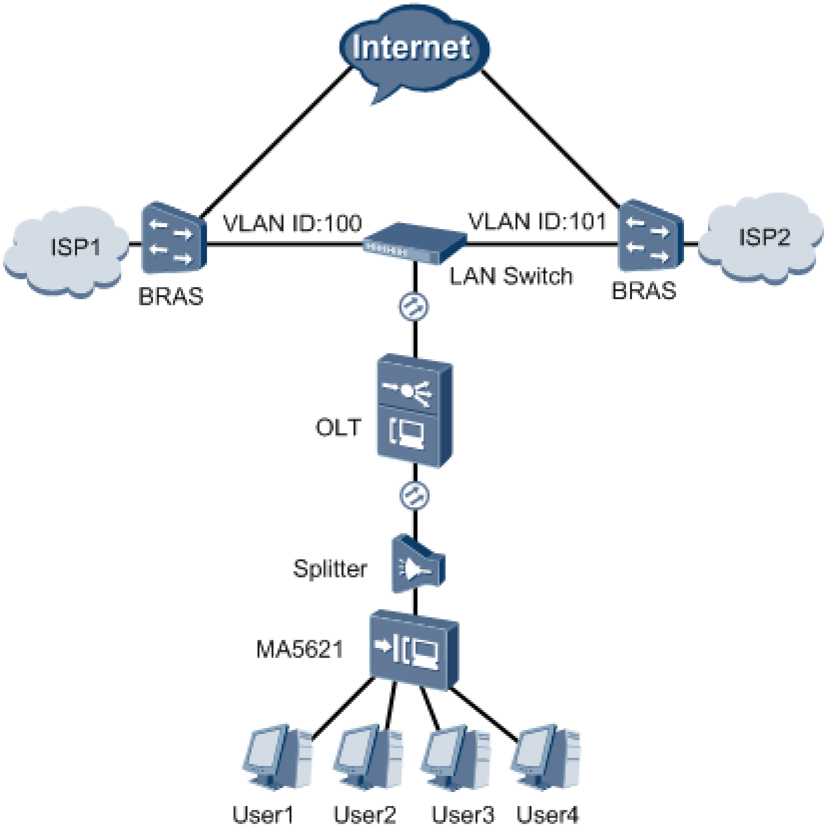
- The user accesses the Internet through the PPPoE dialup.
- The device adds an outer VLAN tag to user packets to identify ISPs, and adds an inner VLAN tag to identify users.

Networking

Figure 8-1 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 MA5621 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 8-1 Example network for configuring the VLAN stacking wholesale service



Data Plan

Table 8-1 provides the data plan for configuring the VLAN stacking wholesale service.

Table 8-1 Data plan for configuring the VLAN stacking wholesale service

Item	Data
ISP 1 user group	Uplink port: 0/0/0
	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: 0/0/0

Item	Data
	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 MA5621. You can also run the **stacking inner-ethertype** command to set the type of inner Ethernet protocol supported by VLAN stacking on the MA5621. 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 0/0/0 to VLAN 100 and VLAN 101.

```
huawei(config)#port vlan 100-101 0/0 0
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the port VLAN(s) having been added is 2
```

Step 4 Add service ports to the VLAN.

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 eth 0/1/0 multi-service user-encap pppoe rx-
cttr 6
```

```
tx-cttr 6
huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-encap pppoe rx-
cttr 6
tx-cttr 6
huawei(config)#service-port 3 vlan 101 eth 0/1/2 multi-service user-encap pppoe rx-
cttr 6
tx-cttr 6
huawei(config)#service-port 4 vlan 101 eth 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
  -------------------------------------------------------------------------
      1  100 stacking eth  0/1/ 0  -    -     encap pppoe      6    6 up
      2  100 stacking eth  0/1/ 1  -    -     encap pppoe      6    6 up
      3  101 stacking eth  0/1/ 2  -    -     encap pppoe      6    6 up
      4  101 stacking eth  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

```
vlan 100 to 101 smart
vlan attrib 100 to 101 stacking
port vlan 100 to 101 0/0 0
service-port 1 vlan 100 eth 0/1/0 multi-service user-encap pppoe  rx-cttr 6 tx-cttr
6
service-port 2 vlan 100 eth 0/1/1 multi-service user-encap pppoe  rx-cttr 6 tx-cttr
6
service-port 3 vlan 101 eth 0/1/2 multi-service user-encap pppoe  rx-cttr 6 tx-cttr
6
service-port 4 vlan 101 eth 0/1/3 multi-service user-encap pppoe  rx-cttr 6 tx-cttr
6
stacking label service-port 1 11
stacking label service-port 2 12
stacking label service-port 3 11
stacking label service-port 4 12
```

8.1.2 Configuration Example of the VLAN ID Extension Service

In the application of the VLAN ID extension, the 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.

Prerequisite

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

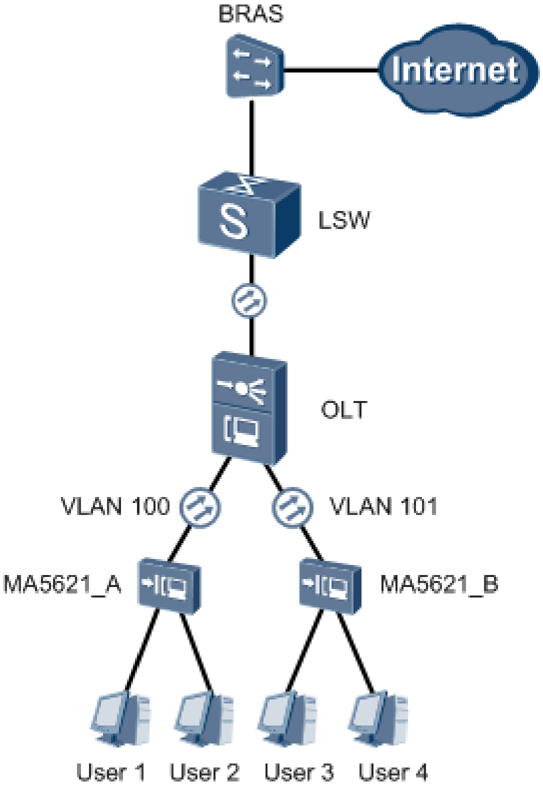
- The Internet access service is deployed on the network.
- Two VLAN IDs are allocated on the BRAS to identify four access users.
- The MA5621 is used on the GPON upstream transmission network.

Networking

Figure 8-2 shows the example network for configuring the VLAN ID extension.

Broadband users through multiple MA5621s 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 MA5621 that accesses users, and the inner VLAN tag identifies the users of the device.

Figure 8-2 Example network for configuring the VLAN ID extension



Data Plan

Table 8-2 provides the data plan for configuring the VLAN ID extension.

Table 8-2 Data plan for configuring the VLAN ID extension

Item	Data
MA5621_A	Uplink port: 0/0/0
	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
MA5621_B	Uplink port: 0/0/0

Item	Data
	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 MA5621_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 0
```

4. Add service ports to the VLAN.

```
huawei(config)#service-port vlan 100 eth 0/1/2 multi-service user-encap
pppoe rx-cttr 6 tx-cttr 6
huawei(config)#service-port vlan 100 eth 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 stacking eth  0/1 /2  -    -     encap pppoe       6   6
up
      1  100 stacking eth  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 MA5621_B is as follows:

  The configuration procedure of MA5621_B is the same as the configuration procedure of MA5621_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 MA5621_A and MA5621_B can access the Internet.

Two users of the MA5621 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 MA5621_A

```
vlan 100 smart
vlan attrib 100 stacking
port vlan 100 0/0 0
service-port 0 vlan 100 eth 0/1/2 multi-service user-encap pppoe  rx-cttr 6 tx-cttr
6
service-port 1 vlan 100 eth 0/1/3 multi-service user-encap pppoe  rx-cttr 6 tx-cttr
6
stacking label service-port 0 11
stacking label service-port 1 12
save
```

Configuration file of MA5621_B

```
vlan 101 smart
vlan attrib 101 stacking
port vlan 101 0/0 0
service-port 0 vlan 101 eth 0/1/2 multi-service user-encap pppoe  rx-cttr 6 x-cttr
6
service-port 1 vlan 101 eth 0/1/3 multi-service user-encap pppoe  rx-cttr 6 x-cttr
6
stacking label service-port 0 11
stacking label service-port 1 12
```

8.2 Configuration Example of the QinQ VLAN Private Line Service

This topic describes how to configure the private line service based on the QinQ feature. A virtual local area network (VLAN) packet with the QinQ attribute has VLAN tags of two layers, inner VLAN tag from the private network and outer VLAN tag from the MA5621. With the two VLAN tags, a Layer 2 virtual private network (VPN) tunnel is formed between private networks. The VPN tunnel is a secure channel for transparently transmitting services between private networks.

Prerequisite

- The network device and the line must be normal.
- The control board and the service boards must be in the normal state.
- The MA5621 must be connected to the upper-layer network through the OLT. The upper-layer network must work in L2 mode, and forwards packets based on the VLAN and the MAC address.

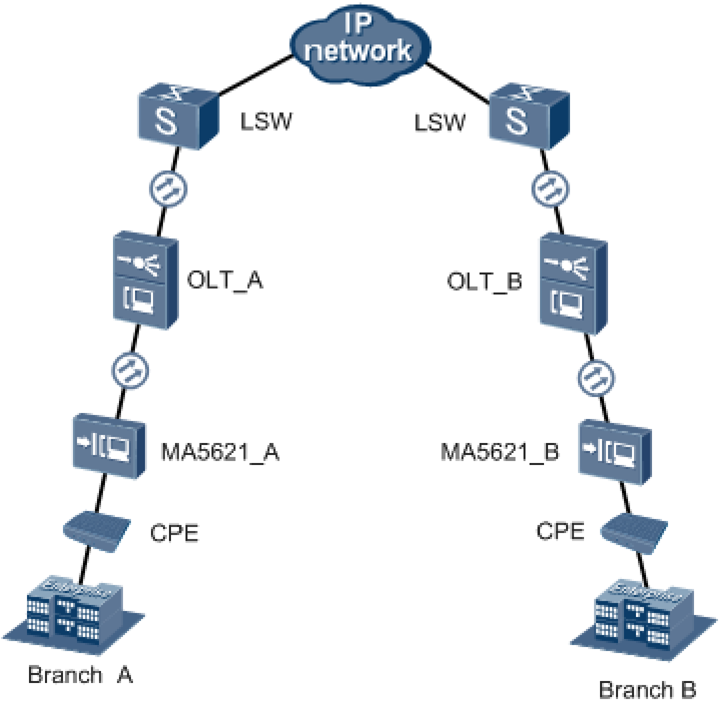
Service Requirements

- The two branches (A and B) of the enterprise are connected to the MAN through MA5621_A and MA5621_B respectively.
- On MA5621_A and MA5621_B, configure the QinQ VLAN private line service for the enterprise, so that the service and the bridge protocol data units (BPDUs) between different branches can be transparently transmitted through the public network.

Networking

Figure 8-3 shows an example network for configuring the QinQ VLAN private line service.

Figure 8-3 Example network for configuring the QinQ VLAN private line service



Data Plan

Table 8-3 provides the data plan for configuring the QinQ VLAN private line service.

Table 8-3 Data plan for configuring the QinQ VLAN private line service

Device	Item	Data
MA5621_A **NOTE** The data plan of MA5621_B is the same as the data plan of MA5621_A.	ETH port	0/1/1
	Upstream port	0/0/0
	Network-side VLAN	100
	VLAN type	Smart VLAN
	VLAN attribute	QinQ
	User-side VLAN	50
	VLAN service profile	Profile ID: 1 Transparent transmission of BPDUs: enable

Procedure

- **The procedure for configuring the QinQ VLAN private line service on MA5621_A is as follows:**

  1. Create a VLAN.

     ```
     huawei(config)#vlan 100 smart
     ```

  2. Set the VLAN attribute to QinQ.

     ```
     huawei(config)#vlan attrib 100 q-in-q
     ```

  3. (Optional) Enable the transparent transmission of BPDUs and bind a VLAN service profile to the VLAN.

     ```
     huawei(config)#vlan service-profile profile-id 1
     huawei(config-vlan-srvprof-1)#bpdu tunnel enable
       Info: Please use the commit command to make modifications take effect
     huawei(config-vlan-srvprof-1)#commit
     huawei(config-vlan-srvprof-1)#quit
     huawei(config)#vlan bind service-profile 100 profile-id 1
     ```

  4. Add an upstream port to the VLAN.

     ```
     huawei(config)#port vlan 100 0/0 0
     ```

  5. Add the service ports to the VLAN. The default traffic profile 6 is applied.

     ```
     huawei(config)#service-port vlan 100 eth 0/1/1 multi-service user-vlan 50
     rx-cttr 6 tx-cttr 6
     ```

  6. Save the data.

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

- **The procedure for configuring the QinQ VLAN private line service on MA5621_B is as follows:**

  The configuration procedure of MA5621_B is the same as the configuration procedure of MA5621_A. Hence, it is not described here.

----End

Result

The branches of the enterprise located in two different places can communicate with each other in the normal state, implementing various services of the private network.

Configuration File

```
vlan 100 smart
vlan attrib 100 q-in-q
vlan service-profile profile-id 1
bpdu tunnel enable
port vlan 100 0/0 0
service-port vlan 100 eth 0/1/1 multi-service user-vlan 50 rx-cttr 6 tx-cttr 6
save
```

9 Configuration Example of the FTTx Service (GPON Access)

About This Chapter

This topic describes how to configure the data service in the GPON access mode in various FTTx scenarios.

The ONU can transmit video monitoring data through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

The ONU can intelligently collect power consumption information in the electrical power system through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

The ONU can automatically transmit power distribution site information in the electrical power system through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

The serial port access service carries the serial port data using the TCP/IP protocol stack. This service, when coupled with the intelligent power distribution solution of the electrical power network, achieves intelligent power distribution and centralized metering.

9.1 Configuration Example of Transmitting Video Monitoring Data by Using the Ethernet Access

The ONU can transmit video monitoring data through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

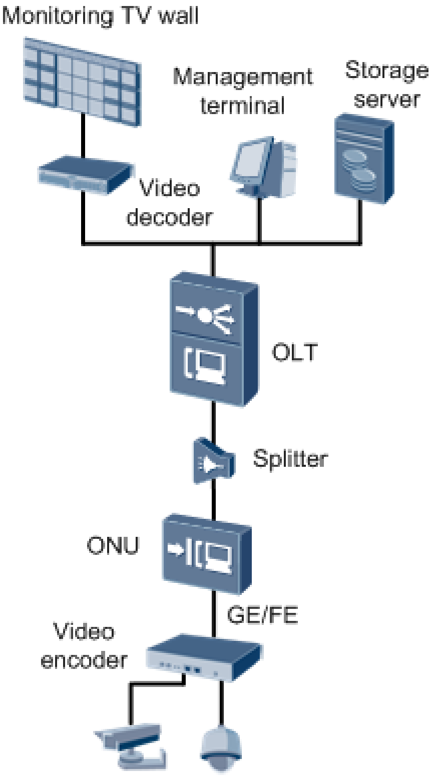
Service Requirements

- Located at a monitored point, the ONU is connected to video encoders through a GE/FE auto-adaptive electrical port. The ONU receives encoded video monitoring information and forwards the information upstream to an optical line terminal (OLT) at the monitoring center.
- The OLT forwards the information to other monitoring devices at the monitoring center.

Networking

Figure 9-1 shows the example network for configuring the video monitoring data transmission over Ethernet.

Figure 9-1 Example network for configuring the video monitoring data transmission over Ethernet



NOTE

This example uses MA5621 as the ONU.

Data Plan

Table 9-1provides the data plan for the OLT, and **Table 9-2** provides the data plan for the ONU.

Table 9-1 Data plan for configuring the video monitoring data transmission over Ethernet-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 100
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 0/3/1 ONU ID: 1 ONUauthentication mode: SN ONU SN: 48575443E6D8B541
DBA profile	Profile name: VideoMonitoring Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s
ONU line profile	Profile ID: 10, bound to the DBA profile named VideoMonitoring GEM port IDs: 0, 1 T-CONT ID: 5
ONU management mode	SNMP

Table 9-2 Data plan for configuring the video monitoring data transmission over Ethernet-ONU side

Configuration Item	Data	Remarks
IP address	Inband management IP address: 192.168.50.2/24	
Traffic profile	Index 6 (default)	-
Service port	0/1/1	-
Uplink port	0/0/0	-
Uplink VLAN	smart VLAN 100	The uplink VLAN must be the same as the user VLAN on the OLT.
User VLAN	smart VLAN 2	-

Procedure

Step 1 Configure the OLT.

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

   Create smart VLAN 100, and then add upstream port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured. For details, see Configuring Upstream Link Aggregation.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

   a. Add a DBA profile.

   You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

   Configure the profile name to VideoMonitoring, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name VideoMonitoring type3 assure
   20480 max 51200
   ```

   b. Add an ONU line profile.

   Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named VideoMonitoring. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10
   huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name
   VideoMonitoring
   ```

   Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting video monitoring information traffic streams. Bind GEM port 0 and GEM port 1 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

NOTE

1) To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the gem add command to configure the ID of the traffic profile bound to the GEM port.
2) When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of video monitoring information SVLAN 100 to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Add an alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port ont-auto-find command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to
  //the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number             : 1
   F/S/P              : 0/3/1
   Ont SN             : 48575443E6D8B541
   Password           :
   VenderID           : HWTC
   Ont Version        : MA5621
   Ont SoftwareVersion : V800R309C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-03-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

----------------------------------------------------------------------
  F/S/P               :
0/3/1
  ONT-ID              :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
  Match state         : match     //Indicates that the capability profile bound
to the ONU is
                                     //consistent with the actual capability
of the ONU.
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/3)#quit
```

   If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

   - If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
   - If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
   - If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

NOTE

If an ONT supports only four queues, the values of 4–7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8 and add upstream port 0/0/0 to it. Configure the inband management IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
255.255.255.0 manage-vlan 8
```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet *192.168.50.2*** command to telnet to the ONU and then configure the ONU.

8. Create a service port.

   Configure the Video Monitoring Data service port ID to 1, SVLAN ID to 100, GEM port ID to 1, CVLAN ID to 100. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 100 rx-cttr 6 tx-cttr 6
```

9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
   cos7 7
   ```

10. Save the data.

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

Step 2 Configure the ONU.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet** ***192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

   ```
   huawei(config)#telnet 192.168.50.2
   { <cr>|service-port<U><0,4294967295> }:

     Command:
             telnet 192.168.50.2
     Press CTRL_] to quit telnet mode
     Trying 192.168.50.2 ...
     Connected to 192.168.50.2 ...
   >>User name:root
   >>User password:       //It is not displayed on the console.
   ```

2. Create a VLAN.

   ```
   huawei(config)#vlan 100 smart
   ```

3. Add an uplink port to the VLAN.

   Add uplink port 0/0/0 to the VLAN.

   ```
   huawei(config)#port vlan 100 0/0 0
   ```

4. Create a service port.

Create service port 2. Its user VLAN ID is 2 and service VLAN ID is 100. Use the default traffic profile (traffic profile 6). To limit the traffic rate, run the **traffic table ip** command to configure the traffic profile.

```
huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-
cttr 6
tx-cttr 6
```

5. Save the data.

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

----End

Result

After the preceding configurations are complete, devices at the monitoring center (such as the storage server, management terminal, and video decoder) will receive video monitoring information.

Configuration File

Configure the OLT.

```
vlan 100 smart
port vlan 100 0/19 0
vlan 8 smart
port vlan 8 0/19 0
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-name VideoMonitoring type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name VideoMonitoring
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 100
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
display ont autofind 1
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU.

```
vlan 100 smart
port vlan 100 0/0 0
service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-cttr 6 tx-cttr 6
save
```

9.2 Configuration Example of Intelligently Collecting Power Consumption Information by Using the Ethernet Access

The ONU can intelligently collect power consumption information in the electrical power system through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

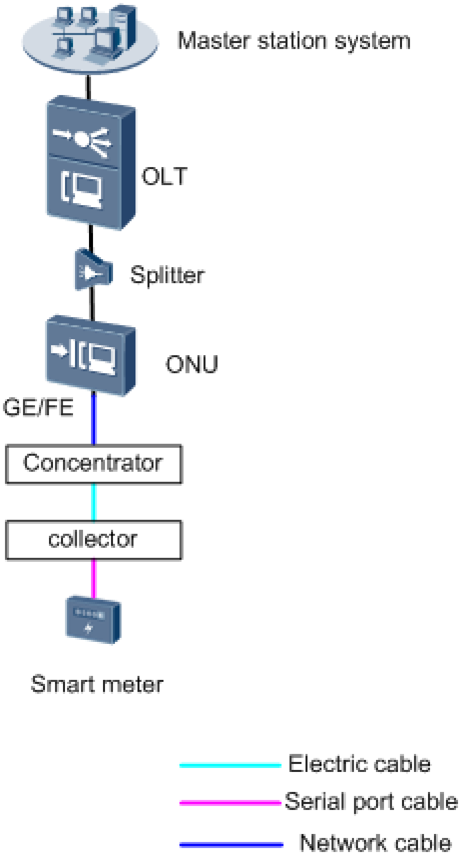
Service Requirements

- The ONU is connected to a concentrator through a GE/FE auto-adaptive electrical port. The concentrator is connected to a collector using power cables and sends the power consumption information collected by the collector to the ONU.
- The ONU forwards the power consumption information to an optical line terminal (OLT) and the OLT forwards the information to the upper-layer device. Then, the upper-layer device forwards the information to an automatic meter reading system (AMR) server.

Networking

Figure 9-2 shows the example network for configuring intelligent collection of power consumption information in the electrical power system over Ethernet.

Figure 9-2 Example network for configuring intelligent collection of power consumption information in the electrical power system over Ethernet



NOTE

This example uses the MA5621 as the ONU.

Data Plan

Table 9-3provides the data plan for the OLT, and **Table 9-4** provides the data plan for the ONU.

Table 9-3 Data plan for configuring intelligent collection of power consumption information in the electrical power system over Ethernet-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 100
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 0/3/1 ONU ID: 1 ONUauthentication mode: SN ONU SN: 48575443E6D8B541
DBA profile	Profile name: Data Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s
ONU line profile	Profile ID: 10, bound to the DBA profile named Data GEM port IDs: 0, 1 T-CONT ID: 5
ONU management mode	SNMP

Table 9-4 Data plan for configuring intelligent collection of power consumption information in the electrical power system over Ethernet-ONU side

Configuration Item	Data	Remarks
IP address	Inband management IP address: 192.168.50.2/24	
Traffic profile	Index 6 (default)	-
Service port	0/1/1	-
Uplink port	0/0/0	-

Configuration Item	Data	Remarks
Uplink VLAN	smart VLAN 100	The uplink VLAN must be the same as the user VLAN on the OLT.
User VLAN	untagged	-

Procedure

Step 1 **Configure the OLT.**

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

   Create smart VLAN 100, and then add upstream port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured. For details, see Configuring Upstream Link Aggregation.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

   a. Add a DBA profile.

      You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

      Configure the profile name to Data, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

      ```
      huawei(config)#dba-profile add profile-name Data type3 assure 20480 max
      51200
      ```

   b. Add an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named Data. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name Data
```

Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting data traffic streams. Bind GEM port 0 and GEM port 1 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

NOTE

1) To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the gem add command to configure the ID of the traffic profile bound to the GEM port.

2) When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of SVLAN 100 to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port ont-auto-find command in the GPON mode to enable the ONU auto-find

function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to
  //the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5621
   Ont SoftwareVersion : V800R309C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-03-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

----------------------------------------------------------------------
  F/S/P                :
0/3/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/3)#quit
```

   If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

   - If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.

- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4–7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
255.255.255.0 manage-vlan 8
```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** command to telnet to the ONU and then configure the ONU.
8. Create a service port.

   Configure the Data service port ID to 1, SVLAN ID to 100, GEM port ID to 1, CVLAN ID to 100. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 100 rx-cttr 6 tx-cttr 6
```

9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
   cos7 7
   ```

10. Save the data.

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

Step 2 Configure the ONU.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet *192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

   ```
   huawei(config)#telnet 192.168.50.2
   { <cr>|service-port<U><0,4294967295> }:

     Command:
             telnet 192.168.50.2
     Press CTRL_] to quit telnet mode
     Trying 192.168.50.2 ...
     Connected to 192.168.50.2 ...
   >>User name:root
   >>User password:       //It is not displayed on the console.
   ```

2. Create a VLAN.

   ```
   huawei(config)#vlan 100 smart
   ```

3. Add an uplink port to the VLAN.

   Add uplink port 0/0/0 to the VLAN.

   ```
   huawei(config)#port vlan 100 0/0 0
   ```

4. Create a service port.

Create service port 2. Its user VLAN ID is untagged and service VLAN ID is 100. Use the default traffic profile (traffic profile 6). To limit the traffic rate, run the **traffic table ip** command to configure the traffic profile.

```
huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan
untagged rx-cttr 5
tx-cttr 5
```

5. Save the data.

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

----End

Result

After the preceding configurations are complete, the power consumption information collected by the smart meter is transmitted to the AMR server.

Configuration File

Configure the OLT.

```
vlan 100 smart
port vlan 100 0/19 0
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-name Data type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name Data
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 100
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU.

```
vlan 100 smart
port vlan 100 0/0 0
service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan untagged rx-cttr 6 tx-
cttr 6
save
```

9.3 Configuration Example of Transmitting Power Distribution Site Information by Using the Ethernet Access

The ONU can automatically transmit power distribution site information in the electrical power system through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

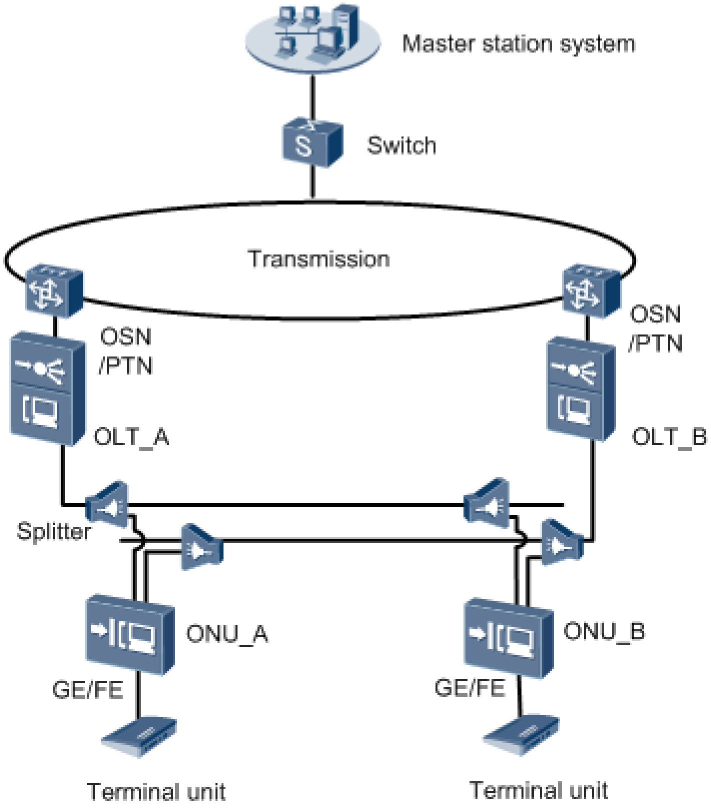
Service Requirements

- ONU_A and ONU_B are connected to the terminal units through GE/FE auto-adaptive electrical ports.
- After receiving a query from the master station server, the terminal unit transmits the message to ONU_A and ONU_B, ONU_A and ONU_B transmit the message to an optical line terminal (OLT) for forwarding. The message is sent to the master station server finally.
- To support the electrical goose function, ONU_A must communicate with ONU_B at Layer 2.
- The unknown multicast suppression function must be disabled so that goose packets are not lost.

Networking

Figure 9-3 shows the example network for configuring the automatic transmission of power distribution site information in the electrical power system over Ethernet.

Figure 9-3 Example network for configuring the automatic transmission of power distribution site information in the electrical power system over Ethernet



NOTE

This example uses the MA5621 as the ONU.

Data Plan

Table 9-5 provides the data plan for the OLT, and **Table 9-6** provides the data plan for the ONU.

Table 9-5 Data plan for configuring the automatic transmission of power distribution site information in the electrical power system over Ethernet-OLT side

Device	Item	Data
OLT_A	VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 200 (used for transmitting the site information about the electric system) SVLAN: smart VLAN 101 (used for transmitting goose packets)
	IP address	Inband management IP address: 192.168.50.1/24
	GPON service board	Port: 0/3/1 ONU ID: 1 ONU authentication mode: SN ONU SN: 48575443E6D8B541
	DBA profile	Profile name: Data Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s
	ONU line profile	Profile ID: 10, bound to the DBA profile named Data GEM port IDs: 0, 1, 2 T-CONT ID: 5
	ONU management mode	SNMP
	Priority	The 802.1p priority is used: The priority of the site information about the electric system is 1 and the priority of goose packets is 6.
OLT_B	The data plan is the same as that of OLT_A.	

Table 9-6 Data plan for configuring the automatic transmission of power distribution site information in the electrical power system over Ethernet-ONU side

Device	Configuration Item	Data	Remarks
ONU_A	IP address	Inband management IP address: 192.168.50.2/24	
	Traffic profile	● Index 10 (used for transmitting the power distribution site information) ● Index 11 (used for transmitting goose packets)	-
	Service port	0/1/1	-
	Uplink port	0/0/0, 0/0/1	-
	Uplink VLAN	● Smart VLAN 100 (used for transmitting power distribution site information) ● Smart VLAN 101 (used for transmitting goose packets)	The uplink VLAN must be the same as the user VLAN on the OLT.
	Priority	The 802.1p priority is used: The priority of power distribution site information is 1 and the priority of goose packets is 6.	-
	User VLAN	Untagged (used for transmitting power distribution site information) Smart VLAN 2 (used for transmitting goose packets)	-
ONU_B	The data plan is the same as that of ONU_A except for the ID of the uplink VLAN used for transmitting power distribution site information and IP address.		

Procedure

Step 1 **Configure the OLT.**

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

   Create smart VLAN 101 and VLAN 200, and then add upstream port 0/19/0 to these VLANs.

   ```
   huawei(config)#vlan 101,200 smart
   huawei(config)#port vlan 101,200 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured. For details, see Configuring Upstream Link Aggregation.

3. Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

a. Add a DBA profile.

You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

Configure the profile name to Data, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

```
huawei(config)#dba-profile add profile-name Data type3 assure 20480 max
51200
```

b. Add an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named Data. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name Data
```

Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting the electric system site information traffic streams and GEM port 2 for transmitting goose packets traffic streams. Bind GEM port 0, GEM port 1 and GEM port 2 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

NOTE

1) To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the gem add command to configure the ID of the traffic profile bound to the GEM port.
2) When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 2 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of the site information SVLAN 200 to GEM port 1 and map the service port of the goose packets SVLAN 101 to GEM port 2.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 200
huawei(config-gpon-lineprofile-10)#gem mapping 2 2 vlan 101
```

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port ont-auto-find command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to
  //the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number             : 1
   F/S/P              : 0/3/1
   Ont SN             : 48575443E6D8B541
   Password           :
   VenderID           : HWTC
   Ont Version        : MA5621
   Ont SoftwareVersion : V800R309C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-03-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

---------------------------------------------------------------------
  F/S/P                :
0/3/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
...//The rest of the response information is omitted.
```

   If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

   - If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
   - If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
   - If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

     NOTE

     If an ONT supports only four queues, the values of 4–7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

```
huawei(config-if-gpon-0/3)#quit
huawei(config)#vlan 8 smart
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

b. Configure the inband management VLAN and IP address of the ONU.

Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
255.255.255.0 manage-vlan 8
```

c. Configure an inband management service port.

Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping** ***192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet** ***192.168.50.2*** command to telnet to the ONU and then configure the ONU.
8. Create a service port.

Configure the site information service port ID to 1, SVLAN ID to 200, GEM port ID to 1, CVLAN ID to 100 and configure the goose packets service port ID to 2, SVLAN ID to 101, GEM port ID to 2, CVLAN ID to 101. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT.

The same port is used for transmitting the site information about the electric system and goose packets. Therefore, the 802.1p priority of each service needs to be set. The priority of the site information about the electric system is lower than that of goose packets. Set the traffic profile index of the site information about the electric system to 20 and the priority to 1; set the traffic profile index of goose packets to 21 and the priority to 6.

The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#traffic table ip index 20 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index            :
20
  TD Name             : ip-traffic-
table_20
  Priority            :
```

```
1
  Copy Priority       :
-
  Mapping Index       :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                 :
off
  CBS                 :
off
  PIR                 :
off
  PBS                 :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#traffic table ip index 21 cir off priority 6 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index            :
21
  TD Name              : ip-traffic-
table_21
  Priority            :
6
  Copy Priority       :
-
  Mapping Index       :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                 :
off
  CBS                 :
off
  PIR                 :
off
  PBS                 :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#service-port 1 vlan 200 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 100 rx-cttr 20 tx-cttr 20
huawei(config)#service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-
service
user-vlan 101 rx-cttr 21 tx-cttr 21
```

9. Disable the unknown multicast suppression function.

   Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the OLT to ensure that goose packets are not lost.

```
huawei(config)#vlan service-profile profile-id 20
huawei(config-vlan-srvprof-20)#packet-policy multicast forward
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-20)#commit
```

10. Enable the bridging function.

    To support the electrical goose function, ONU_A must communicate with ONU_B at Layer 2.

```
huawei(config-vlan-srvprof-20)#user-bridging
enable
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-20)#commit
huawei(config-vlan-srvprof-20)#quit
```

11. Bind the VLAN service profile to the uplink VLAN.

```
huawei(config)#display vlan service-profile profile-id 20


Command:
          display vlan service-profile profile-id
20

  Profile   ID:
20
  Profile Name:
srvprof-20

---------------------------------------------------------------------
  Parameter                        Committed          Not
Committed

---------------------------------------------------------------------
  Forwarding mode                  NotConfig
-
  Anti-macspoofing                 NotConfig
-
  Anti-ipspoofing                  enable
-
  PPPoE MAC mode                   NotConfig
-
  BPDU tunnel                      NotConfig
-
  RIP tunnel                       NotConfig
-
  VTP-CDP tunnel                   NotConfig
-
  DHCP mode                        n/a
-
  DHCP proxy                       enable
-
  DHCP option82                    enable
-
  PITP                             enable
-
  Broadcast packet policy          NotConfig
-
  Multicast packet policy          forward
-
  Unknown unicast packet policy    NotConfig
-
  User-bridging                    enable
-
  VMAC                             NotConfig
-
```

```
  Mismatch IGMP packet policy      discard
-
  VMAC aging mode                  MAC-learning
-
  OSPF tunnel                      enable
-
  Layer-3 protocol tunnel          enable
-
  Mac-address learning fabric      enable
-

---------------------------------------------------------------------
  Binding VLAN list           :
0
  ---------------------------------------------------------------------
huawei(config)#vlan bind service-profile 101 profile-id 20
```

12. Configure queue scheduling.

    The goose service traffic is forwarded in PQ mode.

    Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

    ```
    huawei(config)#queue-scheduler strict-priority
    ```

    Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

    For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

    ```
    huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
    cos7 7
    ```

13. Save the data.

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

Step 2 The following shows the procedure for configuring the automatic transmission of site information about the electric system over Ethernet on ONU_A.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet *192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

   ```
   huawei(config)#telnet 192.168.50.2
   { <cr>|service-port<U><0,4294967295> }:

     Command:
             telnet 192.168.50.2
     Press CTRL_] to quit telnet mode
     Trying 192.168.50.2 ...
     Connected to 192.168.50.2 ...
   >>User name:root
   >>User password:       //It is not displayed on the console.
   ```

2. Configure a traffic profile.

   The same port is used for transmitting power distribution site information and goose packets. Therefore, the 802.1p priority of each service needs to be set. The priority of power distribution site information is lower than that of goose packets. Set the traffic profile index of power distribution site information to 10 and the priority to 1; set the traffic profile index of goose packets to 11 and the priority to 6.

```
huawei(config)#traffic table ip index 10 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index            :
10
  TD Name             : ip-traffic-
table_10
  Priority            :
1
  Copy Priority       :
-
  CTAG Mapping Priority:
-
  CTAG Default Priority:
0
  Priority Policy     : local-
pri
  CIR                 :
off
  CBS                 :
off
  PIR                 :
off
  PBS                 :
off
  Color Mode          : color-
blind
  Referenced Status   : not
used
  ------------------------------------------------
huawei(config)#traffic table ip index 11 cir off priority 6 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index            :
11
  TD Name             : ip-traffic-
table_11
  Priority            :
6
  Copy Priority       :
-
  CTAG Mapping Priority:
-
  CTAG Default Priority:
0
  Priority Policy     : local-
pri
  CIR                 :
off
  CBS                 :
off
  PIR                 :
off
  PBS                 :
off
  Color Mode          : color-
blind
  Referenced Status   : not
```

```
used
  ------------------------------------------------
```

3. Create a VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan 101 smart
```

4. Add an uplink port to the VLAN.

   Add uplink port 0/0/0 and 0/0/1 to the VLAN.

```
huawei(config)#port vlan 100 0/0 0-1
huawei(config)#port vlan 101 0/0 0-1
```

5. Create a service port.

   For power distribution site information, create service port 2 with service VLAN 100 and traffic profile 10. For goose packets, create service port 3 with service VLAN 101 and traffic profile 11.

```
huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan
untagged
 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 3 vlan 101 eth 0/1/1 multi-service user-vlan 2 rx-
cttr 11 tx-cttr 11
```

6. Disable the unknown multicast suppression function.

   Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the ONU to ensure that goose packets are not lost.

```
huawei(config)#vlan service-profile profile-id 10
huawei(config-vlan-srvprof-10)#packet-policy multicast forward
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-10)#commit
```

7. Enable the bridging function.

```
huawei(config-vlan-srvprof-10)#user-bridging
enable
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-10)#commit
huawei(config-vlan-srvprof-10)#quit
```

8. Bind the VLAN service profile to the uplink VLAN.

```
huawei(config)#display vlan service-profile profile-id 10


Command:
          display vlan service-profile profile-id
10

  Profile   ID:
10
  Profile Name:
srvprof-10

---------------------------------------------------------------------
  Parameter                         Committed          Not
Committed

---------------------------------------------------------------------
  Forwarding mode                   VLAN-MAC
-
  BPDU tunnel                       disable
-
  RIP tunnel                        disable
```

```
-
  VTP-CDP tunnel                   disable
-
  Multicast packet policy          forward
-
  User-bridging                    enable
-
  OSPF tunnel                      enable
-

---------------------------------------------------------------------
  Binding VLAN list           :
0
  ---------------------------------------------------------------------
huawei(config)#vlan bind service-profile 101 profile-id 10
```

9. Set the queue scheduling mode to strict priority queue (PQ).

   The goose service traffic is forwarded in PQ mode.

```
huawei(config)#queue-scheduler strict-priority
```

10. Save the data.

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

Step 3 The following describes the procedure for configuring the automatic transmission of site information about the electric system over Ethernet on ONU_B.

The procedure is the same as that on ONU_A except for the ID of the uplink VLAN used for transmitting power distribution site information and IP address.

----End

Result

After the master station server queries the power distribution site information, the power distribution site information is transmitted to the master station server.

Configuration File

Configure the OLT.

```
vlan 101,200 smart
port vlan 101,200 0/19 0
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-name Data type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name Data
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
gem add 2 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 200
gem mapping 2 2 vlan 101
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
```

```
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
traffic table ip index 20 cir off priority 1 priority-policy local-Setting
traffic table ip index 21 cir off priority 6 priority-policy local-Setting
sservice-port 1 vlan 200 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 20 tx-cttr 20
service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-service
user-vlan 101 rx-cttr 21 tx-cttr 21
vlan service-profile profile-id 20
packet-policy multicast forward
user-bridging enable
commit
quit
vlan bind service-profile 101 profile-id 20
queue-scheduler strict-priority
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU.

```
traffic table ip index 10 cir off priority 1 priority-policy local-Setting
traffic table ip index 11 cir off priority 6 priority-policy local-Setting
vlan 100 smart
vlan 101 smart
port vlan 100 0/0 0-1
port vlan 101 0/0 0-1
service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan untagged rx-cttr 10 tx-
cttr 10
service-port 3 vlan 101 eth 0/1/1 multi-service user-vlan 2 rx-cttr 11 tx-cttr 11
vlan service-profile profile-id 10
packet-policy multicast forward
user-bridging enable
commit
quit
vlan bind service-profile 101 profile-id 10
squeue-scheduler strict-priority
save
```

9.4 Configuration Example of Automatically Transmitting Power Distribution Site Information in the Electrical Power System over a Serial Port

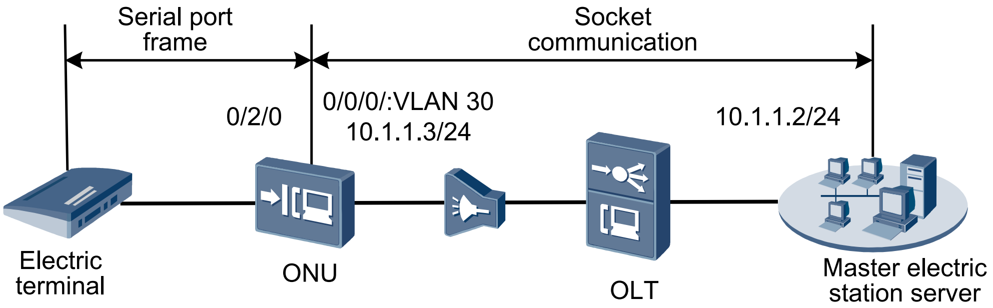
The serial port access service carries the serial port data using the TCP/IP protocol stack. This service, when coupled with the intelligent power distribution solution of the electrical power network, achieves intelligent power distribution and centralized metering.

Service Requirements

- The ONU uses its serial port to transparently transmit the site information collected by a terminal unit to the master station server.
- The ONU obtains the serial port data through a serial port identified by port ID, encapsulates the serial port data into User Datagram Protocol (UDP)/TCP packets, and transmits the packets upstream to a master station server over the IP network through a GPON port. After receiving the UDP/TCP packets sent downstream from the master station server, the ONU restores the UDP/TCP packets to the serial port data flow and transmits the data flow to terminal units.

Networking

Figure 9-4 Network diagram for configuring automatic transmission of site information in electrical power system over a serial port



NOTE

This example uses the MA5621 as the ONU.

Data Plan

Table 9-7 provides the data plan for the OLT, and Table 9-8 provides the data plan for the ONU.

Table 9-7 Data plan for configuring the automatic transmission over a serial port-OLT side

Configuration Item	Data
VLAN	Inband management VLAN: smart VLAN 8 Service VLAN ID: 30, of the smart type, for transmitting power distribution site information
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 0/3/1 ONU ID: 1 ONU authentication mode: SN ONU SN: 48575443E6D8B541
DBA profile	Profile name: SerialAccess Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s

Configuration Item	Data
ONU line profile	Profile ID: 10, bound to the DBA profile named SerialAccess GEM port IDs: 0 T-CONT ID: 5
ONU management mode	SNMP

Table 9-8 Data plan for configuring the automatic transmission over a serial port-ONU side

Configuration Item	Data	Remarks
Attributes of the inband management interface	● Uplink port: 0/0/0 ● VLAN: 8 ● Inband management IP address: 192.168.50.2/24 ● Traffic profile: Index 6 (default)	-
Attributes of the VLAN Layer 3 interface	● Uplink port: 0/0/0 ● VLAN ID: 30 ● IP address of the VLAN Layer 3 interface: 10.1.1.3	The IP address of the master station server is 10.1.1.2.
Attributes of the serial port	● Serial port: 0/2/0 ● Working mode: RS-232 ● Baud rate: 9600	Default value of the baud rate: 9600 Serial port attributes need to be the same as those on the interconnected terminal unit.

Configuration Item	Data	Remarks
Connections of the serial port	● Connection ID: 1 ● Working mode: tcp-server ● Local port ID: 3000 ● Remote port ID: 3000 ● Serial port frame type: ft1.2	If a remote port ID is not specified on the ONU, the system obtains the port ID based on the connection packets received on the serial port from the remote port. **NOTE** When specifying a remote port ID on the ONU, ensure that it is the same as the ID of the source port sending connections packets.

Procedure

Step 1 Configure the OLT.

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

   Create smart VLAN 30, and then add upstream port 0/19/0 to the VLAN.

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

2. (Optional) Configure upstream link aggregation.

   In this example, a single upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured. For details, see Configuring Upstream Link Aggregation.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

a. Add a DBA profile.

You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

Configure the profile name to SerialAccess, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

```
huawei(config)#dba-profile add profile-name SerialAccess type3 assure
20480 max 51200
```

b. Add an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named SerialAccess. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name SerialAccess
```

Add GEM port 0 for transmitting management traffic streams. Bind GEM port 0 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

NOTE

1) To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the gem add command to configure the ID of the traffic profile bound to the GEM port.
2) When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0.

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

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

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

(Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port ont-auto-find command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to
  //the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number             : 1
   F/S/P              : 0/3/1
   Ont SN             : 48575443E6D8B541
   Password           :
   VenderID           : HWTC
   Ont Version        : MA5621
   Ont SoftwareVersion : V800R309C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-03-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

---------------------------------------------------------------------
  F/S/P               :
0/3/1
  ONT-ID              :
1
  Control flag        : active    //Indicates that the ONU is
activated.
  Run state          : online    //Indicates that the ONU already goes online
normally.
  Config state        : normal    //Indicates that the configuration status
of the ONU is normal.
```

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

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4–7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.1/24.

      ```
      huawei(config-if-gpon-0/3)#quit
      huawei(config)#vlan 8 smart
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.1 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

      ```
      huawei(config)#interface gpon 0/3
      huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
      255.255.255.0 manage-vlan 8
      ```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

      ```
      huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
      service user-vlan 8 rx-cttr 6 tx-cttr 6
      ```

7. Confirm that the management channel between the OLT and the ONU is available.

   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.

- You can run the **telnet *192.168.50.2*** command to telnet to the ONU and then configure the ONU.

8. Create a service port.

   The ID of the service flow for the power distribution site information is 1, service VLAN ID is 30, and user-side VLAN ID is 30. In addition, the traffic of upstream and downstream packets is not limited.

   The user-side VLAN is the same as the Layer 3 interface VLAN of the ONU.

```
huawei(config)#traffic table ip index 20 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index             :
20
  TD Name              : ip-traffic-
table_20
  Priority             :
1
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#service-port 1 vlan 30 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 30 rx-cttr 20 tx-cttr 20
```

9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

```
huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
cos7 7
```

10. Save the data.

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

Step 2 Configure the ONU.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet** ***192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

```
huawei(config)#telnet 192.168.50.2
{ <cr>|service-port<U><0,4294967295> }:

  Command:
          telnet 192.168.50.2
  Press CTRL_] to quit telnet mode
  Trying 192.168.50.2 ...
  Connected to 192.168.50.2 ...
>>User name:root
>>User password:       //It is not displayed on the console.
```

2. Configure the VLAN Layer 3 interface.

```
huawei(config)#vlan 30 standard
huawei(config)#port vlan 30 0/0 0
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.1.1.3 24
huawei(config-if-vlanif30)#quit
```

3. Configure the serial port working mode.

```
huawei(config)#interface serial 0/2
huawei(config-if-serial-0/2)#port mode 0 rs232
```

4. (Optional) Configure serial port attributes.

```
huawei(config)#interface serial 0/2
huawei(config-if-serial-0/2)#port config 0 baudrate 9600
```

5. Configure a serial port connection.

```
huawei(config)#serialop-connection 1 port 0/2/0 working-mode tcp-server local-
address
 10.1.1.3 local-port 3000 peer-address 10.10.1.3 frame-type ft1.2
```

6. Save the data.

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

----End

Result

1. Run the **ping** command to verify that the route between the ONU and the master station server is reachable.
2. Run the **display serialop-connection** command to verify that the status of the serial port TCP/IP connection is **established**. **established** indicates that the ONU and the terminal unit communicate with each other normally.

NOTE

If **working-mode** of the serial port connection is **TCP-Client**, run the **display serialop-connection** command to verify that the status of the serial port TCP/IP connection is **connected**. **connected** indicates that the ONU and the terminal unit communicate with each other normally.

If **working-mode** of the serial port connection is **UDP**, run the **display serialop-connection statistics** command to query the number of frames received on or sent from the serial port so as to determine whether the communication between the MA5621 and the terminal unit is proper.

Configuration File

Configure the OLT.

```
vlan 30 smart
port vlan 30 0/19 0
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-name SerialAccess type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name SerialAccess
gem add 0 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
traffic table ip index 20 cir off priority 1 priority-policy local-Setting
service-port 1 vlan 30 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 30 rx-cttr 20 tx-cttr 20
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU.

```
vlan 30 standard
port vlan 30 0/0 0
interface vlanif 30
ip address 10.1.1.3 24
quit
interface serial 0/2
port mode 0 rs232
interface serial 0/2
port config 0 baudrate 9600
serialop-connection 1 port 0/2/0 working-mode tcp-server local-address
 10.1.1.3 local-port 3000 peer-address 10.10.1.3 frame-type ft1.2
save
```

A Acronyms and Abbreviations

A	
AG	Access Gateway
ATM	Asynchronous Transfer Mode
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
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
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
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