AN6001-G16

Optical Line Terminal Equipment

UNM2000 Configuration Guide

Version: A

Code: MN000003552

FiberHome Telecommunication Technologies Co., Ltd.

December 2018

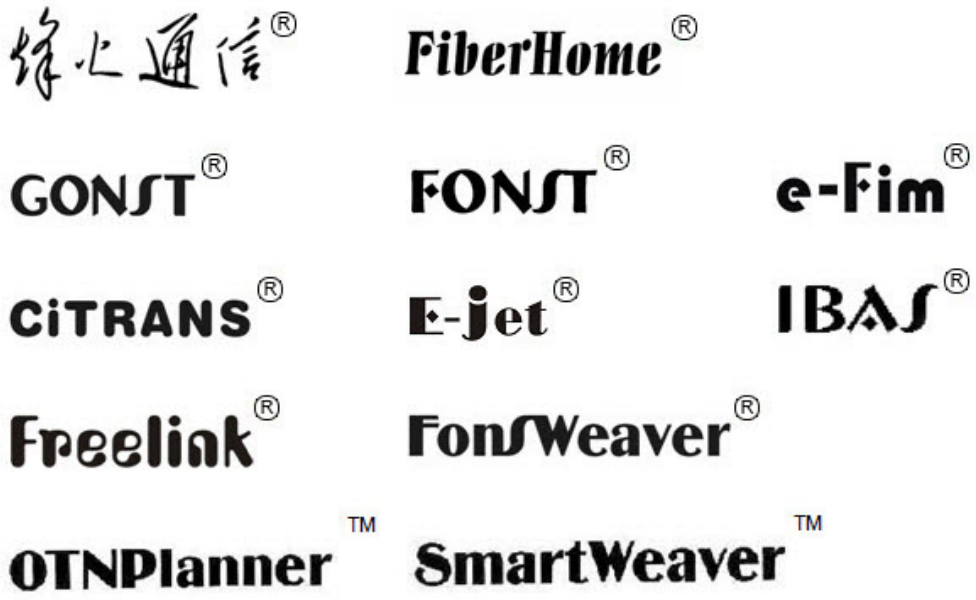
Thank you for choosing our products.

We appreciate your business. Your satisfaction is our goal. We will provide you with comprehensive technical support and after-sales service. Please contact your local sales representative, service representative or distributor for any help needed at the contact information shown below.

Fiberhome Telecommunication Technologies Co., Ltd.

Address: No. 67, Guanggu Chuangye Jie, Wuhan, Hubei, China
Zip code: 430073
Tel: +6 03 7960 0860/0884 (for Malaysia)
+91 98 9985 5448 (for South Asia)
+593 4 501 4529 (for South America)
Fax: +86 27 8717 8521
Website: http://www.fiberhomegroup.com

Legal Notice



are trademarks of FiberHome Telecommunication Technologies Co., Ltd. (Hereinafter referred to as FiberHome)

All brand names and product names used in this document are used for identification purposes only and are trademarks or registered trademarks of their respective holders.

All rights reserved

No part of this document (including the electronic version) may be reproduced or transmitted in any form or by any means without prior written permission from FiberHome.

Information in this document is subject to change without notice.

Operation Safety Rules

The network management computer should be placed away from direct sunlight, electromagnetic interference, heat source, humidity and dust, and with at least 8 cm distance from other objects in order to keep good ventilation.

Use UPS power supply to avoid loss of network management data caused by accidental power failure.

The computer case, UPS power supply and switch (or hub) should be connected to protection earth ground.

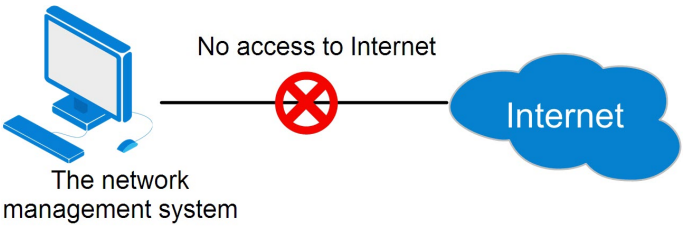
To shut down the network management computer, first exit the operation system normally and then shut off the power supply.

Do not exit the network management system when it is working normally. Exiting the network management system does not interrupt traffic in the network, but precludes centralized control of the networked equipment.

The network management system requires a dedicated computer. Use of unidentified memory devices should be prohibited so as to avoid computer viruses.

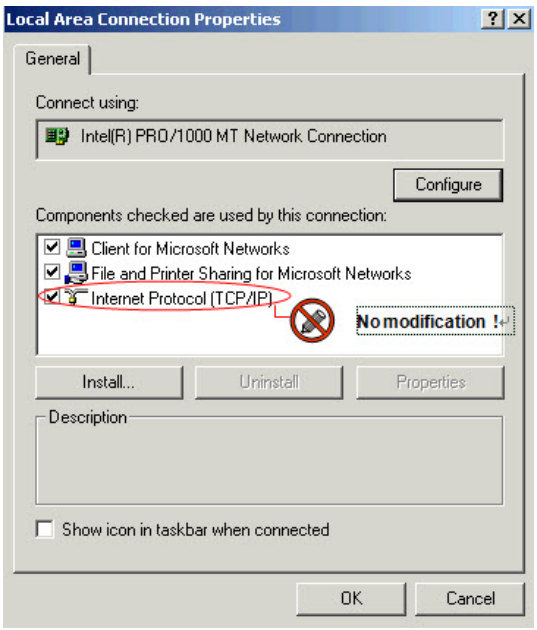
Do not delete any file in the network management system randomly or copy any irrelevant file into the network management computer.

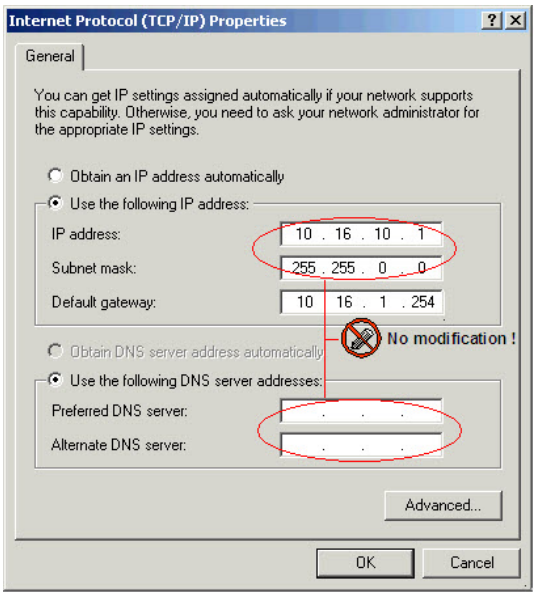
Do not visit Internet via the network management computer. Doing so may increase data flow in the net card and hence affects normal network management data transmission or results in other accidents.

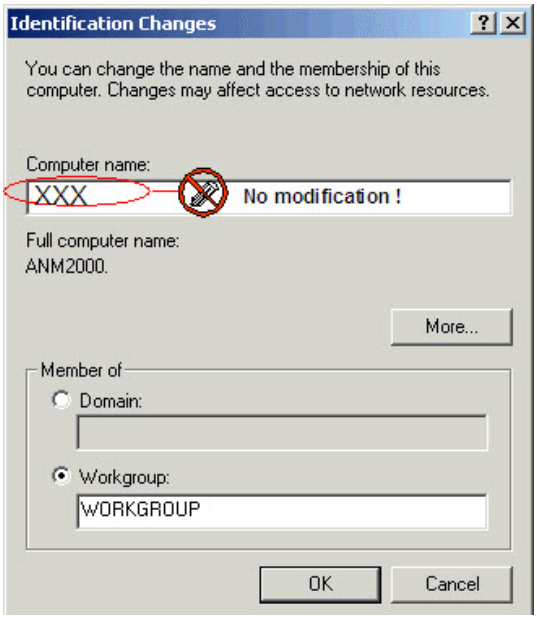


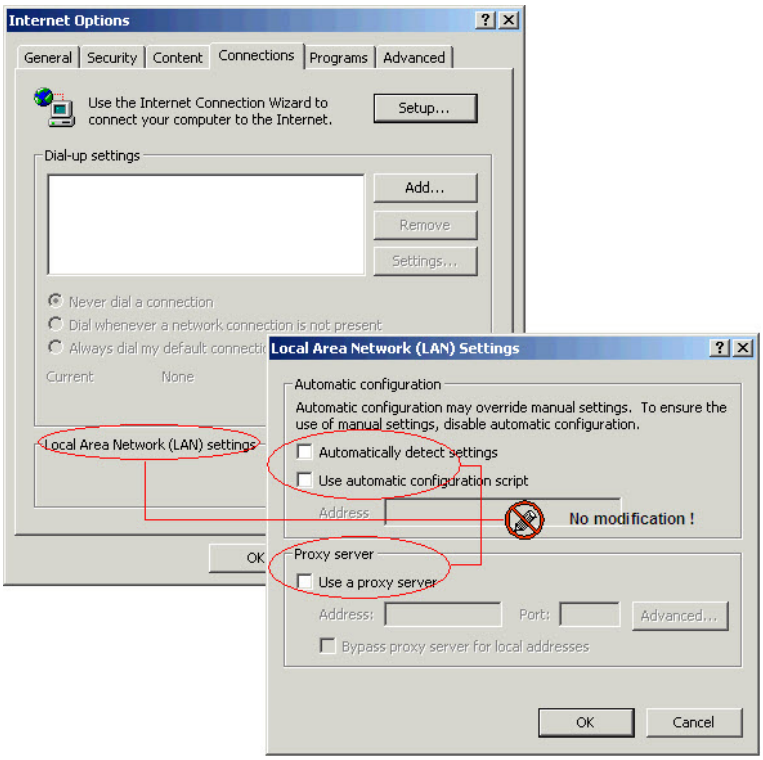
Do not perform service configuration or expansion during service busy hours via the network management system.

Do not modify the network management computer's protocol settings, computer name or LAN settings. Doing so may result in abnormal operation of network management system.




Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 16 . 10 . 1
Subnet mask: 255 . 255 . 0 . 0
Default gateway: 10 . 16 . 1 . 254
No modification !
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel


Identification Changes
You can change the name and the membership of this computer. Changes may affect access to network resources.
Computer name:
XXX
No modification !
Full computer name:
ANM2000.
More...
Member of
Domain:
Workgroup:
WORKGROUP
OK
Cancel


Internet Options
General
Security
Content
Connections
Programs
Advanced
Use the Internet Connection Wizard to connect your computer to the Internet.
Setup...
Dial-up settings
Add...
Remove
Settings...
Never dial a connection
Dial whenever a network connection is not present
Always dial my default connecti
Current
None
Local Area Network (LAN) settings
OK
Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
No modification !
Proxy server
Use a proxy server
Address:
Port:
Advanced...
Bypass proxy server for local addresses
OK
Cancel

Contents

Operation Safety Rules I

1 Documentation Guide 1

2 Configuring the UNM2000 Management Channel 3

2.1 Logging into the Console 4

2.1.1 First-time Login to the Console 4

2.1.2 Subsequent Login to the Console 8

2.2 Configuring the UNM2000 Management Channel 9

2.2.1 Network Scenario 9

2.2.2 Planning Data 10

2.2.3 Configuration Flow 11

2.2.4 Adding VLAN to an Uplink Port 12

2.2.5 Deleting VLAN from an Uplink Port 12

2.2.6 Adding VLAN to Slots / Ports 13

2.2.7 Configuring the Management Information 13

2.2.8 Configuring Static Routing 14

2.2.9 Configuration Result 14

2.3 Logging into the UNM2000 15

3 Adding Equipment 16

3.1 Configuration Flow 17

3.2 Creating the Logical Domain 17

3.3 Creating the Access NE 19

3.4 Adding Cards 20

3.4.1 Configuring Subracks and Cards 21

3.4.2 Adding Cards Automatically 21

3.4.3 Adding Cards Manually 22

3.5 Configuring the SNMP Trap Receiver Address 24

3.6 Synchronizing Time 26

3.7 Saving Current Configuration to the FLASH 27

4 Authenticating and Authorizing an ONU 28

4.1 Authenticating and Authorizing an ONU 29
4.1.1 Configuring the PON Port Authentication Mode 29
4.1.2 Configuring the White List - Manual Authorization 30
4.1.3 Configuring the White List - Automatic Authorization 31
4.2 Modifying the Authentication Mode and Re-authorizing an ONU 32
4.2.1 Deleting an ONU from the Physical Identifier White List - Optional 33
4.2.2 Reconfiguring the Authorized ONUs in the White List 33
4.2.3 Switching the PON Port Authentication Mode 34
5 Basic Configurations 36
5.1 Configuring Local End Outer VLAN Data 37
5.2 Adding Ports to the VLAN 38
5.3 Disabling Suppression of Multicast Packets at the Uplink Port 40
6 Configuring Voice Services 42
6.1 Example of Configuring Voice Service 43
6.1.1 Network Scenario 43
6.1.2 Configuration Flow 44
6.1.3 Configuring the NGN Uplink Interface 44
6.1.4 Configuring the NGN Uplink Subscriber Data 48
6.1.5 Configuring the Voice Service at the ONU Port 51
6.1.6 Configuration Result 53
6.2 Optional Functions 53
6.2.1 Configuring the Softswitch Intercommunication Profile Parameters 53
6.2.2 Configuring NGN Heartbeat Parameters 57
6.2.3 Configuring IAD MD5 Authentication 59
6.2.4 Configuring the Digitmap 60
7 Configuring Data Services 62
7.1 Example of Data Service Configuration in the Transparent / TAG Mode 63
7.1.1 Network Scenario 63
7.1.2 Configuration Flow 63
7.1.3 Configuring Parameters of Data Services at the ONU Ports 64

7.1.4 Configuration Result 67
7.2 Example of Data Service Configuration in the VLAN Translation Mode 68
7.2.1 Network Scenario 68
7.2.2 Configuration Flow 69
7.2.3 Configuring Parameters of Data Services at the ONU Ports 70
7.2.4 Configuration Result 72
7.3 Example of Data Service Configuration in the Selective QinQ Mode 73
7.3.1 Network Scenario 73
7.3.2 Configuration Flow 74
7.3.3 Configuring the OLT QinQ Domain 74
7.3.4 Binding the QinQ Domain to the ONU 76
7.3.5 Configuration Result 77
8 Configuring the Multicast Service 78
8.1 Multicast Service Configuration Example 79
8.1.1 Configuration Rules 79
8.1.2 Network Scenario 79
8.1.3 Configuration Flow 80
8.1.4 Configuring the Multicast Mode 81
8.1.5 Configuring the Multicast VLAN 82
8.1.6 Configuring the Port Service VLAN 83
8.1.7 Configuration Result 85
8.2 Example of Configuring the SSM Service 86
8.2.1 Network Diagram 86
8.2.2 Configuration Flow 87
8.2.3 Configuring the Multicast Protocol Version 88
8.2.4 Configuring the Multicast Mode 88
8.2.5 Configuring the Multicast VLAN 89
8.2.6 Configuring the SSM IP Address Range 90
8.2.7 Configuring the Source IP Address for SSM-Mapping 91
8.2.8 Configuring ONU Multicast Service Parameters 92
8.2.9 Configuration Result 94
8.3 Optional Functions 94
8.3.1 Configuring the Multicast Cascade Port 95

8.3.2 Configuring Maximum Multicast Bandwidth of Uplink Ports 95
8.3.3 Configuring ONU Multicast Parameters 96
8.3.4 Configuring the Prejoin Group 98
8.3.5 Configuring the Multicast Program 98

9 Configuring the Wi-Fi Service 102

9.1 Network Scenario 103

9.2 Wi-Fi Service Configuration Example 103

9.2.1 Configuration Flow 104
9.2.2 Configuring the WAN Connection Service at the TL1 Interface 104
9.2.3 Configuring the Wi-Fi Service 106
9.2.4 Configuration Result 108

10 Configuring the CATV Service 109

10.1 Network Scenario 110

10.2 CATV Service Configuration Example 110

10.2.1 Configuration Flow 110
10.2.2 Starting up the CATV Service 111
10.2.3 Configuration Result 112

11 Configuring Layer 3 Functions 113

11.1 Configuring the ARP Proxy 114

11.1.1 Configuration Rules 114
11.1.2 Example of Configuring ARP Proxy in the Same-VLAN and Same-network Segment Application 114

11.2 Configuring the OSPF Routing Protocol 120

11.2.1 Example of Configuring the OSPF Routing Protocol 120

11.3 Configuring the DHCP Function 129

11.3.1 Configuration Rules 129
11.3.2 Network Scenario 130
11.3.3 Configuration Flow 132
11.3.4 Binding the Super VLAN with the Sub VLANs 132
11.3.5 Configuring the VLAN IP Address 133
11.3.6 Configuring the DHCP Global Switch 133
11.3.7 Configuring the DHCP Interface Mode 134

11.3.8 Configuring the DHCP Server 134
11.3.9 Configuring the DHCP Relay 137
11.3.10 Configuring DHCP Snooping 139

12 Configuring Network Protection 142

12.1 Configuring the MSTP Service 143

12.1.1 Network Scenario 143
12.1.2 Configuration Flow 144
12.1.3 Configuring Basic Properties of the Bridge 145
12.1.4 Configuring Bridge Parameters 146
12.1.5 Configuring Bridge Priority 148
12.1.6 Configuring Port Parameters 149
12.1.7 Configuring the MST Region 150
12.1.8 Configuring Basic Properties of the Instance 151
12.1.9 Configuring the Port Associated with the Instance 152
12.1.10 Configuring Parameters of the Bridge Instance 153
12.1.11 Configuring Instance Tree Parameters for the Port 154
12.1.12 Configuration Result 155

12.2 Configuring the LACP 155

12.2.1 Background Knowledge 155
12.2.2 Example of Configuring the LACP 156

12.3 Configuring the ERPS 162

12.3.1 Background Knowledge 162
12.3.2 Configuration Rules 164
12.3.3 Configuring Single-Ring Single-Instance Protection 164
12.3.4 Configuring Single-Ring Multi-Instance Protection 173
12.3.5 Configuring Tangent Ring Protection 188

13 Configuring Traffic Classification 203

13.1 Configuration Example for Traffic Classification Based on the L4 Source Port 204

13.1.1 Configuration Flow 204
13.1.2 Configuring the Traffic Classification Rules 204
13.1.3 Configuring the Traffic Policy 206
13.1.4 Binding the Traffic Policy to an Uplink Port 207
13.1.5 Configuration Result 208

13.2 Configuration Example for Traffic Classification Based on the SVLAN 208
13.2.1 Configuration Flow 208
13.2.2 Configuring the Traffic Classification Rules 209
13.2.3 Configuring the Traffic Policy 210
13.2.4 Binding the Traffic Policy to an ONU Port 211
13.2.5 Configuration Result 212
14 Configuring Subscriber Line Identifiers 213
14.1 Background Knowledge 214
14.2 Configuration Rules 214
14.3 Example of Configuring Subscriber Line Identifiers 216
14.3.1 Configuration Flow 216
14.3.2 Configuring the Line Identifier Switch 216
14.3.3 Configuring the Line Identifier Format 218
14.3.4 Configuration Result 219
15 Configuring TACACS+ 220
15.1 Background Knowledge 221
15.2 Example of Configuring Tacacs+ 221
15.2.1 Configuration Flow 221
15.2.2 Configuring Information about the Tacacs+ Server 222
15.2.3 Configuring the Authentication Mode 223
15.2.4 Configuring the Authorization Mode 224
15.2.5 Configuring the Accounting Mode 225
15.2.6 Configuration Result 226
16 Configuring RADIUS 227
16.1 Background Knowledge 228
16.2 Example of Configuring RADIUS 229
16.2.1 Configuration Flow 229
16.2.2 Configuring the RADIUS Authentication Mode 230
16.2.3 Configuring the RADIUS Authentication Information 230
16.2.4 Configuration Result 231
17 Configuring Power Supply and Environment Monitoring 232
17.1 Configuring Environment Monitoring 233

17.1.1 Alarm List 233
17.1.2 Configuration Flow 235
17.1.3 Configuring the Threshold Profile 235
17.1.4 Binding the Threshold Profile 238
17.1.5 Configuration Result 239
17.2 Configuring the Discharge Test 239
17.2.1 Configuration Flow 239
17.2.2 Configuring the Discharge Test Parameters 240
17.2.3 Controlling the Discharge Test 241
17.2.4 Viewing the Current Alarms of the HCU Card 242
17.2.5 Configuration Result 243
17.3 Configuring Environment Monitoring Parameters 243
17.4 Configuring the Charging Mode 245
17.5 Enabling the Rectifier Module 246
17.6 Checking the Power Supply Status 247
17.7 Viewing the Current Performance of the HCU Card 248
17.8 Viewing the Current Alarms of the HCU Card 248
17.9 Viewing the Alarm History of the HCU Card 249
18 Detecting the Optical Power 251
18.1 Viewing Optical Module Parameter Information of a GPON Interface Card 252
18.2 Viewing Optical Module Parameter Information of a PON ONU 252
19 FTP Operation Guide 254
19.1 Function Overview 255
19.2 Procedure 255

1 Documentation Guide

Document Orientation

Based on the graphic interface network management system UNM2000, *UNM2000 Configuration Guide* introduces how to configure the services and functions available for the AN6001-G16.

This manual is applicable to the service configuration for the AN6001-G16. To help users better understand and implement service configurations, we provide basic configuration rules, network planning, operation procedures on the network management system, and typical service examples in this manual. The practical network management GUIs and configuration parameters may be different from the ones described here due to different versions of network management system and different network requirements.

Intended Readers

- Commissioning engineers
- Operation and maintenance engineers

Version Information

Version	Description
A	Initial version, corresponding to the equipment version V1R1.

Content

Chapter	Summary
Configuring Equipment Management	◆ Configuring the UNM2000 Management Channel ◆ Adding Equipment ◆ Authenticating and Authorizing an ONU
Configuring Major Services	◆ Basic Configurations ◆ Configuring Voice Services ◆ Configuring Data Services ◆ Configuring the Multicast Service ◆ Configuring the Wi-Fi Service ◆ Configuring the CATV Service

Chapter	Summary
Configuring Layer 3 Functions	◆ Configuring the ARP Proxy ◆ Configuring the OSPF Routing Protocol ◆ Configuring the DHCP Function
Configuring QoS Functions	◆ Configuring Traffic Classification
Configuring User Authentication and Identification	◆ Configuring Subscriber Line Identifiers ◆ Configuring TACACS+ ◆ Configuring RADIUS
Configuring Network Protection	◆ Configuring the MSTP Service ◆ Configuring the LACP ◆ Configuring the ERPS
Configuring Test Functions	◆ Detecting the Optical Power
Reference Information	◆ FTP Operation Guide

Related Documentation

Document	Applied to
AN6001-G16 Optical Line Terminal Equipment Product Overview	Network planning phase
AN6001-G16 Optical Line Terminal Equipment Quick Installation Guide	Network deployment phase / network maintenance phase
AN6001-G16 Optical Line Terminal Equipment UNM2000 Configuration Guide	Network deployment phase / network maintenance phase
AN6001-G16 Optical Line Terminal Equipment CLI Configuration Guide	Network deployment phase / network maintenance phase

2 Configuring the UNM2000 Management Channel

- ☑ Logging into the Console
- ☑ Configuring the UNM2000 Management Channel
- ☑ Logging into the UNM2000

2.1 Logging into the Console

The following introduces how to log into the Console.

2.1.1 First-time Login to the Console

The UNM2000 management channel for the AN6001-G16 can only be configured through command lines on the Console. The following takes the Hyper Terminal of the Windows system as an example to introduce how to log into the Console and access the CLI network management system for the equipment.

Prerequisites

- The CONSOLE port of the HSOA card has been connected to the serial port of the network management computer.
- The network management computer has been started normally.
- The equipment is powered on normally.
- The user name and password for logging into the CLI network management system for the equipment are available.

Procedure

Note:

The Windows XP operating system is used as an example here.

Caution:

To enhance the security of the system, users should memorize their passwords and keep them secret. Regularly changing passwords is strongly recommended.

1. Click the **Start** menu on the desktop, and select **All Programs→Accessories →Telecom→Hyper Terminal** to open the **Connection Description** dialog box.

Note:

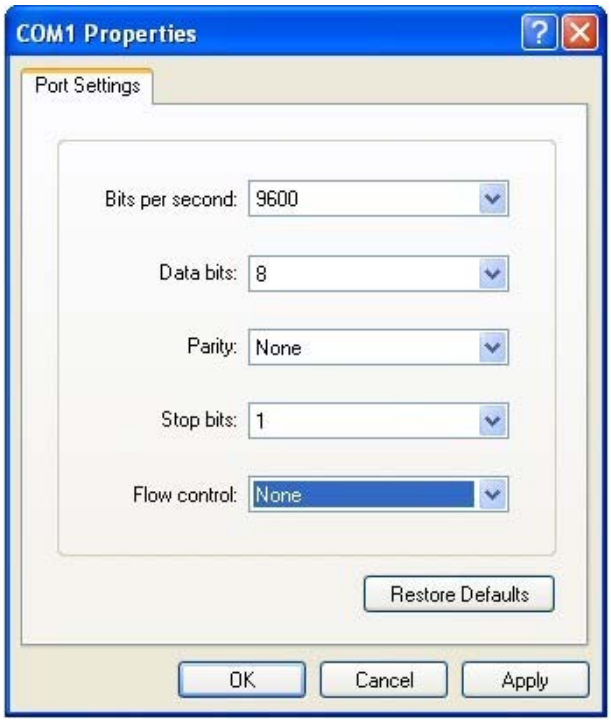
When you run the Hyper Terminal for the first time, the **Position Information** dialog box will appear. Fill in the required information according to practical situations, and click **OK** to open the **Connection Description** dialog box.

2. In the **Connection Description** dialog box, fill in the name of the Console and select an icon for it, and then click **OK**.

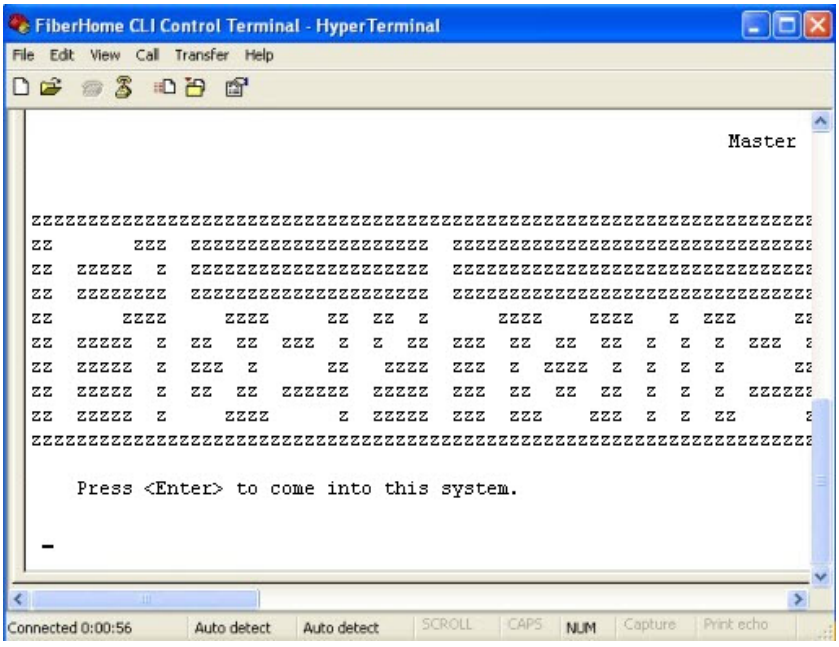
3. In the **Connect To** dialog box, select the number of the network management computer's serial port connecting with the AN6001-G16, such as the **COM1** port, and click **OK**.

4. In the **COM1 Properties** dialog box, click the **Restore Defaults** button. The default settings are as follows:

   - **Bits per second**: 9600
   - **Data bits**: 8
   - **Parity**: None
   - **Stop bits**: 1
   - **Flow control**: None



Click **OK** to start up the Console.



5. Press the Enter key, and type the user name and the password to log into the CLI network management system. The commands are described as follows:

`Login:`**GEPON**

// The default user is a common user, and the user name is "GEPON".

```
Password:*****
// The initial password is "GEPON".
User>enable
// In the read-only mode, users can enter the management mode via the command "enable".
Password:*****
// The initial password of the administrator account is "GEPON".
Admin#
// After the prompt "Admin#" appears, users can type command lines to operate on the AN6001-G16.
```

Note:

- If the command prompt is **User>**, the system is in the common user mode; if the command prompt is **Admin#**, the system is in the administrator mode.
- The user name is case insensitive, while the password should be capitalized.

6. Select **File→Save** from the menu bar of the Console window to save the configurations for the Console.

2.1.2 Subsequent Login to the Console

After exiting the set-up Console for the AN6001-G16 CLI network management system in your first login, you can directly access the Console via the CLI network management system next time.

Prerequisites

- The CONSOLE port of the HSOA card has been connected to the serial port of the network management computer.
- The network management computer has been started normally.
- The equipment is powered on normally.
- The Console for the AN6001-G16's CLI network management system has been set up (the following takes the **FiberHome CLI Control Terminal** as an example).

Procedure

1. Select **Start→Program→Accessories→Telecom→HyperTerminal→ FiberHome CLI Control Terminal** from the desktop to bring up the **Telnet default?** alert box. Then select either operation as follows:
   - Click **Yes** to make Hyper Terminal the default Telnet program;
   - Click **No**, and the Hyper Terminal will not be used as the default Telnet program.

   Start the set-up Console.

Note:

Users can create a shortcut of **FiberHome CLI Control Terminal** on the desktop for quick access.

2.2 Configuring the UNM2000 Management Channel

After logging into the Console, users need to configure the management channel in the GUI of the UNM2000.

2.2.1 Network Scenario

Service Planning

Assign the IP address 10.98.20.247/16 to the AN6001-G16. The IP address of the network management server is 10.98.20.168/16. The server needs to be connected with the to-be-managed AN6001-G16 through the gateway with the IP address 10.98.1.254 to enable in-band management.

Network Diagram

Figure 2-1 shows the network diagram. The AN6001-G16 and the network management server are connected respectively to different ports of the same gateway device. The management information is forwarded via the gateway device to achieve in-band management.

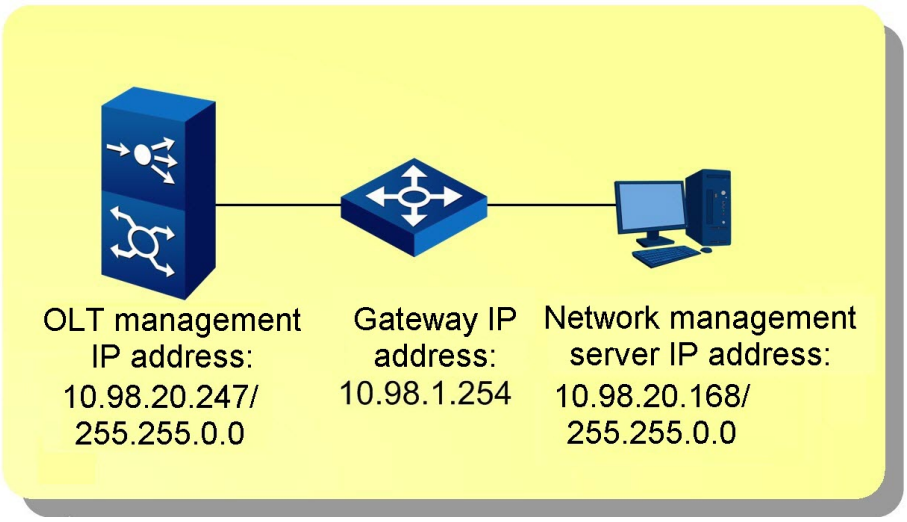


Figure 2-1 Network Diagram of the UNM2000

2.2.2 Planning Data

Item		Description	Example
Adding VLAN to an uplink port / deleting VLAN from an uplink port	VLAN ID	Configure this item according to the network planning of the operator. The value range is 1 to 4085.	100
	Management VLAN tag	Configure the VLAN tag processing method. "tag" indicates that the tag will not be stripped; "untag" indicates that the tag will be stripped.	tag
	Subrack ID	Configure this item according to the network planning of the operator.	1
	Slot No.	The number of the slot accommodating the uplink card.	19
	Port	Configure this item according to the network planning of the operator. The value range is 1 to 6.	1
Adding VLAN to slots / ports	VLAN ID	Configure this item according to the network planning of the operator. The value range is 1 to 4085.	100

Item		Description	Example
Configuring the management information	Management VLAN name	Configure this item according to the network planning of the operator.	test
	Management IP Address	Configure this item according to the network planning of the operator.	10.98.20.247
	Bit number of subnet mask	Configure this item according to the network planning of the operator.	16
Configuring static routing	Dst IP	Configure this item according to the network planning of the operator.	10.98.20.168
	Mask	Configure this item according to the network planning of the operator.	255.255.0.0
	Next-hop IP address	Configure this item according to the network planning of the operator.	10.98.1.254

2.2.3 Configuration Flow

The flow of configuring the UNM2000 management channel is shown in Figure 2-2.

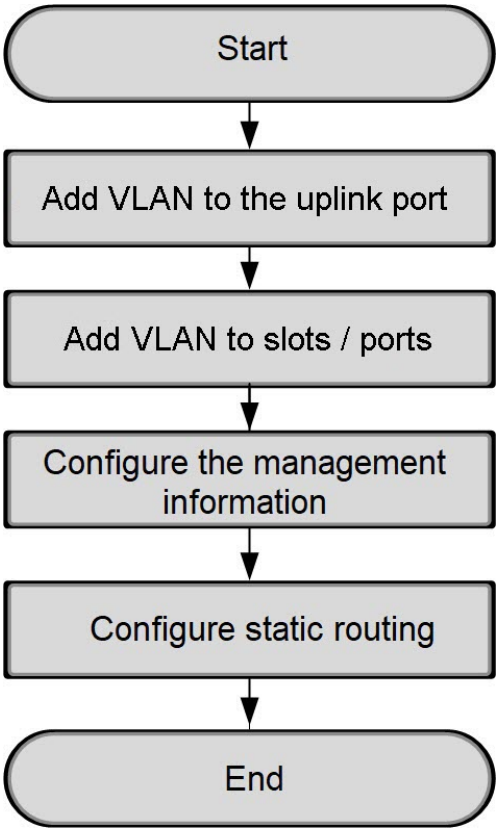


Figure 2-2 Flow of Configuring the UNM2000 Management Channel

2.2.4 Adding VLAN to an Uplink Port

Command Format

Table 2-1 Adding VLAN to an Uplink Port

Command
config
port vlan <vlanid> {to <end-vlanid>}*1 [tag|untag] <frameid/slotid> <port-list>
show port vlan <frameid/slotid/portid>

Procedure

1. Access the config directory.

```
Admin#config
Admin(config)#
```

2. Add VLAN to an uplink port.

```
Admin(config)#port vlan 100 tag 1/19 1
Admin(config)#
```

3. View the VLAN information of the port.

```
Admin(config)#show port vlan 1/19/1
port  19:1, vlan(optin): 100(T)
Admin(config)#
```

2.2.5 Deleting VLAN from an Uplink Port

If a VLAN is incorrectly configured or needs to be deleted, use this command to delete the VLAN.

Command Format

Table 2-2 Deleting VLAN from an Uplink Port

Command
config
no port vlan <vlanid> {to <end-vlanid>}*1 <frameid/slotid> <port-list>

Procedure

1. Access the config directory.

```
Admin#config
Admin(config)#
```

2. Delete VLAN from an uplink port.

```
Admin(config)#no port vlan 100 1/19 1
Admin(config)#
```

2.2.6 Adding VLAN to Slots / Ports

Command Format

Table 2-3 Adding VLAN to Slots / Ports

Command
config
port vlan <vlanid> {to <end-vlanid>}*1 allslot

Procedure

1. Access the config directory.

```
Admin#config
Admin(config)#
```

2. Add VLAN to all the slots / ports.

```
Admin(config)#port vlan 100 allslot
Admin(config)#
```

2.2.7 Configuring the Management Information

Command Format

Table 2-4 Configuring the Management Information

Command
config
manage-vlan <name> svlan <svlan> {cvlan <cvlan>}*1
manage-vlan ipv4 <name> <A.B.C.D/M>

Procedure

1. Access the config directory.

```
Admin#config
Admin(config)#
```

2. Create the management VLAN.

```
Admin(config)#manage-vlan test svlan 100
Admin(config)#
```

3. Configure the management VLAN IP address.

```
Admin(config)#manage-vlan ipv4 test 10.98.20.247/16
Admin(config)#
```

2.2.8 Configuring Static Routing

Command Format

Table 2-5 Configuring Static Routing

Command
config
static-route destination-ip <A.B.C.D> mask [<A.B.C.D>|<mask-length>] nexthop <A.B.C.D> {metric <0-255>}*1

Procedure

1. Access the config directory.

```
Admin#config
Admin(config)#
```

2. Configure the static routing.

```
Admin(config)#static-route destination-ip 10.98.20.168 mask 255.255.0.0 nexthop
10.98.1.254
Admin(config)#
```

2.2.9 Configuration Result

After the aforesaid steps, the configuration of the UNM2000 management channel is completed, and users can log into the UNM2000 to manage and maintain the AN6001-G16.

2.3 Logging into the UNM2000

Prerequisites

- JRE1.6.0 and UNM2000 client end have been installed.
- The server end is running normally.
- The communication between the server end and client end is normal.

Procedure

1. Double-click the UNM2000 client end icon on the desktop to bring up the login dialog box. Enter the IP address of the server end in the **Server** field.

Note:

If the software at the server end has been updated, the updated data will be downloaded accordingly at the client end when the client end is being started.

2. Click **Login**, and wait until the program loading is completed. When the **Main Topology** window appears, the user has logged into the network management system normally.

3 Adding Equipment

After logging into the UNM2000, you need to add the to-be-managed AN6001-G16 to a logical domain so as to manage and maintain it.

- ☑ Configuration Flow
- ☑ Creating the Logical Domain
- ☑ Creating the Access NE
- ☑ Adding Cards
- ☑ Configuring the SNMP Trap Receiver Address
- ☑ Synchronizing Time
- ☑ Saving Current Configuration to the FLASH

3.1 Configuration Flow

Figure 3-1 shows the flow of adding equipment in the UNM2000 system.

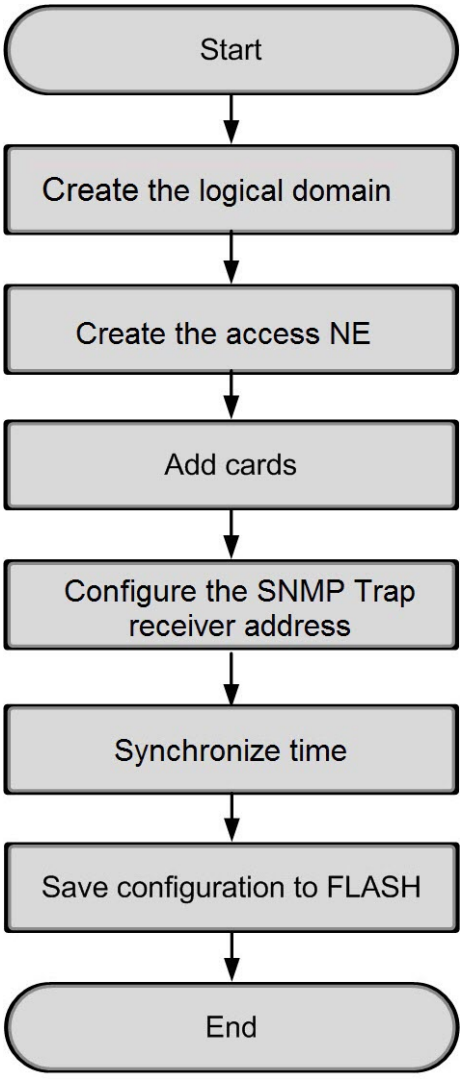


Figure 3-1 Flow of Adding Equipment

3.2 Creating the Logical Domain

Divide the management objects by creating corresponding logical domains according to the requirements of operators to enable management based on authorization and domain.

Procedure

1. Right-click a blank area of the Main Topology pane and select **Create Logical Domain** from the shortcut menu to bring up the **Create Global Logical Domain** dialog box.

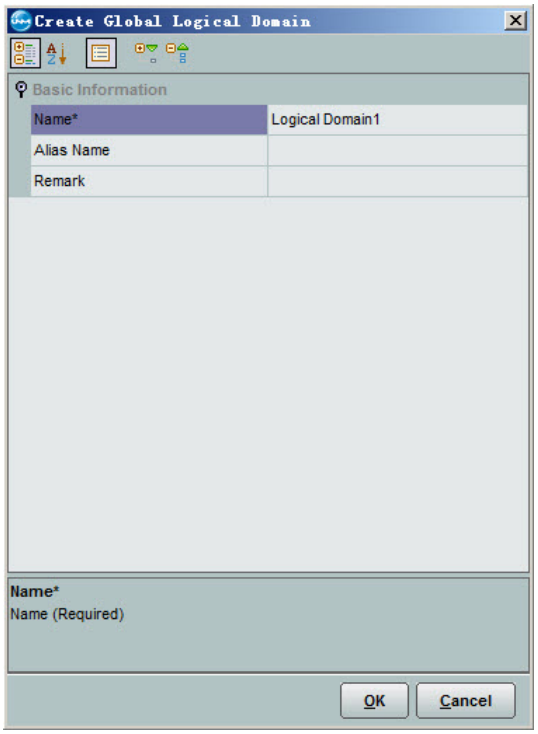


Figure 3-2 Creating the Logical Domain

2. Enter the desired name in the **Logical Domain Name** field. Alias Name and Remark are optional items.
3. Click **OK** to save the settings and create a new logical domain.

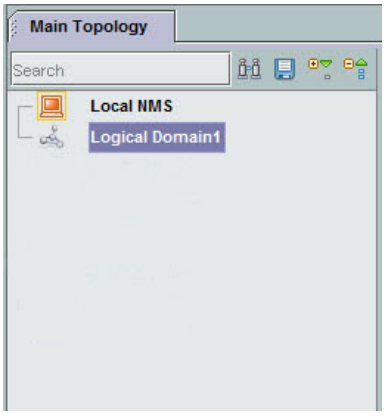


Figure 3-3 Logical Domain Creation Completed

3.3 Creating the Access NE

Procedure

1. Right-click the created logical domain and select **Create NE→Create Access NE...** from the shortcut menu.
2. Configure the parameters in the **Create Access NE** dialog box, as shown in Figure 3-4.

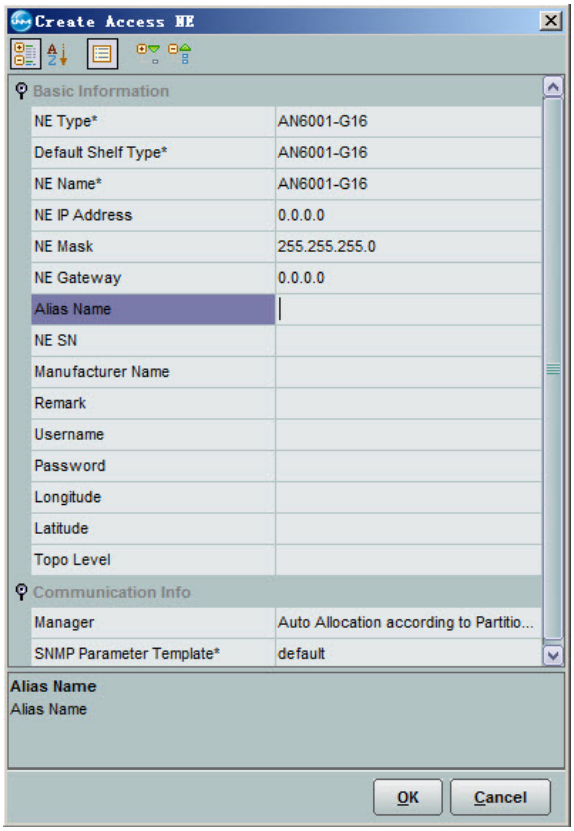


Figure 3-4 Creating the Access NE

3. Click **OK**, and the created access NE will appear in the main topology, as shown in Figure 3-5.

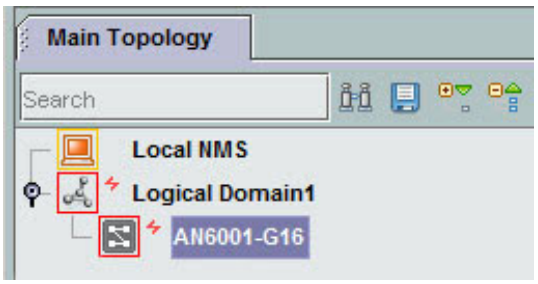


Figure 3-5 The Access NE Created

3.4 Adding Cards

Cards can be added either automatically or manually.

- Automatic adding: You can use the function of detecting physical configuration to add a card automatically if it is present.
- Manual adding: You can add a card that is not present by pre-configuring it. When a card is present, you can also add it manually.

3.4.1 Configuring Subracks and Cards

Table 3-1 describes the mappings between the AN6001-G16 subrack slots and the cards.

Table 3-1 Card Configuration for the Equipment

Card Name	Slot
GPOP	1
HSCP	9
HU2P	19
FAN	23
PWRA / PWRD	24, 25

3.4.2 Adding Cards Automatically

Procedure

1. Right-click the NE to be configured in the **Main Topology** pane and select **Detect Physical Configuration** from the shortcut menu to open the **Detect Physical Configuration** tab.
2. Select the desired synchronization mode. **Overwritten** is recommended for a newly started device, and **Incremental** is recommended for a device that has run for a period of time with cards added or deleted.
3. Click the **Detect Physical Configuration (D)** button and wait until the detection is completed, as shown in Figure 3-6.

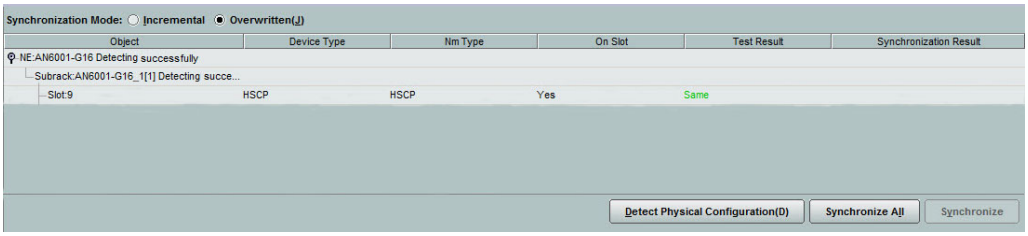


Figure 3-6 Detecting the Physical Configuration

4. Click the **Synchronize All** button and click **OK** when the **Synchronize Operation Succeed.** message appears to complete adding the card automatically.

5. Double-click the NE in the **Main Topology** pane to open the **NE Manager** and check whether the current card configuration conforms to the real situation, as shown in Figure 3-7.

Figure 3-7 Checking the Card Configuration

3.4.3 Adding Cards Manually

Add cards manually for card configurations.

Slot Distribution

After adding the AN6001-G16 NE, double-click this NE in **Main Topology** to open the **NE Manager**. The subrack view will be displayed in the right pane, as shown in Figure 3-8.

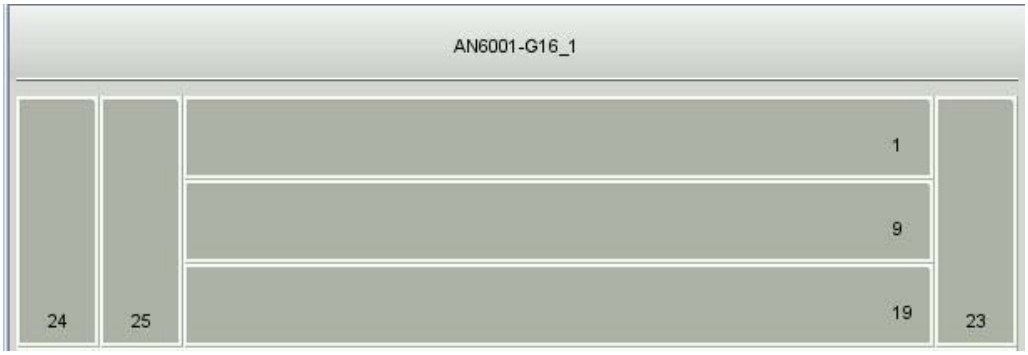


Figure 3-8 Subrack View - Card Not Added

Procedure

Add a GPOP card to Slot 1 manually.

1. Right-click Slot 1 and select **Add PON Card→Add GPOP Card** from the shortcut menu, as shown in Figure 3-9.

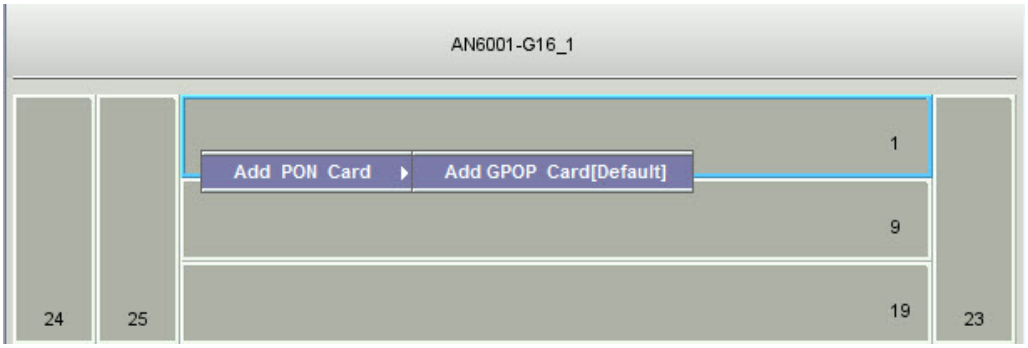


Figure 3-9 Adding the GPOP Card

Modifying a Card

- Modifying card properties

  Right-click the card to be modified in the subrack view or the "Device Tree" on the left, and select **Attribute** from the shortcut menu. Then modify the card properties in the **Property Page** on the right. After finishing the modification, click the **Apply** button to save the modification.

- Deleting a card

Right-click the card to be deleted in the subrack view or the "Device Tree" on the left, and select **Delete Card** from the shortcut menu to delete the selected card.

- Replacing a card

  Right-click the card to be replaced in the subrack view or the device tree on the left pane, and select **Replace Card** from the shortcut menu. Then select the desired card from the submenu. After replacing the card, reconfigure the parameters for the new card or use the default settings.

3.5 Configuring the SNMP Trap Receiver Address

Background Information

Configure the SNMP Trap receiver address, and then the system will send the Trap message to the address.

Planning Data

Item	Description	Example
Trap Receiver IP Address	The IP address to which the alarm is sent. Both IPv4 and IPv6 addresses are supported.	IPv4:10.78.20.122
UDP Port	The number of the user data protocol port. The value ranges from 0 to 65535.	162
Community	Set the community which stands for a group of managed devices. The value contains no more than 32 characters.	public
SNMP Version	Set the SNMP version. When the security class is set to **0**, SNMP V1 and SNMP V2C are supported. For other security classes, only SNMP V3 is supported. ◆ SNMP V1: SNMP V1 protocol version ◆ SNMP V2C: Compared with SNMP V1, this version reduces the communications between the network management stations and the managed devices to enhance network performance. ◆ SNMP V3: Embracing the basic functions of SNMP V1 and SNMP V2C, this version defines a series of management functions concerning security and access control.	SNMP V2C

Item	Description	Example
Enable Signal Trace Report	The switch for enabling / disabling report of the signaling trace information. The default setting is "Disable". Enable the signaling tracing task on the network management system. The uplink device delivers the task parameters to the media gateway via the interface between the network management system and the uplink device. Based on the parameters received, the media gateway sets up the connection with the tracing server (FTP server), and reports the signaling messages that it has obtained to the tracing sever at regular time.	Disable
Security level	Select the desired security level: ◆ 0 ◆ noauth (no authorization and no encryption) ◆ authnopriv (authentication without encryption) ◆ authpriv (authentication and encryption)	0
Source IP Address	The IP address of the network management server. Both IPv4 and IPv6 addresses are supported.	IPv4:10.32.105.180

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. Select **Common Config→SNMP TRAP Receiver IP** from the **Operational Tree** pane to bring up the **SNMP TRAP Receiver IP** tab.
4. Click **Add** on the toolbar, and enter **1** in the dialog box that appears. Click **OK** to create an SNMP TRAP receiver IP address configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 3-10.

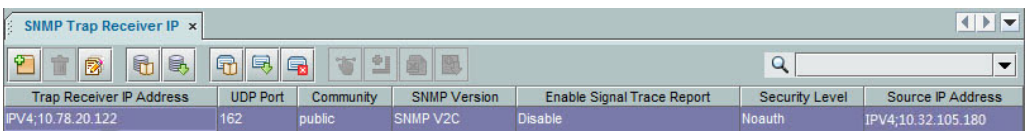


Figure 3-10 Configuring the SNMP TRAP Receiver Address

3.6 Synchronizing Time

System time synchronization aims to synchronize the time of the network management server with that of the AN6001-G16 and check whether the communication between them is smooth.

Procedure

Note:

After being connected to the network management system correctly, the equipment will apply to the network management server for time synchronization. If connected to multiple network management servers, the equipment will apply to the first server connected to it for time synchronization.

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Initialize→Time Calibration** to bring up the **Issue the command** dialog box, as shown in Figure 3-11.

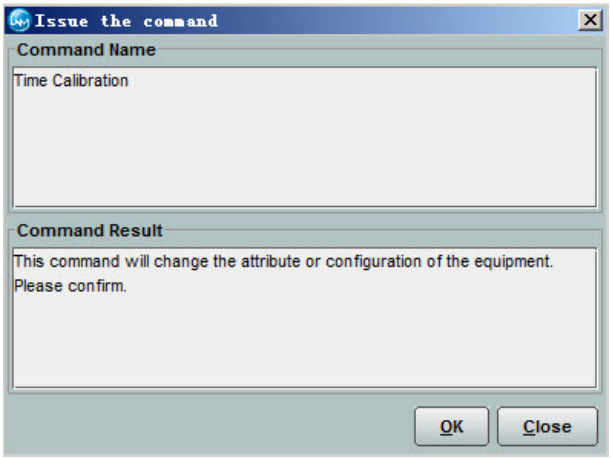


Figure 3-11 Synchronizing Time

4. Click the **OK** button, and the system begins to execute the command of time synchronization.
5. After the time synchronization is completed successfully, click the **Close** button.

3.7 Saving Current Configuration to the FLASH

Background Information

To prevent loss of equipment configuration data subsequent to power failure, it is recommended that users should take this operation after they have completed service provisioning and function configuration.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **System Control→Save Config to Flash** to bring up the **Issue the command** alert box, as shown in Figure 3-12.

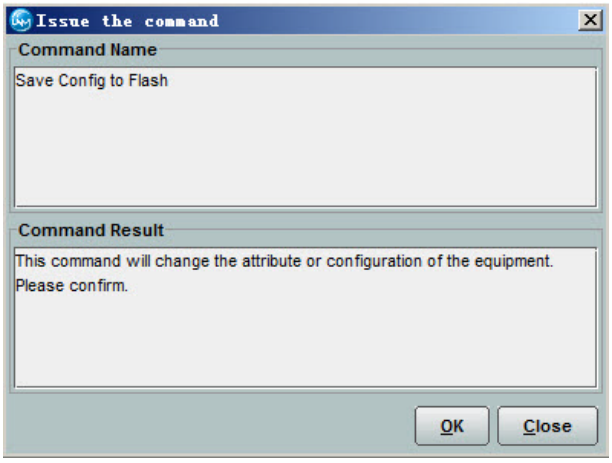


Figure 3-12 Saving Current Configuration to the Flash

4. Click **OK**, and the system begins to execute the command.
5. After the configuration data are successfully saved, click **Close**.

4 Authenticating and Authorizing an ONU

The following introduces the ONU authentication and authorization scenarios such as ONU authentication, modification of ONU authentication, and deletion of authentication / authorization.

☑ Authenticating and Authorizing an ONU

☑ Modifying the Authentication Mode and Re-authorizing an ONU

4.1 Authenticating and Authorizing an ONU

Before configuring the services for the AN6001-G16, users must authenticate and authorize the ONU connected to the service interface card.

4.1.1 Configuring the PON Port Authentication Mode

Before authorizing an ONU, the AN6001-G16 needs to be configured with the PON port authentication mode. In this example, the physical identifier authentication is used.

Planning Data

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	1 to 16
Authentication Mode	Select the ONU authentication mode as needed. The ONU should be authenticated and authorized on the AN6001-G16 in the selected authentication mode.	PHYSIC_ID AUTHENTICATION

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU Authentication** button to access the **ONU Authorization View** tab.
3. Select the **PON Port Authentication Mode** tab in the **ONU Authorization View** pane.
4. Double-click the **Authentication Mode** field in the row for PON port 1 in Slot 1, and select **PHYSIC_ID AUTHENTICATION** from the drop-down menu.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 4-1.

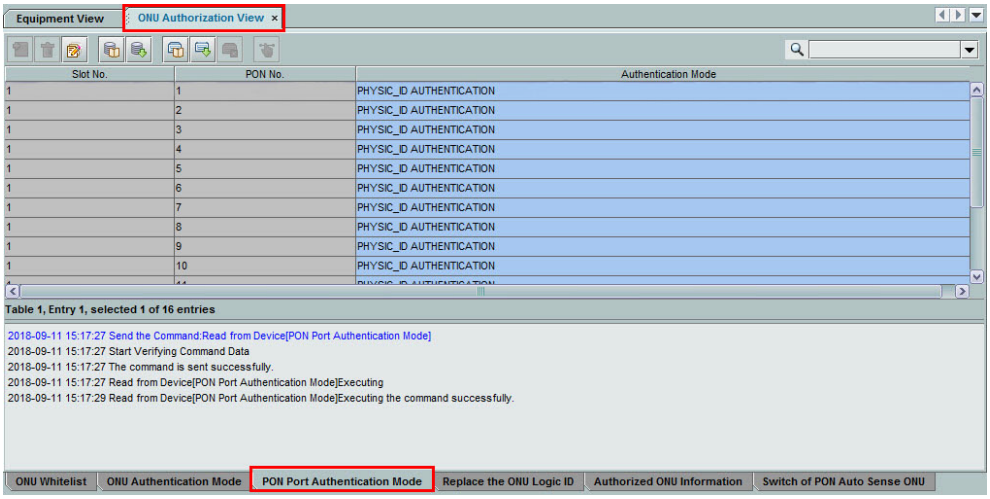


Figure 4-1 Configuring the PON Port Authentication Mode

4.1.2 Configuring the White List - Manual Authorization

Planning Data

Item	Description	Example
Whitelist Type	Select the white list type.	PHYSIC_ID AUTHENTICATION
Physic ID	Enter the physical ID for the ONU.	001122334455
Physic Password	Configure this item when the authentication mode is set to password (ONU physical identifier).	-
SN: LOID	Enter the logical identifier of the ONU.	-
SN: Logical Password	Configure this item when the authentication mode is set to password (ONU logical identifier).	-
Slot No.	Enter the number of the slot housing the card connected to the ONU.	1
PON No.	Enter the number of the PON port connected to the ONU.	1
ONU Type	The type of the ONU.	AN5506-04-B
ONU No.	Enter the ONU authorization number, which ranges from 1 to 256.	10
Enable/Disable	The ONU switch.	Enable
Status	The ONU authorization status.	Implemented

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU Authentication** button to access the **ONU Authorization View** tab.
3. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to add an ONU authorization entry.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar. See Figure 4-2 for the illustration of a successful pre-authorization.

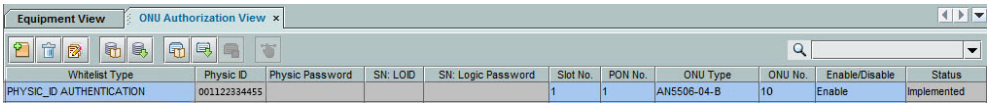


Figure 4-2 Configuring the White List - Manual Authorization

4.1.3 Configuring the White List - Automatic Authorization

Planning Data

Item	Description	Example
Slot Number	The number of the slot housing the card to which the unauthorized ONU is connected (read-only).	1
PON Number	The number of the PON port to which the unauthorized ONU is connected (read-only).	8
Physical Address	The physical address of the unauthorized ONU (read-only).	544b400b34d0
Password	The physical identifier password of the unauthorized ONU (read-only).	-
Logical SN	The logical SN of the unauthorized ONU (read-only).	-
Logical SN Password	The logical SN password of the unauthorized ONU (read-only).	-
ONU Type	The type of the unauthorized ONU (read-only).	AN5506-04-B

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **Obtain Unauthorized ONU** button on the toolbar to bring up the **Switch Object (Unauthorized ONU List)** dialog box.
3. In the **Switch Object (Unauthorized ONU List)** dialog box, select PON Port 8 of the GPOP card in Slot 1 and click **OK**. Then select the ONU whose physical address is 544b400b34d0, as illustrated in Figure 4-3.

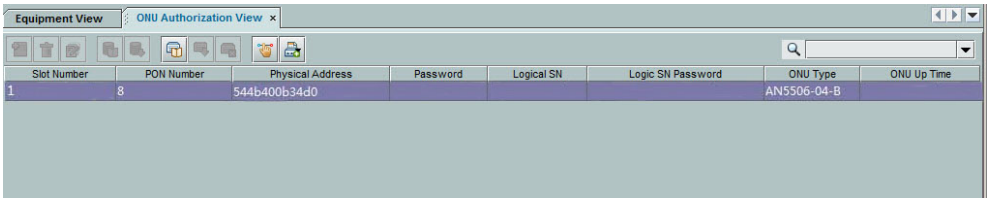


Figure 4-3 Getting Unauthorized ONU - Automatic Authorization Based on Physical Identifier

4. Click the **Add to the ONU Authority List** button on the toolbar, and select **as "Physical ID Authentication Mode" Added to the Whitelist**. In the dialog box that appears, select **Current Row**, and click **OK**.
5. Click the **Create On Device** button on the toolbar. The ONU is successfully authorized, as shown in Figure 4-4.

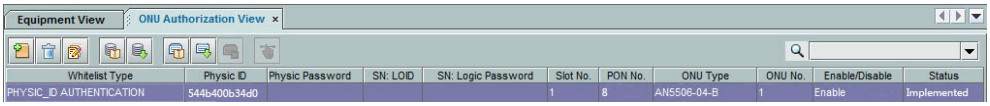


Figure 4-4 Automatic Authorization Succeeded - Based on Physical Identifier

4.2 Modifying the Authentication Mode and Re-authorizing an ONU

The following introduces how to modify the authentication mode for the AN6001-G16 and re-authorize an ONU.

4.2.1 Deleting an ONU from the Physical Identifier White List - Optional

Prerequisites

Make sure that the authentication of the ONU is based on physical identifier before this operation. Otherwise, deletion of the ONU from the white list will neither deauthorize the ONU nor affect the configurations of the ONU.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU Authentication** button to access the **ONU Authorization View** tab.
3. Select the target ONU and click the **Delete on Device** button in the toolbar. In the alert box that appears, select **Current Row** and click **OK** to delete the authorization information of the ONU from the white list.

4.2.2 Reconfiguring the Authorized ONUs in the White List

Configure the logical identifier white list to change the ONU authorization mode.

Planning Data

Item	Description	Example
Whitelist Type	Select the ONU authentication mode as needed. The ONU should be authenticated and authorized on the AN6001-G16 in the selected authentication mode.	PASSWORD AUTHENTICATION
Physic Password	The physical password for the ONU.	5fa5087
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	1
ONU Type	The type of the ONU.	AN5506-04-B
Enable/Disable	The ONU authentication white list switch.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU Authentication** button to access the **ONU Authorization View** tab.
3. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to add an ONU authorization entry.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 4-5.

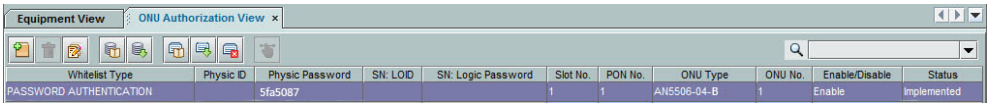


Figure 4-5 ONU White List

4.2.3 Switching the PON Port Authentication Mode

Switch the PON port authentication mode. In this example, the authentication mode is switched from physical identifier authentication to password authentication.

Planning Data

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	1
Authentication Mode	Select the ONU authentication mode as needed. The ONU should be authenticated and authorized on the AN6001-G16 in the selected authentication mode.	PASSWORD AUTHENTICATION

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU Authentication** button to access the **ONU Authorization View** tab.
3. Select **PON Port Authentication Mode** tab in the **ONU Authorization View** pane.
4. Double-click the **Authentication mode** field in the row for PON port 1 in Slot 1, and select **PASSWORD AUTHENTICATION** from the drop-down menu.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 4-6.

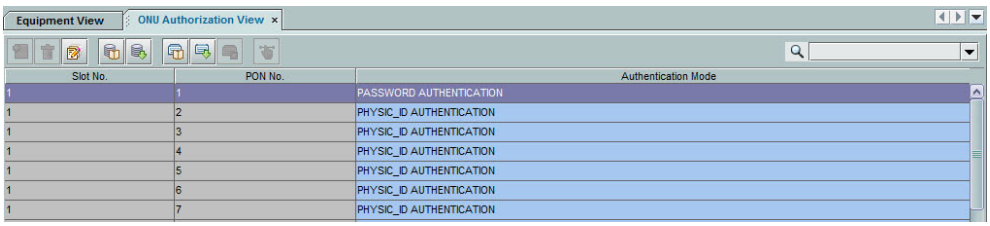


Figure 4-6 Switching the PON Port Authentication Mode

5 Basic Configurations

The following introduces basic configurations of the VLAN service channel for the AN6001-G16.

- ☑ Configuring Local End Outer VLAN Data
- ☑ Adding Ports to the VLAN
- ☑ Disabling Suppression of Multicast Packets at the Uplink Port

5.1 Configuring Local End Outer VLAN Data

Background Information

You need to set up the VLAN service channel before configuring services on the AN6001-G16. In this example, the VLAN channel for voice service is set up.

Planning Data

Item	Description	Example
Service Name	You can enter numbers, letters and underlines not exceeding 23 characters for the subscriber service name.	ngn
Starting VLAN ID	The starting value of the service VLAN ID. The value ranges from 1 to 4085. The starting VLAN ID should not be larger than the ending VLAN ID.	4080
Ending VLAN ID	The ending value of the service VLAN ID. The value ranges from 1 to 4085. The starting VLAN ID should not be larger than the ending VLAN ID.	4080
Service Type	The service VLAN type. Select it according to the type of service to be configured. ◆ Data: data service. ◆ IPTV: IPTV service. ◆ NGN: voice service in the carrier network. ◆ VoIP: voice service based on Internet. ◆ VOD: video-on-demand service. ◆ CNCView: CNC service. ◆ System: system service.	NGN

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **VLAN Service→VLAN Local Config→ Local End Service Outer VLAN** to bring up the **Local End Service Outer VLAN** tab.

4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a VLAN configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 5-1.

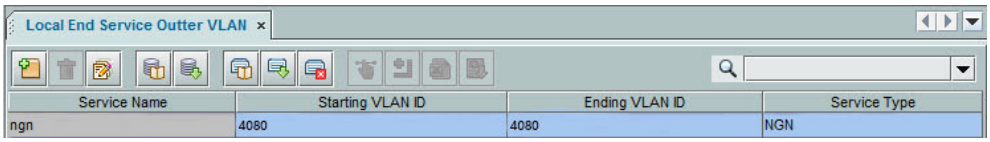


Figure 5-1 Configuring Local End Outer VLAN Data

5.2 Adding Ports to the VLAN

Background Information

You need to specify the service uplink / downlink port after the local end service VLAN is created.

Planning Data

Item	Description	Example
VLAN ID	The VLAN ID.	3500
VLAN Type	Read only.	Common VLAN

Item	Description	Example
Interface No.	Specify the object to be bound with the service VLAN. The object can either be a single uplink port or a created aggregation group. After the configuration, the packets forwarded via the specified uplink port / aggregation group will be added with the corresponding service VLAN.	19:SFP+1 All slots
TAG/UNTAG	Configure the tag processing mode for the uplink service VLAN. Two options are available: **UNTAG** and **TAG**. ◆ In the **UNTAG** mode, the tags of the uplink packets will be stripped automatically when they pass the port and the packets will be further transmitted in the untagged mode, while the downlink untagged packets will be added with corresponding tags when they pass the port. ◆ In the **TAG** mode, the tags of the uplink / downlink data packets will not be processed when they pass the port.	TAG

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **VLAN Service→Add vlan to port** to open the **Add vlan to port** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a VLAN ID configuration entry.
5. Select the right pane, click **Add**, enter **2** in the dialog box that appears, and click **OK** to add two uplink port number or TRUNK group number configuration entries.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 5-2.

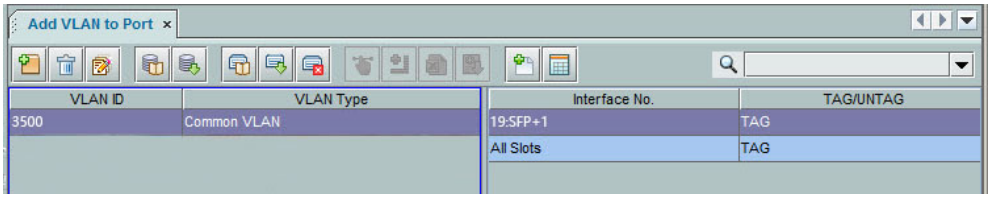


Figure 5-2 Adding Ports to the VLAN

5.3 Disabling Suppression of Multicast Packets at the Uplink Port

Background Information

Suppression of multicast packets at the uplink port of the AN6001-G16 restrains broadcast, multicast and unknown packets from the system. To ensure normal service operation for system users, you need to disable the suppression function.

Planning Data

Item	Description	Example
Port No.	Read-only item, indicating the number of the uplink port to be configured.	19:SFP+1
Type of Packet	Read-only item. Three options are available: ◆ Broadcast Package ◆ Multicast Package ◆ Unknown Package	Multicast Package
Enable/Disable	Enable / Disable	Disable
Speed (Packet/Second)	The speed limit on data packets. The value ranges from 0 to 262142.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Data Service→Packet Suppression→Upport Packet Rate Control** to bring up the **Upport Packet Rate Control** tab.

4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 5-3.

Figure 5-3 Suppression of Packets at the Uplink Port

6 Configuring Voice Services

The following introduces how to start up the voice services for the AN6001-G16.

☑ Example of Configuring Voice Service

☑ Optional Functions

6.1 Example of Configuring Voice Service

Traditional analog voice signals are compressed and packetized, and then transported over the IP-based packet switched network. This is known as VoIP voice service, which has lower cost and can enhance bandwidth utilization.

The AN6001-G16 supports communication with the Media Gateway Controller (MGC) or IP Multimedia Subsystem (IMS) based on the H.248 or SIP protocol to provide voice services.

In this example, voice service configuration for an individual device is described.

6.1.1 Network Scenario

Service Planning

- The subscriber services are accessed via the GPON ONU.
- The subscriber services include the POTS, IPT, and POS machine services.
- The single-tagged service VLAN is used.

Network Diagram

Figure 6-1 shows the network diagram for the voice services.

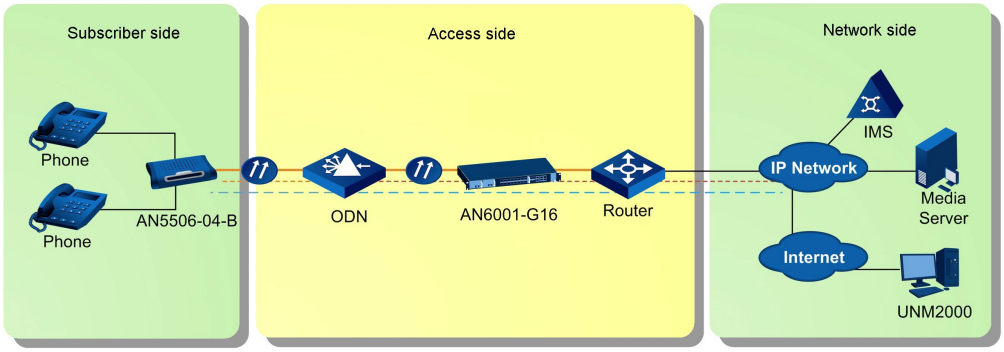


Figure 6-1 Network Diagram for the Voice Service

6.1.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

Figure 6-2 shows the flow of configuring voice services for the AN6001-G16 individually.

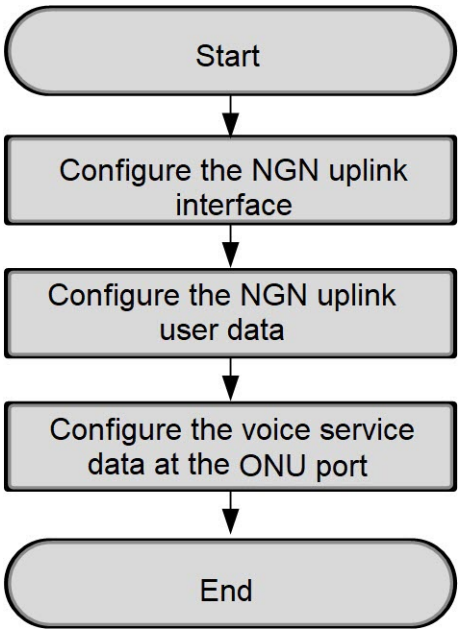


Figure 6-2 Flow of Configuring Voice Services

6.1.3 Configuring the NGN Uplink Interface

Configuration Rules

- When the H.248 protocol is used to control the access terminals, set the MGC protocol type to H.248 and the protocol port No. to 2944 for VoIP services.
- When the SIP protocol is used to control the access terminals, set the MGC protocol type to SIP and the protocol port No. of the register server and proxy server to 5060 for VoIP services.

- When standby configuration exists, enter the corresponding value in the standby item field; when the standby value does not exist, the configuration is not needed.
- To delete a configured proxy server, users need only to clear this field. The IP address of a server cannot be set to 0.0.0.0.

Planning Data

Item		Description	Example
H.248	Signaling Service Name	Select the name set in the **Local End Service Outer VLAN**.	H248
	Interface ID	The logical identifier set for the NGN uplink interface to identify the NGN uplink services when a local VLAN corresponds to multiple NGN uplink services.	H248
	Protocol Type	Select the matching protocol type: MGCP, H.248 or SIP.	H.248
	MGC1 IP Address / Standby SIP Register Server Address	The IP address or the domain name of the active softswitch platform MGC1.	10.20.30.40
	MGC1 Port / Standby SIP Register Sever Port	The communication port of the active softswitch platform MGC1. The default setting is 2944.	2944
	MGC2 IP Address / Standby SIP Proxy Server Address	The IP address or domain name of the standby softswitch platform. Leave this item blank if no standby platform is configured.	-
	MGC2 Port / Standby SIP Proxy Server Port	The communication port of the standby softswitch platform. The default setting is 2944. Leave this item blank if no standby platform is configured.	-
	MGC3 IP Address	The IP address or domain name of the standby softswitch platform. Leave this item blank if no standby platform is configured.	-
	MGC3 Port	The communication port of the standby softswitch platform. The default setting is 2944. Leave this item blank if no standby platform is configured.	-
	Keep-alive	Controls whether the ONU regularly sends keep-alive messages to the softswitch platform MGC. Options available are "Enable Initiative", "Enable Passive" and "Disable".	Enable Initiative

Item		Description	Example
	Master DNS Server	The IP address of the master domain name system. Users need to configure the DNS server when the MGC is configured as the domain name. When the MGC is configured as the IP address, this item is invalid.	-
	Slave DNS Server	The IP address of the slave domain name system. Users need to configure the DNS server when the MGC is configured as the domain name. When the MGC is configured as the IP address, this item is invalid.	-
SIP	Signaling Service Name	Select the name set in the **Local End Service Outer VLAN**.	SIP
	Interface ID	The logical identifier set for the NGN uplink interface to identify the NGN uplink services when a local VLAN corresponds to multiple NGN uplink services.	SIP
	Protocol Type	Select the matching protocol type: MGCP, H.248 or SIP.	SIP
	MGC1 IP Address / Standby SIP Register Server Address	The address of the SIP standby register server. Leave this item blank if no standby server is configured.	-
	MGC1 Port / Standby SIP Register Sever Port	The port number of the SIP standby register server. The default setting is 5060. Leave this item blank if no standby server is configured.	-
	MGC2 IP Address / Standby SIP Proxy Server Address	The address of the SIP standby register server. Leave this item blank if no standby server is configured.	-
	MGC2 Port / Standby SIP Proxy Server Port	The port number of the SIP standby register server. The default setting is 5060. Leave this item blank if no standby server is configured.	-
	Keep-alive	Controls whether the ONU regularly sends keep-alive messages to the softswitch platform MGC. Options available are "Enable Initiative", "Enable Passive" and "Disable".	Enable Initiative
	Master DNS Server	The IP address of the master domain name system. Users need to configure the DNS server when the MGC is configured as the domain name. When the MGC is configured as the IP address, this item is invalid.	-

Item		Description	Example
	Slave DNS Server	The IP address of the slave domain name system. Users need to configure the DNS server when the MGC is configured as the domain name. When the MGC is configured as the IP address, this item is invalid.	-
	SIP Registrar Server Address	The IP address or domain name of the SIP registrar.	10.20.30.41
	SIP Registrar Server Port	The port number of the SIP registrar. The default setting is 5060.	5060
	SIP Proxy Server Address	The IP address or domain name of the SIP proxy server.	10.20.30.42
	SIP Proxy Server Port	The port number of the SIP proxy server. The default setting is 5060.	5060
	SIP Expires (S)	The timeout period of SIP. The value ranges from 120 to 86400. The default value is 3600.	3600

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **POTS Service→NGN Uplink→NGN Interface** to open the **NGN Interface** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and then click **OK** to add an NGN uplink interface configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in the figure below.

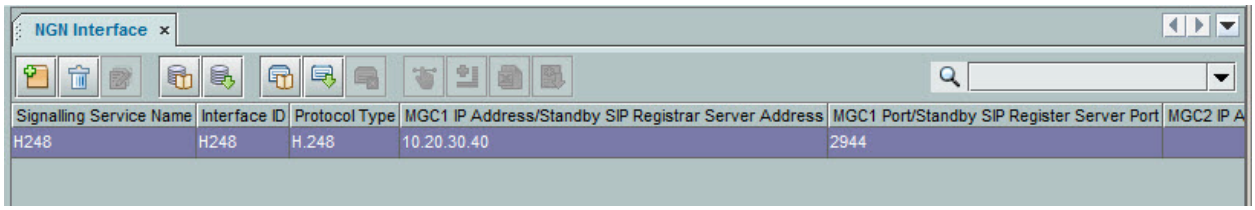


Figure 6-3 The H.248 Protocol

Figure 6-4 The SIP Protocol

6.1.4 Configuring the NGN Uplink Subscriber Data

Planning Data

Item		Description	Example
H.248	Service Name @ Interface ID	Select the **Signaling Service Name** and **Interface ID** configured in **NGN Interface**.	H248@H248
	Signaling VLAN ID	The voice service signaling VLAN; it is CVLAN when QinQ is enabled.	200
	IP Config Mode	Select the public network IP address configuration mode for the ONU. The IP address can be configured manually as a static one or obtained dynamically.	Static
	ONU Public IP	Configure this item according to the network planning of the operator. When the DHCP or the PPPoE function is enabled, the IP address assigned to the ONU dynamically will override the public IP address assigned to the ONU by the system.	IPv4:20.30.40.50/255.255.255.0
	ONU Public IP Gateway	Configure this item according to the network planning of the operator.	20.30.40.1
	Endpoint Domain Name/SIP User Name Postfix	The domain name address of the gateway. Configure this item according to the operator's network planning.	20.30.40.50
	ONU Protocol Port No.	Configure this item according to the operator's network planning. The default setting is 2944.	2944
	User Index	The logical number in the system. It is advised to set this item to the phone number defined by the softswitch platform. The value ranges from 1 to 4294967294.	1001
	Endpoint User Name/SIP Telephone No.	When the H.248 protocol is used, this item stands for the endpoint user name, i.e. the Termination ID corresponding to the port. Configure this item according to the network planning of the operator.	aaln/0

Item		Description	Example
SIP	Service Name @ Interface ID	Select the **Signaling Service Name and Interface ID** configured in **NGN Interface**.	SIP@SIP
	Signaling VLAN ID	The voice service signaling VLAN; it is CVLAN when QinQ is enabled.	300
	SVLAN State	The QinQ enabling / disabling state. Configure this item according to the operator's network planning; the default setting is "Disable".	Disable
	SVLAN ID	It is the SVLAN ID when QinQ is enabled. The SVLAN ID value should be within the uplink VLAN ID range. It is invalid when QinQ is disabled.	-
	COS1	It is the outer VLAN priority when QinQ is enabled; it is invalid when QinQ is disabled.	-
	COS2	It is the inner VLAN priority when QinQ is enabled; and it is the single-tagged VLAN priority when QinQ is disabled.	-
	IP Config Mode	Select the public network IP address configuration mode for the ONU. The IP address can be configured manually as a static one or obtained dynamically.	DHCP
	ONU Public IP	Configure this item according to the network planning of the operator. When the DHCP or the PPPoE function is enabled, the IP address assigned to the ONU dynamically will override the public IP address assigned to the ONU by the system.	-
	ONU Public IP Gateway	Configure this item according to the network planning of the operator.	-
	Endpoint Domain Name/SIP User Name Postfix	The domain name address of the gateway. Configure this item according to the operator’s network planning.	-
	ONU Protocol Port No.	Configure this item according to the operator’s network planning. The default setting is 5060.	-
	User Index	The logical number in the system. It is advised to set this item to the phone number defined by the softswitch platform. The value ranges from 1 to 4294967294.	1
	Endpoint User Name/SIP Telephone No.	When the SIP protocol is used, this item is the SIP telephone number. Configure this item according to the network planning of the operator.	87654321
	SIP User Name	The user name authenticated by the SIP endpoint and the SIP registrar. Configure this item according to the operator’s network planning.	87654321

Item		Description	Example
	SIP User Password	The user password authenticated by the SIP endpoint and the SIP registrar. Configure the item according to the operator's network planning.	123456
	Confirm Password	The password here should be consistent with the **SIP User Password**.	123456

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **POTS Service→NGN Uplink→NGN Configuration** to open the **NGN Configuration** tab.
4. Select the left pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to add an NGN service configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in the figure below.

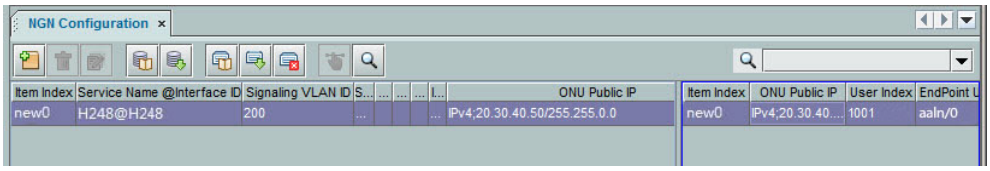


Figure 6-5 Configuring the NGN Uplink User Data - H.248

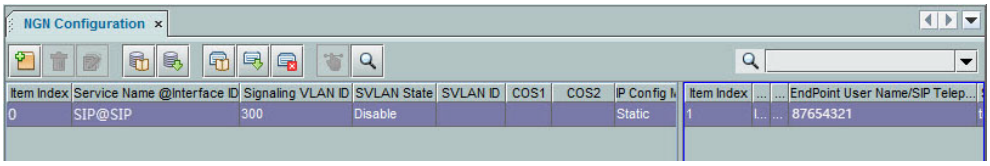


Figure 6-6 Configuring the NGN Uplink User Data - SIP

6.1.5 Configuring the Voice Service at the ONU Port

Configuration Rules

- When configuring the VoIP service VLAN, make sure that the signaling VLAN ID is within the range of the local end service VLAN ID if a single-tagged VLAN is used.
- If stacked VLANs are used, make sure that the SVLAN ID is within the range of the local end service VLAN ID, and you can assign the CVLAN ID as needed.

Planning Data

Parameters of the voice service at an ONU port are configured likewise for both voice protocols. In this example, the SIP protocol is used.

Item		Description	Example
SIP	Port Number	The number of the ONU's port physically connected with the subscriber phone.	1
	Port Name	The name of the ONU's port physically connected with the subscriber phone.	VOIP1
	User Index	This item should be consistent with the user index in the **NGN Configuration** tab.	1
	Signal VLAN ID	The voice service VLAN ID; it is the CVLAN ID when QinQ is enabled.	300
	SVLAN Enable	The QinQ enabling / disabling state. Configure this item according to the operator's network planning; the default setting is "Disable".	Disable
	SVLAN ID	It is the SVLAN ID when QinQ is enabled. The SVLAN ID value should be within the uplink VLAN ID range. It is invalid when QinQ is disabled.	-
	Outer COS	It is the outer VLAN priority when QinQ is enabled; it is invalid when QinQ is disabled.	-
	Inner COS	It is the inner VLAN priority when QinQ is enabled; and it is the single-tagged VLAN priority when QinQ is disabled.	-
	Silence Switch	Configure this item according to the operator’s network planning. The default setting is "Disable".	Disable
	Echo Cancel	Configure this item according to the operator’s network planning. The default setting is "Enable".	Enable

Item		Description	Example
	Voice Codec	Configure this item according to the operator's network planning. The default setting is G.711A.	G.711A
	Fax Control Mode	Configure this item according to the operator's network planning; the default setting is Voice Channel.	Voice Channel
	Fax Mode	Configure this item according to the operator's network planning; the default setting is "Transparent".	Transparent
	DTMF Mode	Configure this item according to the operator's network planning; the default setting is "Transparent".	Transparent
	Input Gain (-32 to 32)	Configure this item according to the operator's network planning. The default setting is 0.	0
	Output Gain (-32 to 32)	Configure this item according to the operator's network planning. The default setting is 0.	0
	Charging Mode	The charing mode for the voice service at the port.	Reverse Polarity

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click the ONU to be configured, and select **Port Service Config** from the shortcut menu that appears to bring up the **Port Service Config** tab.
4. Select the **Voice port**, and configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 6-7.

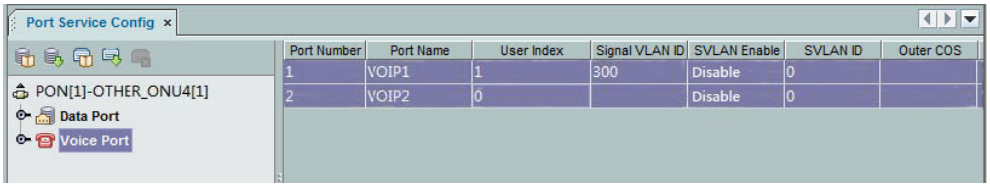


Figure 6-7 Configuring Parameters of the Voice Service at the ONU Port

6.1.6 Configuration Result

The voice service at the VOIP1 port of the ONU has been started up and subscribers can call each other normally.

6.2 Optional Functions

The following introduces how to configure the optional functions related to voice services provided by the AN6001-G16.

6.2.1 Configuring the Softswitch Intercommunication Profile Parameters

The following introduces how to configure the softswitch intercommunication profile and bind the profile to the ONU.

6.2.1.1 Configuring the Softswitch Intercommunication Parameter Profile

To enable the VoIP service, you need to configure the parameters required for intercommunication between the ONU and the Softswitch platform.

Configuration Rules

- The RTP resource needs to be configured only when the H.248 protocol is used.
- The Digitmap needs to be configured only when the SIP is used.

Planning Data

Item	Description	Example
Profile Name	The name of the softswitch intercommunication profile for the AN6001-G16. The character "|" is not allowed.	ngn
RTP Name Fixed Part	The prefix of the RTP resource name.	RTP/
RTP Name Var Begin	The "RTP Name Var Begin" value must be smaller than the "RTP Name Var End" value. The value ranges from 0 to 65534, and the default value is 4000.	4000

Item	Description	Example
RTP Name Var End	The "RTP Name Var End" value must be larger than the "RTP Name Var Begin" value. The value ranges from 0 to 65534, and the default value is 9000.	9000
RTP Name Var Step	The increment for the variable part of the RTP resource name. The value ranges from 1 to 65534, and the default value is 1.	1
RTP Name Fixed Length	You can select "Fixed" or "Unfixed" for the length of the RTP resource name. The default setting is "Fixed", i.e., the variable part of the RTP name is filled with **0** so that the name has the fixed length.	Fixed
Digitmap Begin Timer (s)	The duration of waiting for the initial dial. The value ranges from 1 to 254, the default value is 16, and the unit is second.	16
Digitmap Short Timer (s)	The digit string has matched a numbering scheme of the DigitMap but with more digits it may match an alternative numbering scheme as well. Therefore, you need to configure the time of waiting to receive digits. The value ranges from 1 to 254, the default value is 4, and the unit is second.	4
Digitmap Long Timer (s)	When at least one digit is required to match any numbering scheme of DigitMap, you need to set the time of waiting for receiving the digit. The value ranges from 1 to 254, the default value is 16, and the unit is second.	16
Notify Match Each Map	The matching result will be reported as soon as the digit string matches any numbering scheme of DigitMap. The default setting is "Notify Match Only".	Notify Match Only
VBD State	Select whether to enable regulation of the "VBD Tx Interval (ms)" and the "VBD Rx Interval (ms)". The default setting is "Disable".	Disable
VBD Tx Interval (ms)	The interval for sending packets. The options include 10, 20, 30, 40, 50 and 60, the default value is 20, and the unit is millisecond.	20
VBD Rx Interval (ms)	The interval for receiving packets. The options include 10, 20, 30, 40, 50 and 60, the default value is 10, and the unit is millisecond.	10
VBD Voice Coder	Choose the speech encoding method used in the T.30 transparent transmission mode. The options include "G.711U", "G.711A", and "no change". The default setting is "no change".	G.711U
Offhook Warning Tone Timeout	Register the howler tone timeout function to stop playing the howler tone when the timer expires. The default setting is "Unregistered".	Unregistered
Flash Threshold (ms)	The FLASH low-pulse signal width. The value ranges from 90 to 2490, the default value is 90, and the unit is millisecond.	90
RFC2833 Nego state	Select whether to register the RFC2833 auto-negotiation function to encapsulate DTMF based on the RFC2833. The default setting is "Unregistered".	Unregistered

Item	Description	Example
Def RFC2833 PT	The default RFC2833 load type. The value range is 0 and 96 to 127. The default value is 97.	97
Def RFC2198 PT	The default RFC2198 load type. The value range is 0 and 96 to 127. The default value is 96.	96
T.38 Event Detect Mode	The T.38 event detection and report mode. The options include "normal", "only V21" and "all V21".	normal
Caller ID mode	The caller ID mode. The options include FSK and DTMF, and the default setting is FSK.	FSK
On Hook Detect Time (ms)	The polling check time for on-hook events. The value ranges from 100 to 2500, the default value is 600, and the unit is millisecond.	600
Dial Tone Timeout (s)	The dialing tone timeout value. The value ranges from 1 to 254, the default value is 60, and the unit is second.	60
No Answer Tone Timeout (s)	The ringing (no answer tone) timeout value. If the set period of time expires, it is considered that the phone is not answered. The value ranges from 1 to 254, the default value is 60, and the unit is second.	60
Busy Tone Timeout (s)	The busy tone timeout value. The value ranges from 1 to 254, the default value is 60, and the unit is second.	60
ROH Timeout (s)	The timeout value for the howler tone played after the busy tone. The value ranges from 1 to 254, the default value is 60, and the unit is second.	60
Retransmit Timeout (s)	The retransmission timeout value: The timer counts the time after the MG sends a request to the MGC; when the timer expires, the MG retransmits the request. The value ranges from 1 to 60, the default value is 25, and the unit is second.	25
EC Mode	The error correction function switch. When the function is enabled, the packets with errors will be corrected. The default setting is "Disable".	Enable
CLI Language	The CLI language used by the IAD; the options include Chinese and English.	English
NGN Register Timer Threshold (s)	The value ranges from 1 to 3600, the default value is 600, and the unit is second.	600
NGN Register User Threshold	The value ranges from 1 to 4096, and the default value is 1.	1
Alive Format	Two options are available: "Notify" and "Service Change". The default setting is "Notify".	Notify
3-Party Establishing Mode	The way to establish three-party calling.	0

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. Inthe **Operational Tree** pane, select **POTS Service→Softswitch Parameters Profile** to open the **Softswitch Parameters Profile** tab.
4. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a profile configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 6-8.

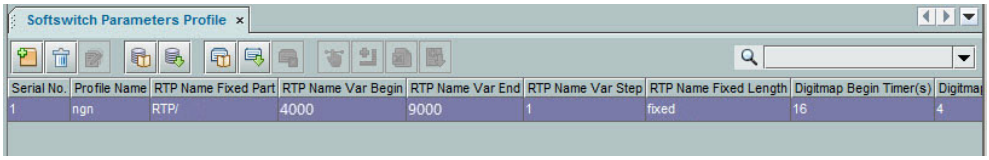


Figure 6-8 The Softswitch Platform Intercommunication Parameter Profile

6.2.1.2 Binding the IAD Softswitch Intercommunication Profile

Background Information

After configuring the Softswitch intercommunication profile, you need to bind the profile to the port of the GPON service card.

Planning Data

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	1

Item	Description	Example
ONU No.	The ONU authorization number. Configure this item according to the network planning of the operator.	1
Profile Name	Select the configured softswitch intercommunication profile to bind.	ngn

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **POTS Service→IAD Softswitch Profile Binding** to open the **IAD Softswitch Profile Binding** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a port binding entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 6-9.

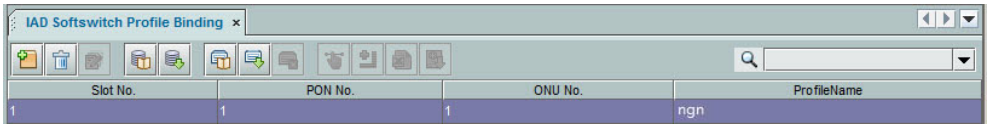


Figure 6-9 Binding the IAD Softswitch Intercommunication Profile

6.2.2 Configuring NGN Heartbeat Parameters

The following introduces how to configure the parameters of the heartbeat between the MG and the MGC.

Prerequisites

The **Keep Alive** in the **Uplink Interface** tab is set to **Enable Initiative** or **Enable Passive**.

Planning Data

Item	Description	Example
Signaling Service Name @ Interface ID	This item should be consistent with the Service Name set in **Local End Service Outer VLAN** and the Service Name set in **NGN Uplink Interface**.	H248@H248
Alive Interval (s)	The interval of sending keep-alive messages. The value ranges from 1 to 43200, the default value is 30, and the unit is second.	30
Alive Times	The maximum timeout times that the softswitch platform MGC allows for the ONU to send the keep-alive messages; if the value is exceeded, it is considered that the MGC loses its communication with the ONU. The value ranges from 1 to 120, and the default value is 3.	3

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **POTS Service→Keep Alive** to open the **Keep Alive** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 6-10.

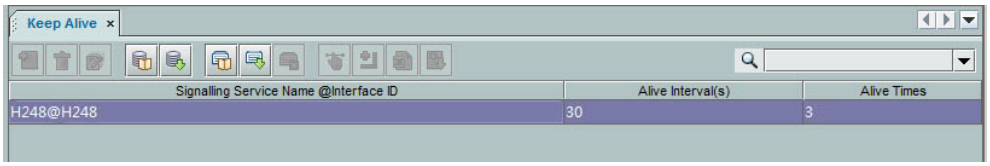


Figure 6-10 Configuring NGN Heartbeat Parameters

6.2.3 Configuring IAD MD5 Authentication

Prerequisites

The endpoint domain name has been configured on the **NGN Configuration** tab.

Planning Data

Item	Description	Example
Endpoint Domain Name	It should be consistent with the endpoint domain name configured on the **NGN Configuration** tab.	20.30.40.50
MD5 State	Configure this item according to the network planning of the operator.	Enable
MG ID	Configure this item according to the network planning of the operator.	123456
KEY	Configure this item according to the network planning of the operator.	123abc
DHG Value	Configure this item according to the network planning of the operator.	2
DHP Value	Configure this item according to the network planning of the operator.	FFFFFFFFFFFFFFFFA63A3620F44C42E9625E7EC6E485B5766D51C2454FE1356DF25F1437302B0A6DCD3A431BEF9519B38E3404DD514A08793B139B22020BBEA68A67CC7429024E0880DC1CD1C4C6628B2168C234C90FDAA2FFFFFFFFFFFFFFFF

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **POTS Service→IAD MD5 Configuration** to open the **IAD MD5 Configuration** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.

6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 6-11.

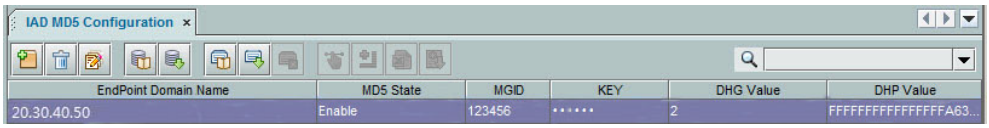


Figure 6-11 Configuring the IAD MD5 Authentication

6.2.4 Configuring the Digitmap

The digitmap can be configured when the protocol SIP is used. In course of dialing, the gateway matches the dialed digits against the numbering scheme in the digitmap and reports to the Softswitch or IMS when a match is found.

Note:

Please configure the digitmap according to the practical project conditions to allow quick match of the digits.

Prerequisites

The VoIP service has been started up, and the configuration of the softswitch intercommunication profile has been completed.

Planning Data

Item	Description	Example
Digitmap	Configure this item according to the network planning of the operator.	[0-9ABCD].|[EF][0-9ABCDEF].

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **POTS Service→Default DigitMap** to bring up the **Default DigitMap** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 6-12.

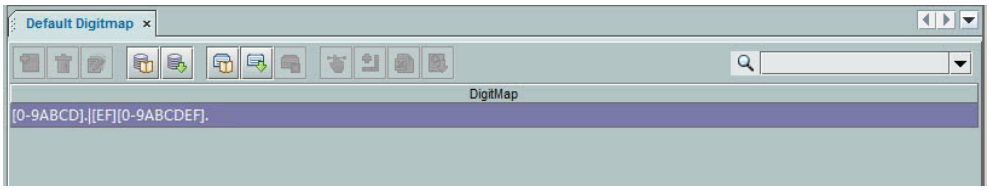


Figure 6-12 Digitmap

7 Configuring Data Services

The following introduces how to configure data services for the AN6001-G16 using examples.

- ☑ Example of Data Service Configuration in the Transparent / TAG Mode
- ☑ Example of Data Service Configuration in the VLAN Translation Mode
- ☑ Example of Data Service Configuration in the Selective QinQ Mode

7.1 Example of Data Service Configuration in the Transparent / TAG Mode

In this example, data service configuration for an individual device is described.

7.1.1 Network Scenario

Service Planning

- The subscribers are accessed via the ONUs.
- The subscriber services include IPTV, broadband Internet services and so on, which have high requirement on bandwidth.
- The QinQ transparent transmission or TAG mode is applied to the subscriber packets, with the outer VLAN identifying services and the inner VLAN identifying subscribers.

Network Diagram

Figure 7-1 shows the network diagram for the data service.

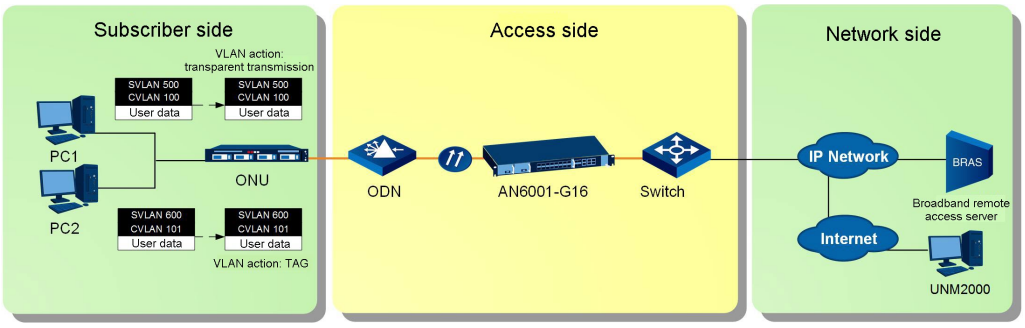


Figure 7-1 Network Diagram for Data Services in the Transparent / TAG Mode

7.1.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

Figure 7-2 shows the flow of configuring data services individually in the transparent / TAG mode.

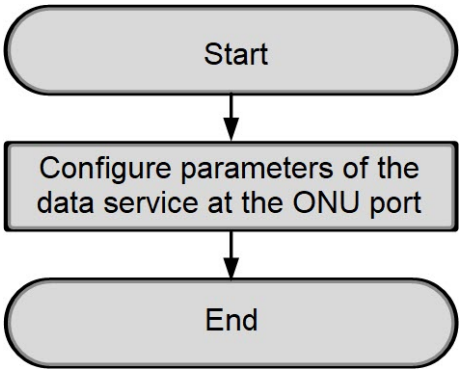


Figure 7-2 Flow of Configuring Data Services in the Transparent / TAG Mode

7.1.3 Configuring Parameters of Data Services at the ONU Ports

The following introduces how to configure the parameters of services at each LAN port of the ONU, including VLAN settings, service mode, priority level and protocol identifier.

Configuration Rules

The VLAN ID of the ONU ranges from 1 to 4085.

- To add stacked VLAN tags to the data service, make sure the SVLAN ID is within the range of the local end VLAN.
- To add a single VLAN tag to the data service, make sure the CVLAN ID is within the range of the local end VLAN.

Planning Data

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	3
ONU No.	The authorization number of the ONU.	1

Item			Description	Example	
Port No.			The number of the ONU port actually used.	LAN1	
Basic Information	Enable Port		Configure this item according to the operator’s network planning. The default setting is "Enable".	Enable	
	Enable Flow Control		Configure this item according to the operator's network planning. The default setting is "Disable".	Disable	
	Port Auto Negotiation		Configure this item according to the operator’s network planning. The default setting is "Enable".	Enable	
Service Configuration	Basic Information	TLS	Configure this item according to the network planning of the operator. Select "TLS" or "Non TLS".	Non TLS	
		Service Type	Select "Unicast".	Unicast	
		CVLAN Mode	Configure this item according to the network planning of the operator. Select "Tag" or "Transparent".	Transparent	Tag
		CVLAN ID	Configure this item according to the network planning of the operator. The value ranges from 1 to 4085.	100	101
		Priority or COS	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	7	
		TPID	The CVLAN tag protocol identifier. The default setting is 33024.	33024	
		ISP VLAN	VLAN ID of the ISP service.	-	
		ISP COS	Priority of the ISP service.	-	
		Up Bandwidth Profile	The service uplink bandwidth profile, used for restricting the uplink bandwidth.	-	
		Down Bandwidth Profile	The service downlink bandwidth profile, used for restricting the downlink bandwidth.	-	
		Data Service Type	Select the data service bandwidth type.	-	
		Priority Queue	Configure the priority queue. The value ranges from 0 to 7, and the default value is 0.	-	

Item			Description	Example	
		GEM Port	Configure the GEM port. The value ranges from 0 to 4095, and the default value is 0.	-	
	QinQ Settings	Enable QinQ Status	Enables / disables the QinQ.	Enable	
		QinQ Profile	The QinQ configuration profile, recommended for batch configuration.	-	
		Service Name	Select the service name configured in the local end VLAN.	DATA	
		SVLAN ID	Configure the SVLAN ID according to the network planning of the operator. The value ranges from 1 to 4085.	500	600
		Priority or COS	The SVLAN priority. The value ranges from 0 to 7, with 7 standing for the highest priority level, and 0 the lowest one.	7	
		TPID	The default value is 33024.	33024	

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click the ONU to be configured, and select **Port Service Config** from the shortcut menu that appears to bring up the **Port Service Config** tab.
4. Select the LAN port to be configured from **Data Port**. Then select the **Service Configuration** tab on the right pane, click **Add**, and enter the desired number in the **Enter the number of rows to add** dialog box that appears according to the planning data, as shown in Figure 7-3. Click **OK**.

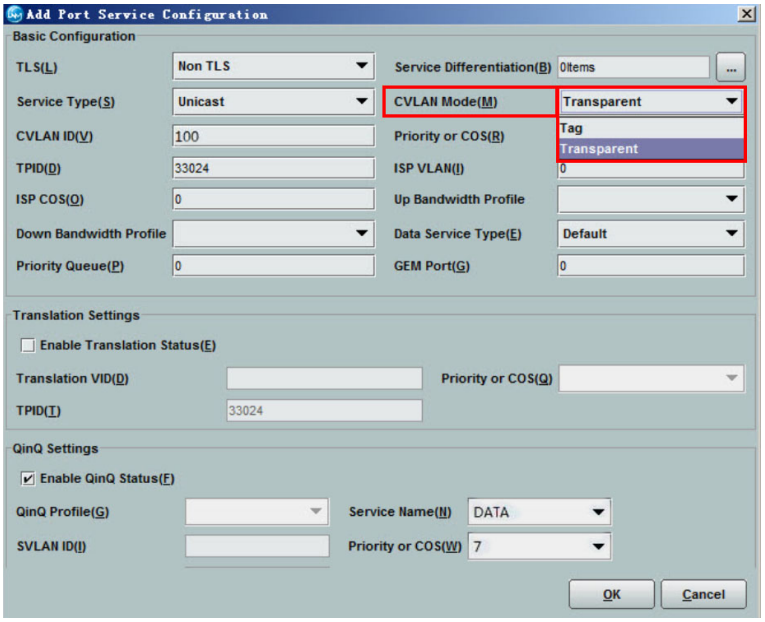


Figure 7-3 Adding Service to a Port

5. Configure the other LAN ports respectively following Step 4.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 7-4.

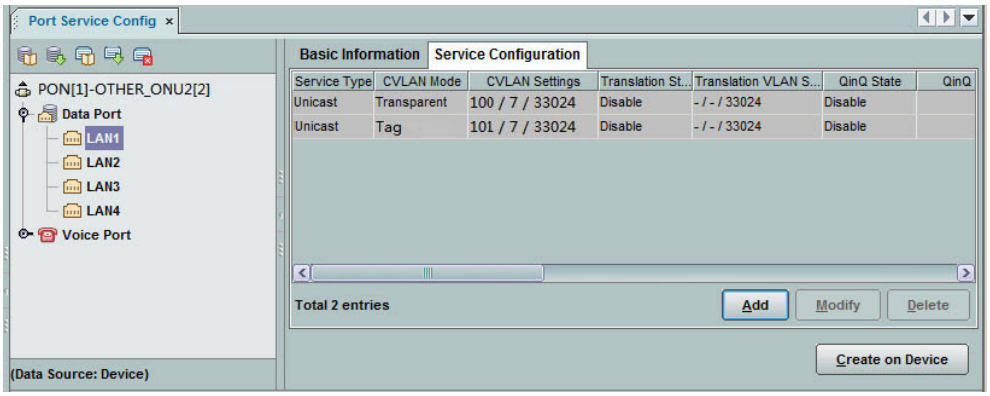


Figure 7-4 Service Configuration

7.1.4 Configuration Result

The subscribers connected with the ONU can access the network.

7.2 Example of Data Service Configuration in the VLAN Translation Mode

The following uses an example to introduce how to configure data services in the VLAN N:1 translation mode individually. The data services in the VLAN 1:1 translation mode are configured likewise.

7.2.1 Network Scenario

Service Planning

The subscriber PCs are connected to the ONU via home gateways. The home gateways add different VLAN tags to the subscribers' packets, and then transmit the packets to the ONU. The ONU translates the varied VLAN IDs into 1000 and sends the packets to the AN6001-G16. The AN6001-G16 then adds the SVLAN to the subscribers' packets and sends them to the upper layer network.

Network Diagram

The network diagram for the data service in the VLAN translation mode is shown in Figure 7-5.

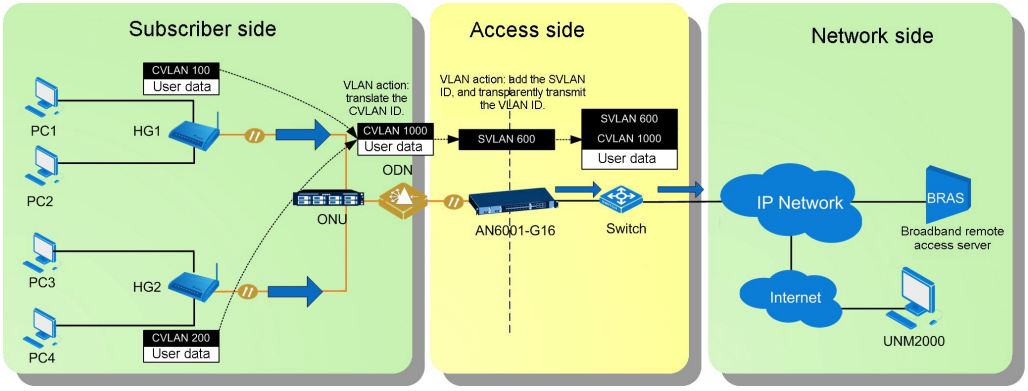


Figure 7-5 Network Diagram for Data Services in the VLAN N:1 Translation Mode

- In the uplink direction, the data services uploaded by the two subscriber PCs are added with different CVLAN IDs by the home gateways and uplinked to the ONU. The ONU translates the CLVAN IDs and transmits the data services to the AN6001-G16 via the splitters. The AN6001-G16 adds SVLAN IDs to the data services and transmits the data services to the providers network via the uplink interface.
- In the downlink direction, the data services carrying stacked VLAN tags pass by the AN6001-G16. The AN6001-G16 strips the SVLAN tags off the data, and transmits the data services to the ONU via the splitter. The ONU translates the CVLAN tags and sends the data services to the corresponding HGs. The HGs strip the CVLAN tags off the data and transmit the data to the subscriber PCs.

7.2.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

The flow of configuring data services individually in the VLAN N:1 translation mode is shown in Figure 7-6.

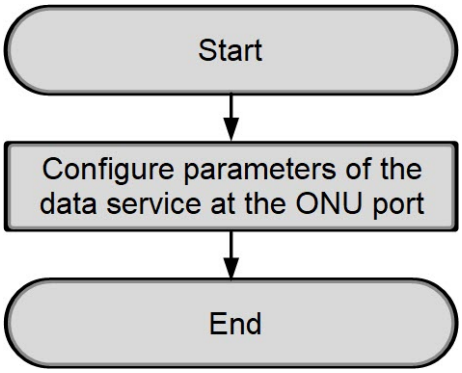


Figure 7-6 Flow of Configuring Data Services in the VLAN N:1 Translation Mode Individually

7.2.3 Configuring Parameters of Data Services at the ONU Ports

The following introduces how to configure the parameters of services at each LAN port of the ONU, including VLAN settings, service mode, priority level and protocol identifier.

Configuration Rules

The VLAN ID of the ONU ranges from 1 to 4085.

- To add stacked VLAN tags to the data service, make sure the SVLAN ID is within the range of the local end VLAN.
- To add a single VLAN tag to the data service, make sure the CVLAN ID is within the range of the local end VLAN.

Planning Data

Item			Description	Example	
Slot No.			The number of the slot housing the card connected to the ONU.	1	
PON No.			The number of the PON port connected to the ONU.	3	
ONU No.			The ONU authorization number. Configure this item according to the network planning of the operator.	1	
Port No.			The number of the ONU port actually used.	LAN1	LAN2
Basic Information	Enable Port		Configure this item according to the operator’s network planning. The default setting is "Enable".	Enable	
	Enable Flow Control		Configure this item according to the operator's network planning. The default setting is "Disable".	Disable	
	Port Auto Negotiation		Configure this item according to the operator’s network planning. The default setting is "Enable".	Enable	
Service Configura-tion	Basic Information	TLS	Configure this item according to the network planning of the operator. Select "TLS" or "Non TLS".	Non TLS	
		Service Type	Select "Unicast".	Unicast	

Item			Description	Example	
		CVLAN Mode	Configure this item according to the network planning of the operator. Select "Tag" or "Transparent".	Transparent	
		CVLAN ID	Configure this item according to the network planning of the operator. The value ranges from 1 to 4085.	100	200
		Priority or COS	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	0	
		TPID	The CVLAN tag protocol identifier. The default setting is 33024.	33024	
	Translation Settings	Enable Translation Status	Configure this item according to the network planning of the operator.	Enable	
		Translation VID	The translated VLAN ID. Configure this item according to the network planning of the operator. The value ranges from 1 to 4085.	1000	
		Priority or COS	The priority of the translated VLAN. The value ranges from 0 to 7, with 7 standing for the highest priority, and 0 the lowest one.	0	
		TPID	The translated VLAN tag protocol identifier. The default setting is 33024.	33024	

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click the ONU to be configured, and select **Port Service Config** from the shortcut menu that appears to bring up the **Port Service Config** tab.
4. Select the LAN port to be configured from **Data Port**. Then select the **Service Configuration** tab on the right pane, click **Add**, and enter the desired number in the **Enter the number of rows to add** dialog box that appears according to the planning data, as shown in Figure 7-7. Click **OK**.

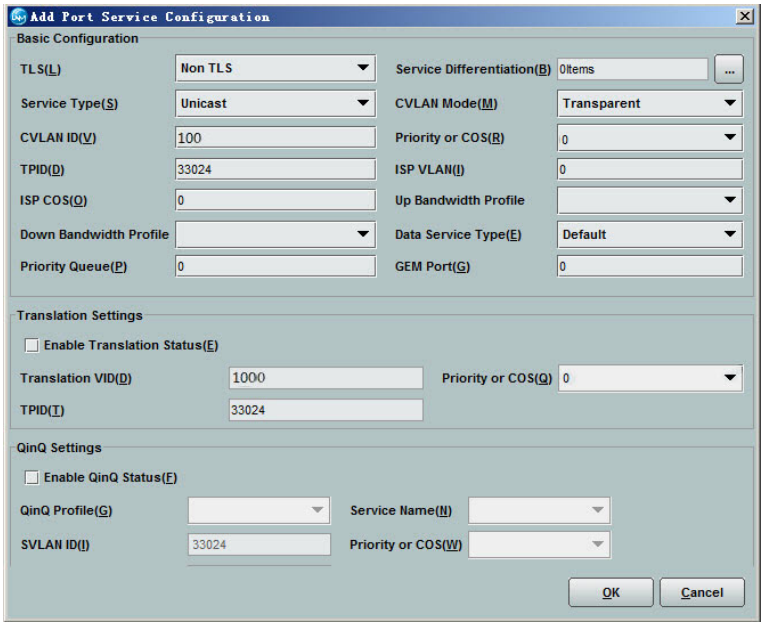


Figure 7-7 Adding Service to a Port

5. Configure the other LAN ports respectively following Step 4.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 7-8.

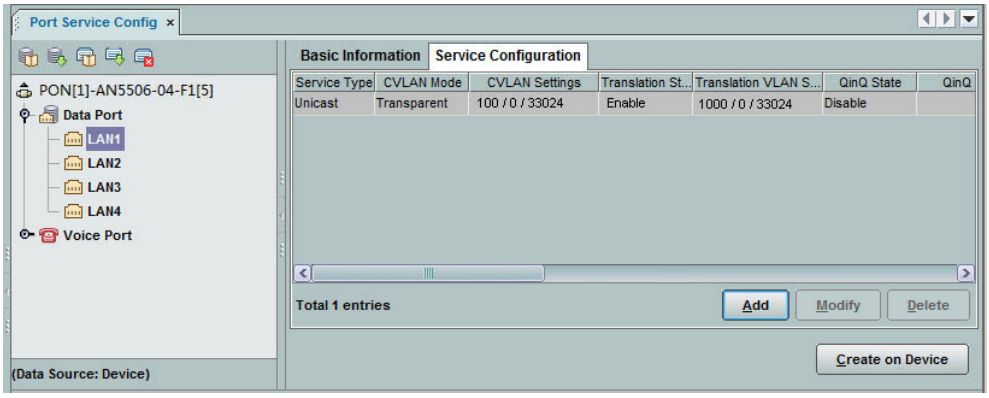


Figure 7-8 Service Configuration

7.2.4 Configuration Result

The subscribers connected with the ONU can access the network.

7.3 Example of Data Service Configuration in the Selective QinQ Mode

The following uses an example to introduce how to configure the data service in the selective QinQ mode.

7.3.1 Network Scenario

Service Planning

When enabled with the selective QinQ function, the AN6001-G16 can add VLAN IDs flexibly to subscriber services according to the service type, MAC address and other information.

Network Diagram

The network diagram for the data service in the selective QinQ mode is shown in Figure 7-9.

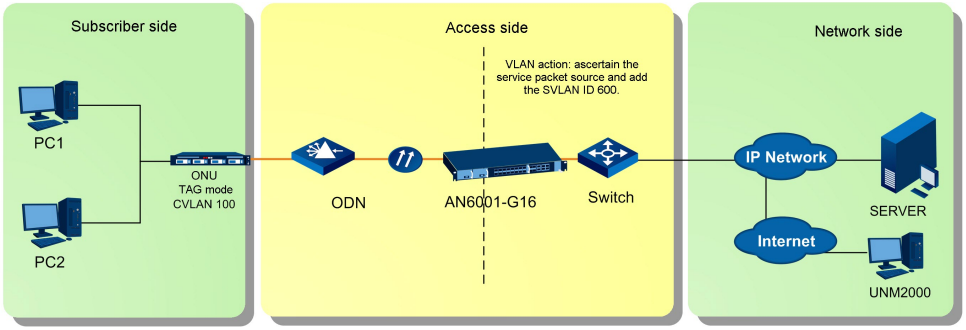


Figure 7-9 Network Diagram for the Data Service in the Selective QinQ Mode

- In the uplink direction, the data services uploaded by the subscriber PCs are added with a CVLAN tag by the ONU and then transmitted to the AN6001-G16 via the splitter. The AN6001-G16 classifies the data service flow received, adds an SVLAN tag to the service flow with the corresponding source MAC address, and transmits the service flow to the providers network via the uplink port.

- In the downlink direction, the data services carrying two VLAN tags pass through the AN6001-G16. The AN6001-G16 classifies the data service flow and strips the SVLAN tag from the service flow with the corresponding source MAC address and transmits the data to the ONU via the splitter. The ONU strips the CVLAN tag and transmits the data to the subscriber PCs.

7.3.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

Figure 7-10 shows the flow of configuring data services individually in the selective QinQ mode.

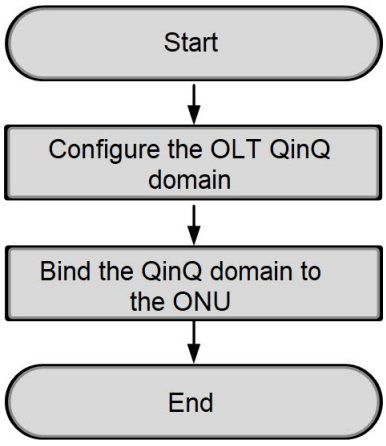


Figure 7-10 Flow of Configuring Data Services in the Selective QinQ Mode Individually

7.3.3 Configuring the OLT QinQ Domain

The items to be configured for local end QinQ domain include service type, stacked VLAN related parameters and uplink / downlink rule clause.

Planning Data

Item		Description	Example
Domain Name		The name of selective QinQ domain.	abc
Upstream Rule Clause	Rule Type	Configure this item according to the network planning of the operator.	Source MAC Address
	Operator	Configure this item according to the network planning of the operator.	Match If Present
	Rule Value	Configure this item according to the network planning of the operator.	00-11-22-33-44-55
Downstream Rule Clause	Rule Type	Use the default setting.	Source MAC Address
	Operator	Use the default setting.	Never Match
	Rule Value	Use the default setting.	00-00-00-00-00-00
Old_CVLAN Low	Old_CVLAN Low	The CVLAN ID transparently transmitted.	100
	Old_ CVLANCoslow	The priority of the transparently transmitted CVLAN ID. The value ranges from 0 to 7, with 7 stands for the highest priority, and 0 the lowest one.	0
	Action	If **Old_CVLAN Low** is configured, you can set the action to **Transparent** or **Translation**; if **Old_ CVLAN Low** is not configured, you can set the action to **Transparent** or **Add**.	Transparent
	TPID	The default value is 33024.	33024
Old_CVLAN High	Action	Select **Add**.	Add
	TPID	The default value is 33024.	33024
	COS	The SVLAN priority. The value ranges from 0 to 7, with 7 standing for the highest priority level, and 0 the lowest one.	0
	New VID	The SVLAN ID.	600

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **VLAN Service→QinQ→QinQ Domain** to open the **QinQ Domain** tab.

4. Select the left pane, click **Add**, enter **1** in the dialog box that appears, and then click **OK** to add a QinQ domain configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 7-11.

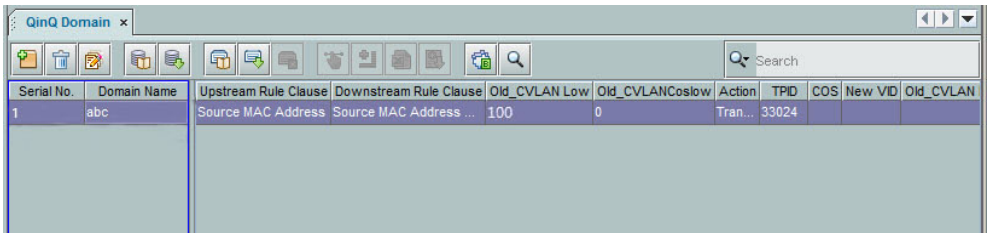


Figure 7-11 Configuring the OLT QinQ Domain in the Selective QinQ Mode

7.3.4 Binding the QinQ Domain to the ONU

Bind the PON port to the OLT QinQ domain to apply the configured QinQ rules to the PON port.

Planning Data

Table 7-1 Planning Data for Configuring Data Services in the Selective QinQ Mode

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU. Read only.	1
PON No.	The number of the PON port connected to the ONU. Read only.	1 to 16
Action	Bind the QinQ domain to PON ports.	Attach
Domain Name	The bound QinQ domain.	abc

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree**, select **Common Config→PON→PON Attach/Detach Domain** to bring up the **PON Attach/Detach Domain** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 7-12.

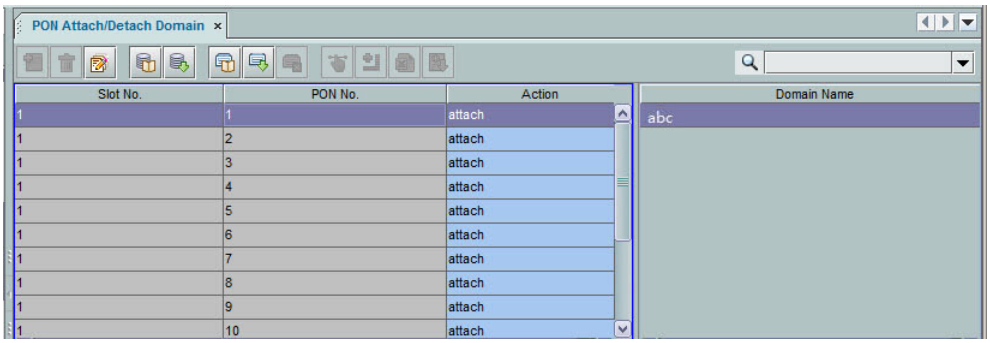


Figure 7-12 Binding the PON Port to the QinQ Domain in the Selective QinQ Mode

7.3.5 Configuration Result

The subscribers connected with the ONU can access the network.

8 Configuring the Multicast Service

The following introduces how to configure the multicast service for the AN6001-G16.

- Multicast Service Configuration Example
- Example of Configuring the SSM Service
- Optional Functions

8.1 Multicast Service Configuration Example

The following uses an example to introduce how to configure the multicast service in the proxy-snooping mode. The multicast services in other multicast modes are configured likewise.

8.1.1 Configuration Rules

The following describes the rules for global configuration of the multicast service for the AN6001-G16:

- When the multicast mode is disabled, the multicast subscribers cannot watch the programs in the multicast VLAN.
- The AN6001-G16 supports processing multicast protocol packets (including those requesting joining / leaving a multicast group and those for querying).
- The AN6001-G16 supports VLAN adding or translation for the subscriber protocol packets.
- The multicast mode cannot be switched directly. You should switch the current mode to **Disable** first and then switch to another mode.
- The multicast mode is based on the VLAN. Different multicast modes can be set for different VLANs on the same equipment.
- Generally, default values can be used for the parameters in common or special multicast queries.

8.1.2 Network Scenario

Service Planning

Two subscribers are connected to the GPON ONU, and they can use the set top boxes (STB) to watch IPTV programs. The service in this case is the multicast service in the proxy-snooping mode. Accordingly, the AN6001-G16 should work in the proxy-snooping mode.

Network Diagram

Figure 8-1 shows the network diagram for the multicast services implemented by the AN6001-G16 in the proxy-snooping mode.

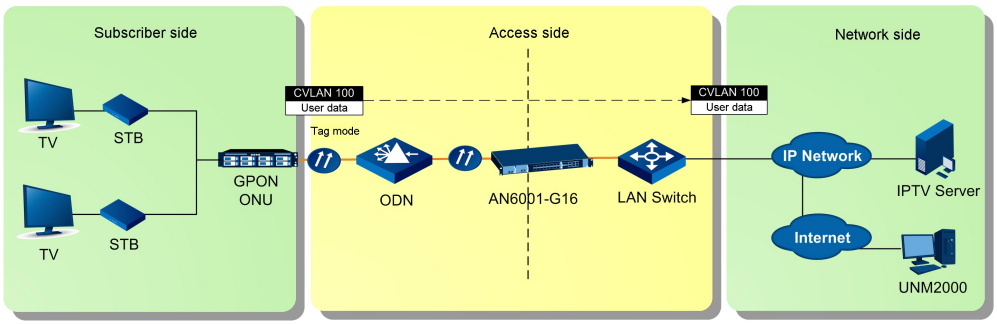


Figure 8-1 Network Diagram for the Multicast Service in the Proxy-snooping Mode

- In the downlink direction, the ONU strips the tag from the multicast stream (VLAN ID=100) on the AN6001-G16 side, and transmits the stream to the set top box. Then the set top box forwards the stream to video subscribers.
- In the uplink direction, the ONU attaches the tag (VLAN ID=100) to the joining / leaving multicast protocol packets received from the set top box, and transmits the packets to the AN6001-G16. The AN6001-G16 then forwards the protocol packets to the IPTV server.

8.1.3 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

The flow of configuring multicast services is shown in Figure 8-2.

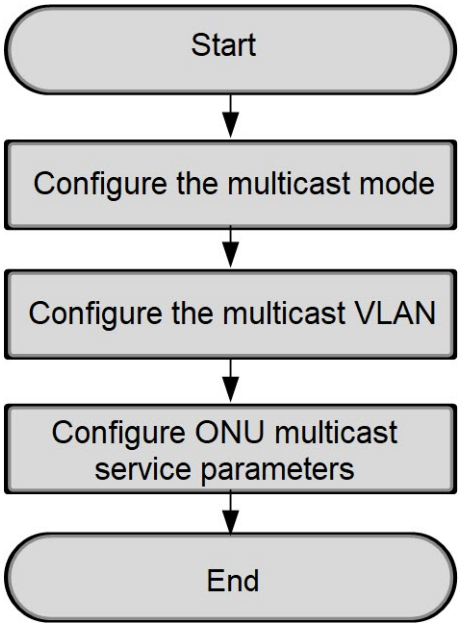


Figure 8-2 Flow of Configuring Multicast Services

8.1.4 Configuring the Multicast Mode

Configure the multicast mode for the AN6001-G16.

Background Information

- In the proxy-snooping mode, the core switch card works in the proxy mode, while the GPON interface card works in the snooping mode. In this way, the proxy mode and the snooping mode are combined.
- In the multicast proxy mode, the equipment serves as a multicast server from the view of users; while from the view of the upper layer network, the equipment serves as a multicast user. The proxy mode helps reduce the multicast protocol message flow on the network side.
- In the multicast snooping mode, the OLT equipment snoops on the messages of communication between users and the multicast router to obtain the information concerned and maintain the multicast forwarding table. The equipment does not process the multicast packets from the multicast VLAN but transmits them transparently.

- In the controlled mode, the AN6001-G16 controls the multicast programs sent to the ONU according to the white list. The ONU does not receive the multicast programs that are not on the white list.

Planning Data

Item	Description	Example
IGMP Mode	Configure this item according to the network planning of the operator.	Proxy-Snooping Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→IGMP Param. Config→IGMP Mode** to access the **IGMP Mode** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-3.

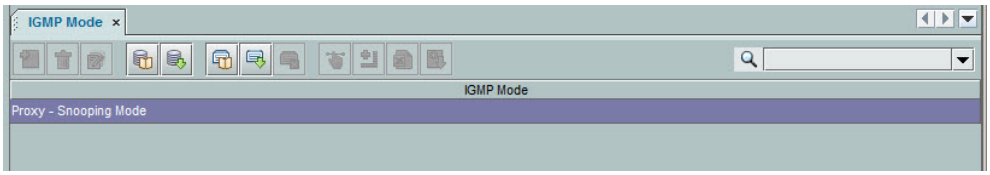


Figure 8-3 Configuring the Multicast Mode

8.1.5 Configuring the Multicast VLAN

Configure the default VLAN for the multicast services of the AN6001-G16.

Configuration Rules

- The multicast VLAN should be within the range of the local end VLAN.

- A multicast program can belong to only one multicast VLAN, while a multicast VLAN can contain a multicast program or a multicast program group (a collection of multicast programs subject to the same management authority).

Planning Data

Item	Description	Example
VLAN	Configure this item according to the network planning of the operator. The multicast VLAN should be within the range of the local end VLAN.	100

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→Multicast VLAN→ Multicast VLAN** to bring up the **Multicast VLAN** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-4.

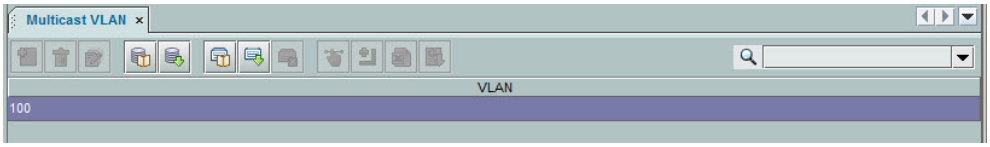


Figure 8-4 Configuring the Multicast VLAN

8.1.6 Configuring the Port Service VLAN

Configure the parameters of the multicast service at the ONU data port.

Precautions

You need not configure VLAN CoS for multicast services. The CoS of the downlink multicast stream is carried by the multicast stream and cannot be modified on the AN6001-G16 or ONU. The CoS of the uplink / downlink multicast protocol packets is 0 by default.

Planning Data

Item	Description	Example	
Slot No.	The number of the slot housing the card connected to the ONU.	2	
PON No.	The number of the PON port connected to the ONU.	2	
ONU No.	The ONU authorization number. Configure this item according to the network planning of the operator.	1	
ONU Port No.	The number of the ONU port actually connected.	LAN1	LAN2
Service Type	Select "Multicast" for the multicast service.	Multicast	
CVLAN Mode	Configure this item according to the network planning of the operator. Two options are available: "Tag" and "Transparent". In the "Tag" mode, the downlink multicast data stream is stripped of tag when it passes the ONU port. In the "Transparent" mode, the downlink multicast data stream is transparently transmitted.	Tag	
CVLAN ID	The VLAN ID carried by the downlink multicast data stream. Configure this item according to the network planning of the operator.	100	

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click the ONU to be configured, and select **Port Service Config** from the shortcut menu that appears to bring up the **Port Service Config** tab.

4. Select the LAN port to be configured from **Data Port**. Then select the **Service Configuration** tab on the right pane, click **Add**, and enter the desired number in the **Enter the number of rows to add** dialog box that appears according to the planning data, as shown in Figure 8-5. Click **OK**.

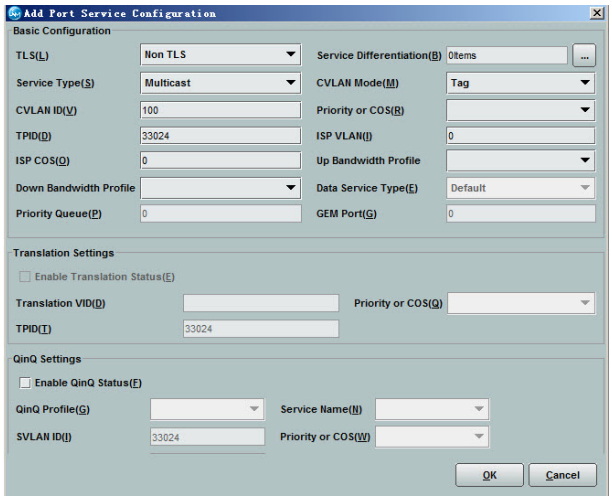


Figure 8-5 Adding Service to a Port

5. Configure the other LAN ports respectively following Step 4.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-6.

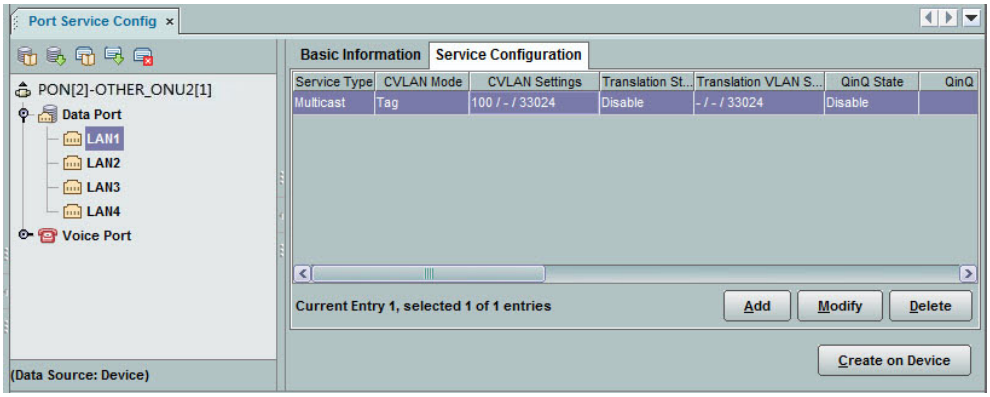


Figure 8-6 Service Configuration at the Port Completed

8.1.7 Configuration Result

The multicast services on the LAN1 and LAN2 ports of the ONU are started up, and subscribers can watch the video programs whose multicast VLAN is 100 normally.

8.2 Example of Configuring the SSM Service

The following introduces how to configure the SSM multicast service using an example.

8.2.1 Network Diagram

Service Planning

A subscriber needs to watch the IPTV programs in the SSM mode using the set top box. The subscriber is connected to the OLT equipment AN6001-G16 via an ONU.

Network Diagram

The network diagram for the SSM service is shown in Figure 8-7.

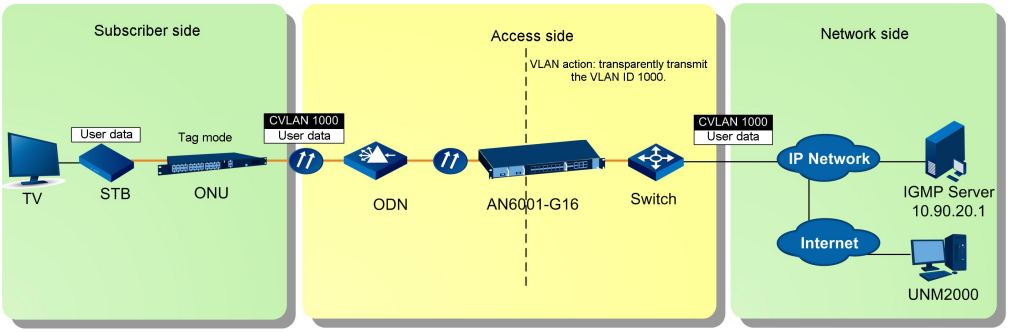


Figure 8-7 Network Diagram for Configuring the SSM Service

- In the downlink direction, the multicast shortest path tree (SPT) is set up between the multicast source and the AN6001-G16. The multicast source 10.90.20.1 provides special source multicast service for the subscribers connected with the AN6001-G16. The ONU strips the VLAN tag from the multicast packets and then forwards the packets to the set top box on the subscriber side.
- In the uplink direction, the ONU adds the tag to the joining / leaving multicast protocol packets received from the set top box, and sends the packets to the AN6001-G16. Then the AN6001-G16 forwards the protocol packets to the IPTV server.

8.2.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

The flow of configuring the SSM service is shown in Figure 8-8.

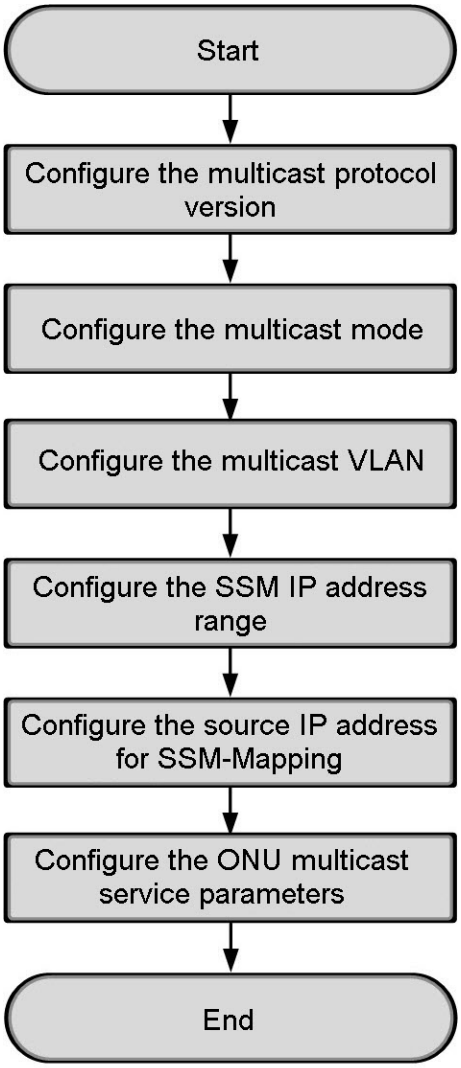


Figure 8-8 Network Diagram for Configuring the Mulitcast Service Individually in the SSM Translation Mode

8.2.3 Configuring the Multicast Protocol Version

Configure the IGMP protocol version used by the AN6001-G16. The options include v1, v2 and v3. When SSM is configured, the IGMP protocol version is IGMP v3.

Planning Data

Item	Description	Example
Igmp version	Configure this item according to the network planning of the operator.	IGMP V3

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→IGMP Param. Config→MLD Version** to access the **MLD Version** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-9.

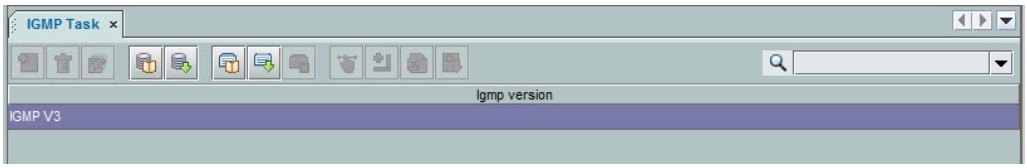


Figure 8-9 Configuring the Multicast Protocol Version

8.2.4 Configuring the Multicast Mode

Configure the multicast mode for the AN6001-G16.

Planning Data

Item	Description	Example
IGMP Mode	Configure this item according to the network planning of the operator.	Proxy-Proxy Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→IGMP Param. Config→IGMP Mode** to access the **IGMP Mode** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-10.

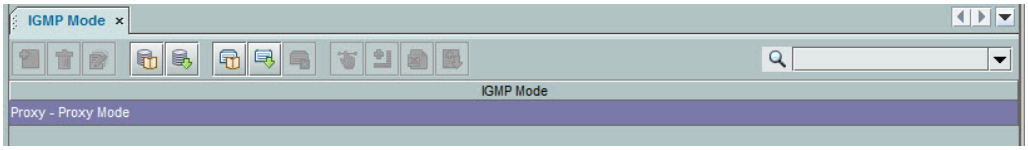


Figure 8-10 Configuring the Multicast Mode - SSM

8.2.5 Configuring the Multicast VLAN

Configure the default VLAN for the multicast services of the AN6001-G16.

Configuration Rules

- The multicast VLAN should be within the range of the local end VLAN.
- A multicast program can belong to only one multicast VLAN, while a multicast VLAN can contain a multicast program or a multicast program group (a collection of multicast programs subject to the same management authority).

Planning Data

Item	Description	Example
VLAN	Configure this item according to the network planning of the operator. The multicast VLAN should be within the range of the local end VLAN.	1000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→Multicast VLAN→Multicast VLAN** to bring up the **Multicast VLAN** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-11.

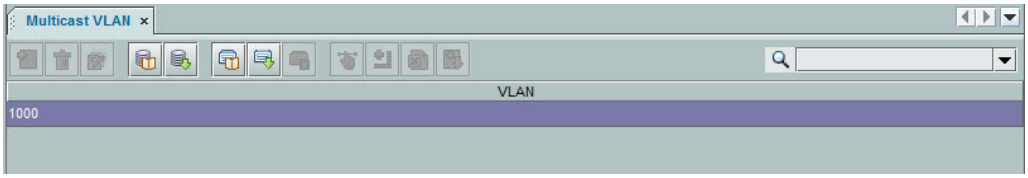


Figure 8-11 Configuring the Multicast VLAN - SSM

8.2.6 Configuring the SSM IP Address Range

Configure the range of the multicast IP address to start up a specific source multicast mode.

Planning Data

Item	Description	Example
SSM Ip Address Range	Configure this item according to the network planning of the operator.	IPv4:225.0.0.1/255.255.0.0

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Multicast Service→Multicast IP→IGMP SSM IP Address Range**to open the **IGMP SSM IP Address Range** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-12.

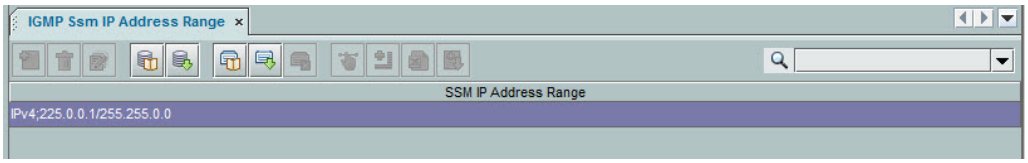


Figure 8-12 Configuring the SSM IP Address Range

8.2.7 Configuring the Source IP Address for SSM-Mapping

Configure the static SSM policy. When the client end VOD program does not support the IGMPv3, the multicast messages are forwarded based on the source specific multicast (SSM) IP address.

Configuration Rules

When configuring the source IP address of the multicast SSM-Mapping, set the IP address to the unicast IP address; when configuring the multicast SSM destination IP address range, set the IP address to the multicast IP address.

Planning Data

Item	Description	Example
SSM-Mapping IP Address	Configure this item according to the network planning of the operator.	IPv4:10.90.20.1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Multicast Service→Multicast IP→IGMP SSM-Mapping Source IP Address**to open the **IGMP SSM-Mapping Source IP Address** tab.
4. Click **Add** on the toolbar, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-13.

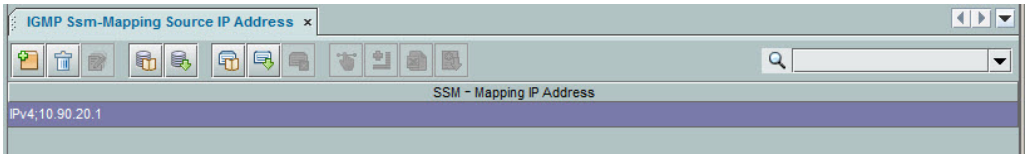


Figure 8-13 Configuring the Source IP Address for SSM-Mapping

8.2.8 Configuring ONU Multicast Service Parameters

Configure the VLAN for the multicast data traffic and that for the uplink / downlink multicast protocol messages. Configure ONU multicast service parameters, including multicast service type, VLAN mode, CVLAN ID and priority.

Precautions

You need not configure VLAN CoS for multicast services. The CoS of the downlink multicast stream is carried by the multicast stream and cannot be modified on the AN6001-G16 or ONU. The CoS of the uplink / downlink multicast protocol packets is 0 by default.

Planning Data

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	1
ONU No.	The ONU authorization number. Configure this item according to the network planning of the operator.	1

Item	Description	Example
Port No.	The number of the ONU port actually connected.	LAN1
Service Type	Select **Multicast** for the multicast service.	Multicast
CVLAN Mode	Configure this item according to the network planning of the operator.	Tag
CVLAN ID	The VLAN ID prior to translation when the translation function is enabled. It is unconfigurable when the CVLAN mode is set to "Untag". The value ranges from 1 to 4085.	1000
Priority or COS	The priority of the VLAN before translation. The value ranges from 0 to 7, with 7 standing for the highest priority, and 0 the lowest one.	5

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click the ONU to be configured, and select **Port Service Config** from the shortcut menu that appears to bring up the **Port Service Config** tab.
4. Select the LAN port to be configured from **Data Port**. Then select the **Service Configuration** tab on the right pane, click **Add**, and enter the desired number in the **Enter the number of rows to add** dialog box that appears according to the planning data, as shown in Figure 8-14. Click **OK**.

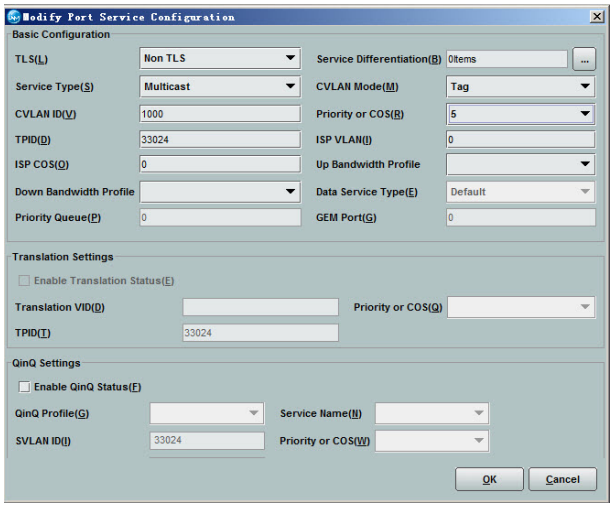


Figure 8-14 Adding Service Configuration to the Port - SSM

5. Click the **Create on Device** button to complete the configuration, as shown in Figure 8-15.

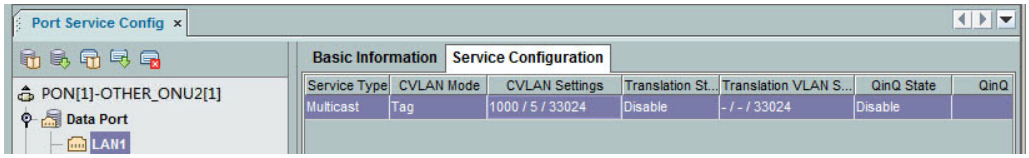


Figure 8-15 Configuring ONU Multicast Service Parameters - SSM

8.2.9 Configuration Result

The multicast services on the LAN1 port of the ONU are started up, and the subscribers can watch the video programs whose multicast VLAN is 1000 normally via the set top box.

8.3 Optional Functions

The following introduces how to configure multicast related optional functions provided by the equipment.

8.3.1 Configuring the Multicast Cascade Port

When the equipment is cascaded with other equipment to provide the multicast service, users should set the uplink port connected to the cascaded equipment as the cascade port.

Planning Data

Item	Description	Example
Cascade Ports No.	Configure this item according to the network planning of the operator.	19:SFP+1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→IGMP Cascade Ports**to open the **IGMP Cascade Ports** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click OK to add a multicast cascade port entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 8-16.

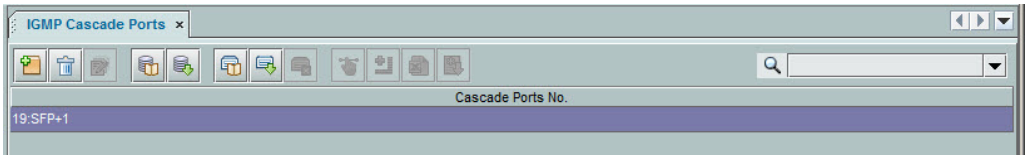


Figure 8-16 Configuring the Multicast Cascade Port

8.3.2 Configuring Maximum Multicast Bandwidth of Uplink Ports

Configure the maximum bandwidth of the uplink ports for multicast services.

Planning Data

Item	Description	Example
Uplink Bandwidth (Kbit/s)	Configure this item according to the operator's network planning. The default value is 0.	60000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→IGMP Cascade Ports**to open the **IGMP Cascade Ports** tab.
4. Click the **Max Uplink IGMP Bandwidth** tab in the lower part.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 8-17.

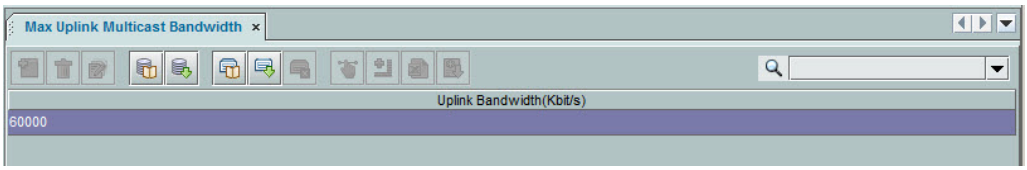


Figure 8-17 Configuring Maximum Multicast Bandwidth of Uplink Ports

8.3.3 Configuring ONU Multicast Parameters

Configure the ONU multicast parameters.

Planning Data

Item	Description	Example
Slot No.	The number of the slot housing the card connected to the ONU.	1
PON No.	The number of the PON port connected to the ONU.	3
ONU Authorized No.	The authorization number of the ONU.	1

Item	Description	Example
Leave Mode	Configure the way in which the users under the ONU ports leave the multicast group according to the network planning of the operator. The options include **FAST LEAVE** and **NON FAST LEAVE**.	NON FAST LEAVE
Robustness count	The times of sending multicast downlink query messages by the ONU. The value ranges from 0 to 12, and the default value is 2.	2
Last Member Query Count	The times of sending specific group query messages by the ONU. The value ranges from 0 to 12, and the default value is 2.	2
IGMP Mode	The multicast mode of the ONU. The options include **snooping mode**, **proxy mode** and **controlled mode**.	proxy mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select**Multicast Service→ONU Configuration** to open the **ONU Configuration** tab.
4. Click **Add**, and enter **1** in the dialog box that appears to add an ONU multicast parameter configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 8-18.

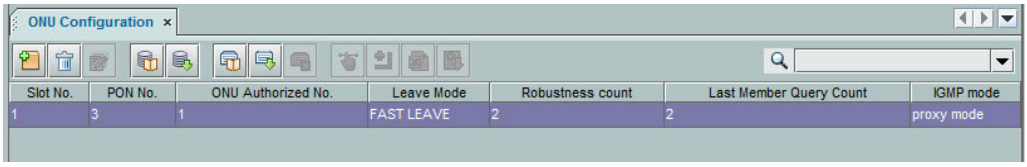


Figure 8-18 Configuring ONU Multicast Parameters

8.3.4 Configuring the Prejoin Group

Save the prejoined multicast program flows to uplink ports, so that subscribers can have quick access to the programs on demand.

Planning Data

Item	Description	Example
Prejoin Group	Configure this item according to the network planning of the operator.	224.0.1.1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Multicast Service→Multicast Profile & Port→Prejoin Groups** to access the **Prejoin Groups** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a prejoin group configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 8-19.

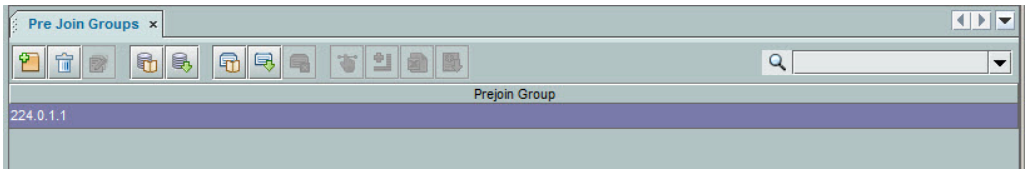


Figure 8-19 Configuring the Prejoin Group

8.3.5 Configuring the Multicast Program

Configure the multicast program parameters.

Planning Data

Item		Description	Example
Configuring a group VLAN	Group Address Begin	Configure this item according to the network planning of the operator.	IPv4:224.0.1.10
	Group Address End	Configure this item according to the network planning of the operator.	IPv4:224.0.1.50
	Group VLAN	Configure this item according to the network planning of the operator. The value range is 0 to 4085.	1000
	Bandwidth (Kbs)	Configure this item according to the network planning of the operator. The value ranges from 0 to 30000, and the unit is Kbit/s.	5000
	Signaling VLAN	Configure this item according to the network planning of the operator. The value range is 0 to 4095.	300
	Prejoin	The options include **Enable** and **Disable**.	Enable
	Source IP	Configure this item according to the network planning of the operator.	10.90.20.1
Configuring program packets	Packet Name	Configure this item according to the network planning of the operator.	IPTV
	Group Address Begin	Configure this item according to the network planning of the operator.	IPv4:224.0.1.10
	Group Address End	Configure this item according to the network planning of the operator.	IPv4:224.0.1.50
	Authority	The options include **Normal**, **Preview** and **Forbid**. The default setting is **Normal**.	Preview
Binding program packets to a port	Slot No.	The number of the slot accommodating the PON interface card connected to the ONU.	2
	PON No. / Port No.	The number of the PON port connected to the ONU.	3
	ONU Authorized No.	The authorization number of the ONU.	1
	ONU Port No.	The ONU port number.	1
	Control Switch	Configure this item according to the network planning of the operator.	Controlled
	Packet	The bound program packet.	IPTV

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the NE manager.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. Configure the group VLAN.
   1) In the **Operational Tree** pane, select **Multicast Service→Multicast Packet Config→Group VLAN** to bring up the **Group VLAN** tab.
   2) Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a group VLAN configuration entry.
   3) Configure the parameters according to the planning data.
   4) Click the **Create on Device** button on the toolbar to complete the configuration, as shown in the figure below.

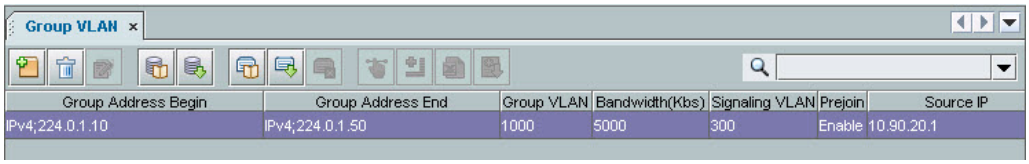


Figure 8-20 Configuring a Group VLAN

4. Configure the program packet.
   1) In the **Operational Tree** pane, select **Multicast Service→Multicast Packet Config→Packet Config** to bring up the **Packet Config** tab.
   2) Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a program packet name configuration entry.
   3) Select the right pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a program packet IP address configuration entry.
   4) Configure the parameters according to the planning data.
   5) Click the **Create on Device** button on the toolbar to complete the configuration, as shown in the figure below.

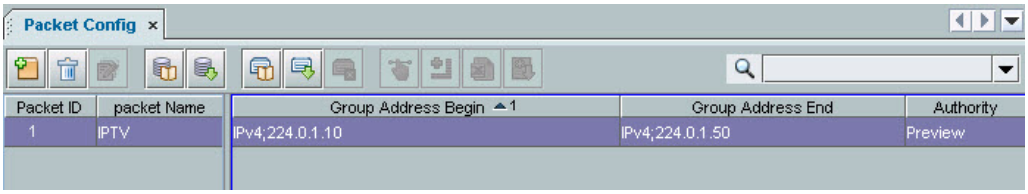


Figure 8-21 Configuring Program Packets

5. Bind the program packet to a port.

   1) In the **Operational Tree** pane, select **Multicast Service→Multicast Packet Config→Port Bind Packet** to bring up the **Port Bind Packet** tab.

   2) Select the left pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a port configuration entry.

   3) Select the right pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a program packet configuration entry.

   4) Configure the parameters according to the planning data.

   5) Click the **Create on Device** button on the toolbar to complete the configuration, as shown in the figure below.

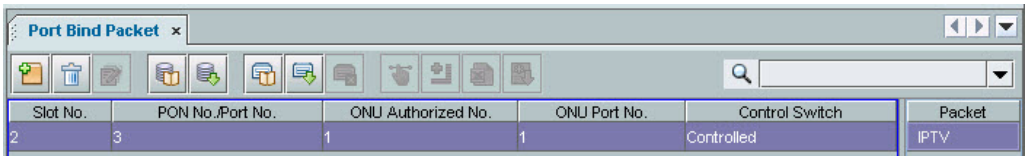


Figure 8-22 Binding Program Packets to a Port

9 Configuring the Wi-Fi Service

The following gives an example to introduce how to configure the Wi-Fi service for the AN6001-G16.

☑ Network Scenario

☑ Wi-Fi Service Configuration Example

9.1 Network Scenario

Service Planning

Use the ONU supporting the Wi-Fi function to provide the Wi-Fi connection service for fiber broadband family subscribers and access other user terminals.

Network Diagram

Figure 9-1 shows the network diagram for the Wi-Fi service of the AN6001-G16.

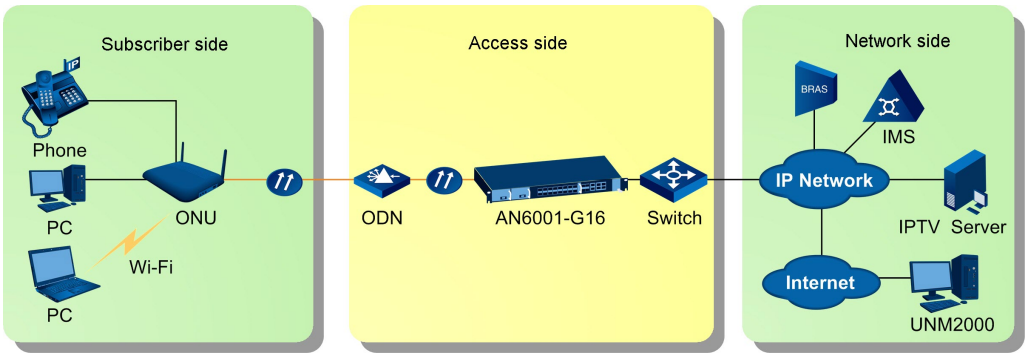


Figure 9-1 Network Diagram for the Wi-Fi Service

The wireless terminal equipment accesses the network via the Wi-Fi interface of the ONU.

- Uplink direction:

  The ONU is connected to the AN6001-G16 via the GPON interface to provide integrated access services.

- Downlink direction:

  The ONU is connected to the wireless equipment via the Wi-Fi interface to access the WLAN service.

9.2 Wi-Fi Service Configuration Example

The following gives an example to introduce how to configure the Wi-Fi service.

9.2.1 Configuration Flow

Prerequisites

- The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.
- The ONU used supports the Wi-Fi function.

Configuration Flow

See Figure 9-2 for the flow of configuring the Wi-Fi services.

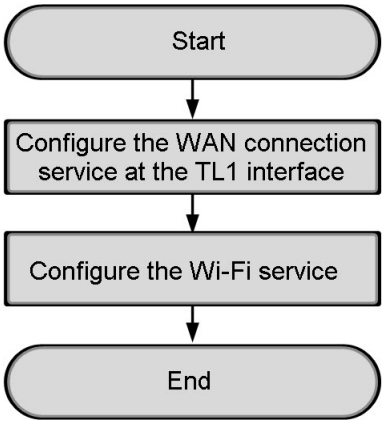


Figure 9-2 Flow of Configuring the Wi-Fi Service

9.2.2 Configuring the WAN Connection Service at the TL1 Interface

Configure the WAN connection service at the TL1 interface, and set the parameters such as the WAN connection mode.

Configuration Rules

The VLAN ID for the WAN connection service should be within the local VLAN ID range for the Wi-Fi service on the AN6001-G16 side.

Planning Data

Item		Description	Example
ONU information	Slot No.	The number of the slot housing the card connected to the ONU.	1
	PON No.	The number of the PON port connected to the ONU.	1
	ONU No.	The authorization number of the ONU.	2
WAN connection service	Wan_Mode	Select INTERNET or the mode with INTERNET for the Wi-Fi service.	INTERNET
	Wan_Conn_Type	Select "Bridging" or "Routing" according to the requirement of Internet service providers (ISP). "Bridging" stands for the L2 bridge connection mode, while "Routing" stands for the L3 route connection mode.	Routing
	WAN_Vlan_Id	Set the VLAN ID (within the range of 1 to 4096) of WAN connection according to the requirement of the ISP. The VLAN ID should not be occupied by other connections, and should be within the local VLAN ID range of the Wi-Fi service on the AN6001-G16 side.	200
	Wan_Cos	The 802.1p priority of WAN connection. The value ranges from 0 to 7, with 7 standing for the highest priority, and 0 the lowest one.	1
	Wan_NAT_Enable	Select, according to the ISP requirement, to enable or disable the network address translation function that converts the private network IP address to the public network IP address.	Disable
	Wan_D_S_P	Select the IP address obtaining mode for the WAN connection according to the ISP requirement.	DHCP
	Binding LAN1 to LAN4 Binding 10G LAN 2.4G_SSD1 to 2.4G_ SSD4 5G_SSD1 to 5G_SSD4	Select the Ethernet port or SSID to be bound with the WAN connection. The selected item is enabled.	Binding LAN1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click an ONU and select **Service Configuration** from the menu.

4. In the **Operational Tree** pane, select **Common Config→WAN Service** to open the **WAN Service** tab.
5. Click **Add** at the right pane, enter **1** in the dialog box that appears, and then click **OK** to add a WAN connection service.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 9-3.

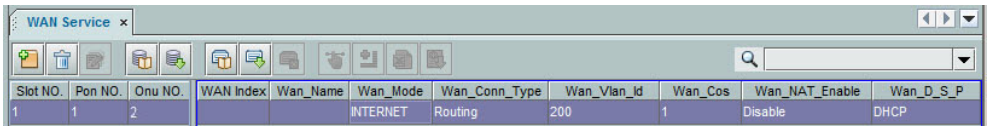


Figure 9-3 The WAN Connection Service

9.2.3 Configuring the Wi-Fi Service

Configure the related parameters of the Wi-Fi service.

Configuration Rules

The password configuration rules are described as follows:

- When the WLAN authentication mode is **OPEN** and the encryption type is **NONE**, users need not configure the password.
- When the WLAN authentication mode is **OPEN**, **SHARED** or **WEPAUTO**, users need to configure WEP key 1 through WEP key 4, and the key indexes determine the valid password.
- In other cases, users should configure the WPA pre-shared key.

Planning Data

Item		Description	Example
ONU information	Slot No.	The number of the slot housing the card connected to the ONU.	1
	PON No.	The number of the PON port connected to the ONU.	1
	ONU No.	The authorization number of the ONU.	2

Item		Description	Example
Configuring the Wi-Fi service	IGD_WLAN_AP Module Enable	Select whether to enable the Wi-Fi function.	Enable
	IGD_WLAN_ COUNTRY	Sets the wireless channel range.	ETSI
	IGD_WLAN_ CHANNEL	The sequence number of the wireless channel.	0
	IGD_WLAN_ STANDARD	The wireless network standards that the equipment complies with. Configure this item according to the operator's network planning.	802.11b/g/n
	IGD_WLAN_SSID	The wireless network identifier. Configure this item according to the operator's network planning.	abc
	IGD_WLAN_ENABLE	Select whether to enable the SSID.	Enable
	IGD_WLAN_ SSIDHide	Select whether to hide the SSID.	Available
	IGD_WLAN_ AuthMode	Configure this item according to the network planning of the operator.	WPAPSK
	IGD_WLAN_ EncrypType	Configure this item according to the network planning of the operator.	AES
	IGD_WLAN_ Presharedkey	The WPA encrypted key, containing no more than 64 characters.	123456
	IGD_WLAN_ WPARekeyInterval	The WPA key refreshing interval; the unit is second.	86400

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click an ONU and select **Service Configuration** from the menu.
4. In the **Operational Tree** pane, select **Common Config→WiFi Service Config** to open the **WiFi Service Config** tab.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 9-4.

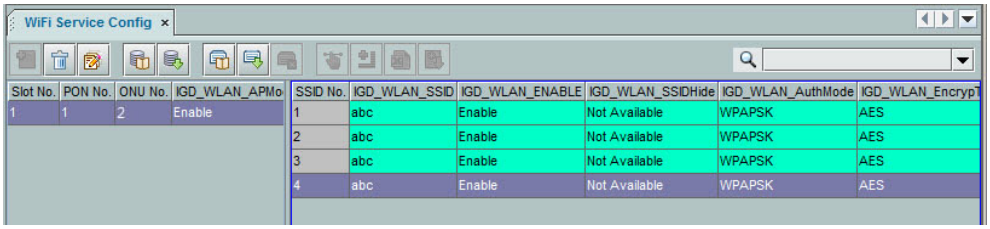


Figure 9-4 Configuring the Wi-Fi Service

9.2.4 Configuration Result

After the configuration is completed, users can access the Wi-Fi wireless network.

10 Configuring the CATV Service

The following gives an example to introduce how to configure the CATV service for the AN6001-G16.

☑ Network Scenario

☑ CATV Service Configuration Example

10.1 Network Scenario

The CATV service uses the WDM technology. Via a multiplexer, the TV signal is multiplexed with the data signal and voice signal. The downlink data wavelength is 1490 nm, the uplink data wavelength is 1310 nm, and the CATV signal wavelength is 1550 nm. Figure 10-1 shows the network diagram.

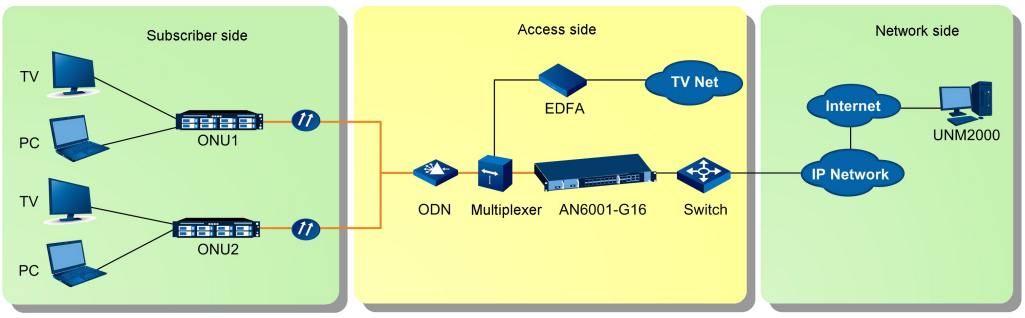


Figure 10-1 Network Diagram for the CATV Service

10.2 CATV Service Configuration Example

The following gives an example to introduce how to configure the CATV service.

10.2.1 Configuration Flow

Prerequisites

- The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.
- The ONU used supports the CATV function.

Configuration Flow

Figure 10-2 illustrates the flow of configuring the CATV service.

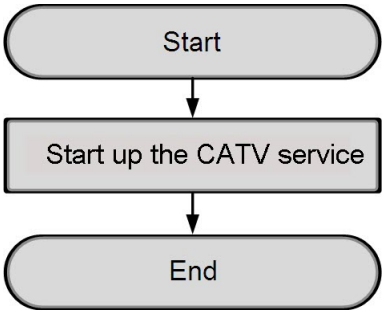


Figure 10-2 Flow of Configuring the CATV Service

10.2.2 Starting up the CATV Service

The following introduces how to start up the CATV service.

Planning Data

Item		Description	Example
ONU information	Slot No.	The number of the slot housing the card connected to the ONU.	1
	PON No.	The number of the PON port connected to the ONU.	3
	ONU No.	The ONU authorization number. Configure this item according to the network planning of the operator.	1
	ONU MAC	Configure this item according to the network planning of the operator.	54-4b-40-08-13-d8
	ONU Type	The type of the ONU.	AN5506-04-GG
Configuring service at the port	Enable CATV	Select whether to enable the CATV service.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.

3. Right-click the ONU to be configured, and select **Port Service Config** from the shortcut menu that appears to bring up the **Port Service Config** tab.
4. Select **CATV** in the left pane, and configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 10-3.

Figure 10-3 Configuring Service at the Port

10.2.3 Configuration Result

The subscribers can use the CATV service.

11 Configuring Layer 3 Functions

The following uses examples to introduce how to configure the Layer 3 functions of the AN6001-G16.

☑ Configuring the ARP Proxy

☑ Configuring the OSPF Routing Protocol

☑ Configuring the DHCP Function

11.1 Configuring the ARP Proxy

The following introduces how to configure the ARP proxy function for the AN6001-G16.

11.1.1 Configuration Rules

The ARP proxy can be configured flexibly according to network planning. The configuration rules are as follows:

- Supports binding with multiple VLANs.
- Supports binding crossing network segments.
- Supports binding with multiple VLANs crossing network segments.

11.1.2 Example of Configuring ARP Proxy in the Same-VLAN and Same-network Segment Application

The following introduces how to configure and implement the ARP proxy function between user equipment, taking the most frequently used same-VLAN and same-network segment scenario as an example. The configurations of other scenarios are similar to this.

11.1.2.1 Network Scenario

Service Planning

The AN6001-G16 serves as ARP proxy to allow internetworking among users in the same network segment (10.90.10.0/24) in the same VLAN. A Super VLAN is provided at the AN6001-G16 and bound with Sub VLANs. The ARP proxy service is then provided through L3 forwarding.

Network Diagram

Figure 11-1 shows the network diagram for ARP proxy in the same-VLAN and same-network segment application.

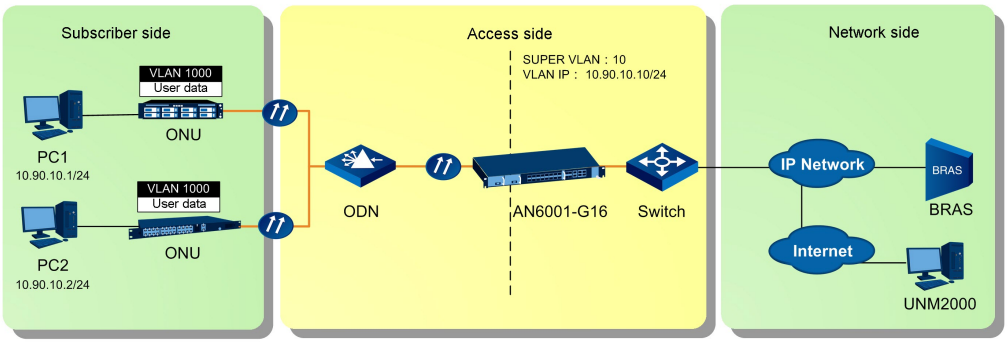


Figure 11-1 Network Diagram for the ARP Proxy in the Same-VLAN and Same-Network Segment Application

Two subscriber PCs, which belong to the same VLAN with the ID 1000, are connected to the AN6001-G16 via ONUs.The IP addresses of the two PCs are 10.90.10.1 and 10.90.10.2 respectively. Configure a Super VLAN and a Sub VLAN at the AN6001-G16, and bind them together. After the VLAN IP address is set for the Super VLAN, the ARP proxy service can be provided by means of L3 forwarding.

11.1.2.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

Figure 11-2 shows the flow of configuring ARP proxy in the same-VLAN and same-network segment application.

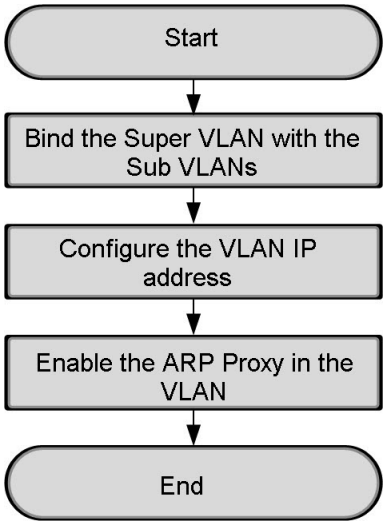


Figure 11-2 Flow of Configuring the ARP Proxy

11.1.2.3 Binding the Super VLAN with the Sub VLANs

Bind the Super VLAN with the Sub VLANs to set up the mappings between them.

Configuration Rules

The following describes the rules for binding the Super VLAN with the Sub VLANs:

- The VLAN IDs set for the Super VLANs and the Sub VLANs range from 1 to 4085.
- One Super VLAN can be bound to multiple Sub VLANs simultaneously yet one Sub VLAN can be bound to only one Super VLAN.
- The IP address bound to the downlink Super VLAN should be in the same network segment with the IP address of the succeeding equipment.
- The IP address bound to the uplink Super VLAN should be in the same network segment with the IP address of the previous equipment that runs the OSPF protocol such as the switch.

Planning Data

Item	Description	Example
Super VLAN ID	Select the created Super VLAN ID.	10
VLAN Property	Set the Super VLAN to "manager VLAN" or "supervlan".	supervlan
Sub VLAN ID	The Sub VLAN ID bound to the Super VLAN.	1000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **VLAN Service→Bind Sub VLAN to Super VLAN** to open the **Bind Sub VLAN to Super VLAN** tab.
4. Select the left pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a Super VLAN configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a Sub VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-3.

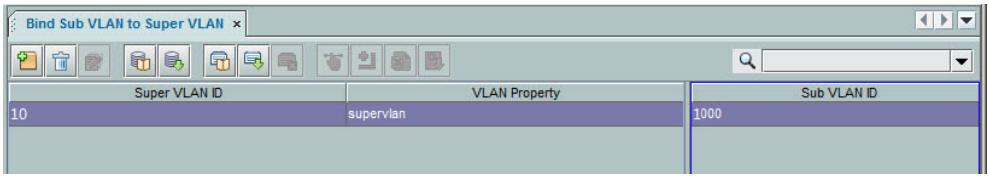


Figure 11-3 Binding Super VLAN with Sub VLANs

11.1.2.4 Configuring the VLAN IP Address

Configure an IP address for the Super VLAN to implement the L3 forwarding function.

Configuration Rules

Select a free IP address for the Super VLAN from the network segment where the user equipment is located.

Planning Data

Item	Description	Example
VLAN ID	Enter the ID of the VLAN to be configured with IP addresses.	10
Primary IP Address	Set the primary IP address of the VLAN.	10.90.10.10/255.255.255.0
Secondary IP Address	Set a standby IP address for the VLAN. This item is not configured in this example.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the**Operational Tree** pane, select **VLAN Service→Configure VLAN IP** to open the **Configure VLAN IP** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a VLAN IP address configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-4.

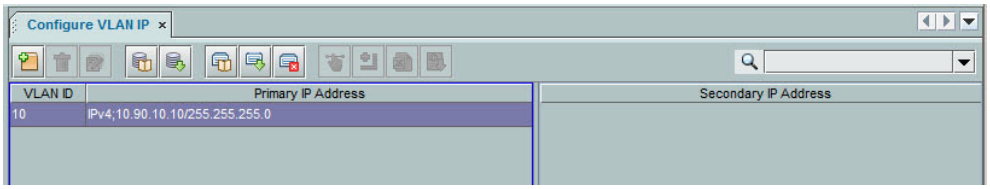


Figure 11-4 Configuring the VLAN IP Address

11.1.2.5 Enabling the ARP Proxy Function in the VLAN

Enable the ARP proxy function for the configured Super VLAN.

Planning Data

Item	Description	Example
VLAN ID	Read only	10
ARP Proxy Switch (Router)	Enable or disable the cross-network segment ARP proxy function.	Enable
ARP Proxy Switch (Inner Sub VLAN)	Enable or disable the intra-VLAN ARP proxy function.	Enable
ARP Proxy Switch (Outer Sub VLAN)	Enable or disable the inter-VLAN ARP proxy function.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→ARP Proxy Manage →ARP Proxy Switch On VLAN** to open the **ARP Proxy Switch On VLAN** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-5.

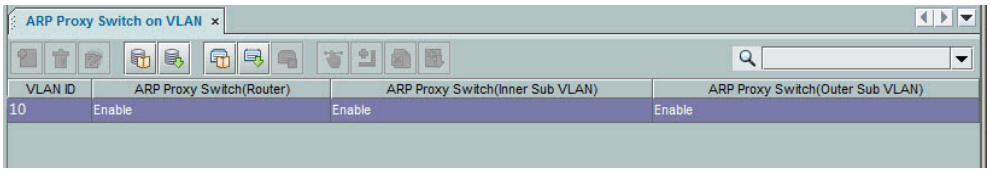


Figure 11-5 Function Switch for the ARP Proxy in the VLAN

11.1.2.6 Configuration Result

After the configuration is completed, the two subscriber PCs can access each other normally.

11.2 Configuring the OSPF Routing Protocol

The following gives an example to introduce how the AN6001-G16 running the OSPF routing protocol performs the routing and forwarding function together with the adjacent router that also runs the OSPF protocol.

11.2.1 Example of Configuring the OSPF Routing Protocol

The following gives an example to introduce how to configure the OSPF routing protocol for the AN6001-G16 equipment.

11.2.1.1 Network Scenario

Service Planning

The AN6001-G16 should serve as the OSPF edge routing equipment to provide the OSPF routing function when users need to access an external network IP address.

Network Diagram

Figure 11-6 shows the network diagram for configuring the OSPF routing protocol.

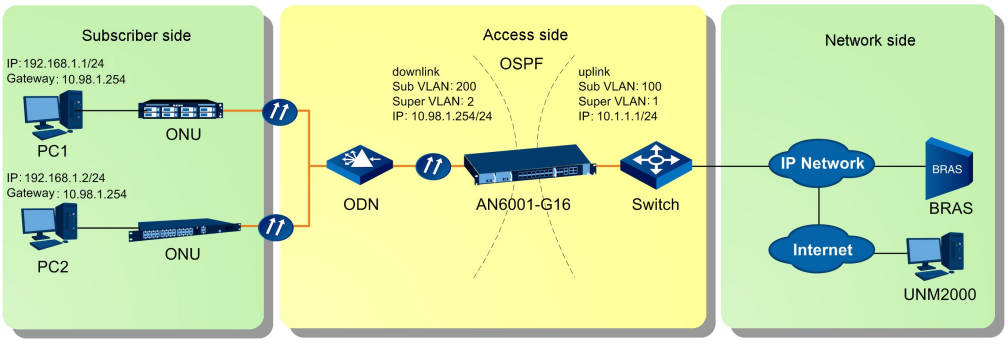


Figure 11-6 Network Diagram for Configuring the OSPF Routing Protocol

The AN6001-G16 is configured with uplink and downlink Super VLANs and Sub VLANs to act as a router. When the OSPF protocol is run on it, the equipment implements the OSPF routing function. If the user's address and the preset address to access are not in the same network segment, routing and forwarding are implemented via the AN6001-G16 to enable the access crossing network segments.

11.2.1.2 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

The flow of configuring the OSPF routing protocol is shown in Figure 11-7.

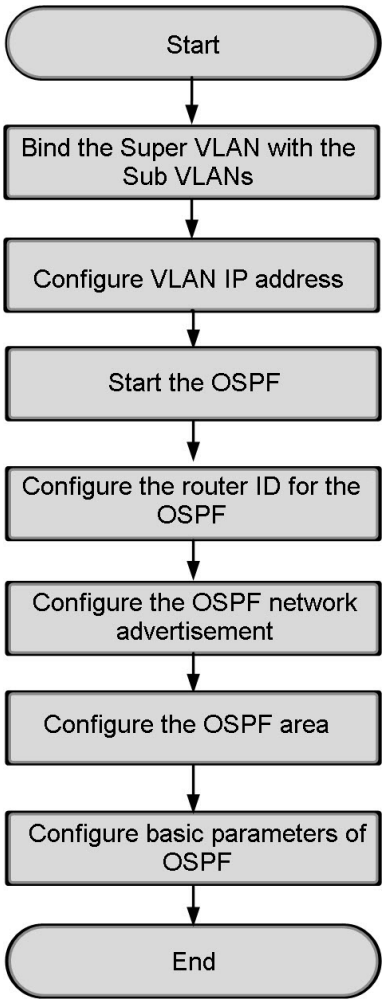


Figure 11-7 Flow of Configuring the OSPF Routing Protocol

11.2.1.3 Binding the Super VLAN with the Sub VLANs

Bind the Super VLAN with the Sub VLANs to set up the mappings between them.

Configuration Rules

The following describes the rules for binding the Super VLAN with the Sub VLANs:

- The VLAN IDs set for the Super VLANs and the Sub VLANs range from 1 to 4085.
- One Super VLAN can be bound to multiple Sub VLANs simultaneously yet one Sub VLAN can be bound to only one Super VLAN.
- The IP address bound to the downlink Super VLAN should be in the same network segment with the IP address of the succeeding equipment.
- The IP address bound to the uplink Super VLAN should be in the same network segment with the IP address of the previous equipment that runs the OSPF protocol such as the switch.

Planning Data

Item	Description	Example	
Super VLAN ID	Select the created Super VLAN ID.	1	2
VLAN Property	Set the Super VLAN to "manager VLAN" or "supervlan".	supervlan	
Sub VLAN ID	The Sub VLAN ID bound to the Super VLAN.	100	200

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **VLAN Service→Bind Sub VLAN to Super VLAN** to open the **Bind Sub VLAN to Super VLAN** tab.
4. Select the left pane, click **Add**, enter **2** in the displayed dialog box, and click **OK** to add two Super VLAN configuration entries.
5. Select a Super VLAN entry and select the right pane. Click **Add**, and enter **1** in the dialog box that appears to add a Sub VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-8.

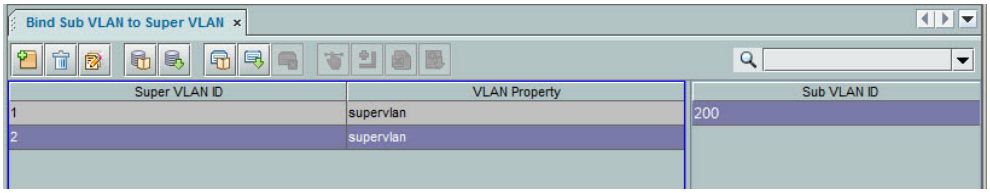


Figure 11-8 Binding Super VLAN with Sub VLANs

11.2.1.4 Configuring the VLAN IP Address

Set the IP address for the configured Super VLAN.

Planning Data

Item	Description	Example	
VLAN ID	The Super VLAN ID.	1	2
Primary IP Address	The IP address added to the Super VLAN.	10.1.1.1/255.255.255.0	10.98.1.254/255.255.255.0

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the**Operational Tree** pane, select **VLAN Service→Configure VLAN IP** to open the **Configure VLAN IP** tab.
4. Select the left pane, click **Add**, enter **2** in the displayed dialog box, and click **OK** to add two VLAN IP address configuration entries.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-9.

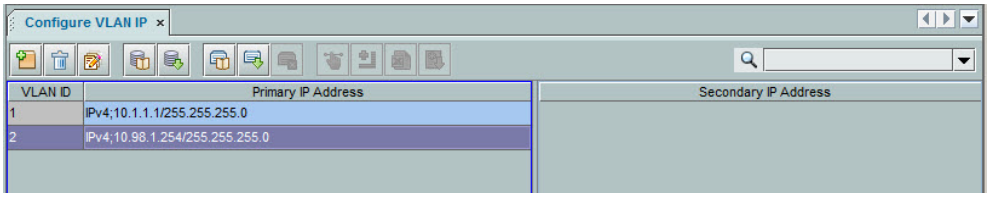


Figure 11-9 Configuring the VLAN IP Address

11.2.1.5 Starting the OSPF

Enable the OSPF function.

Planning Data

Item	Description	Example
Start/Stop	Enable / disable the OSPF protocol.	Start

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→OSPF→Router OSPF** to open the **Router OSPF** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-10.

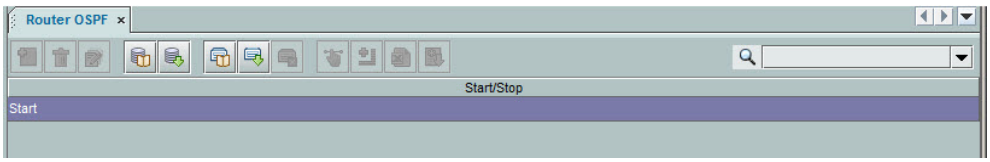


Figure 11-10 Starting the OSPF

11.2.1.6 Configuring the Router ID for the OSPF

Configure the router ID for the OSPF.

Planning Data

Item	Description	Example
IP Address	Configure this item according to the network planning of the operator.	10.12.1.3

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→OSPF→OSPF Router_ID Configure** to open the **OSPF Router_ID Configure** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-11.

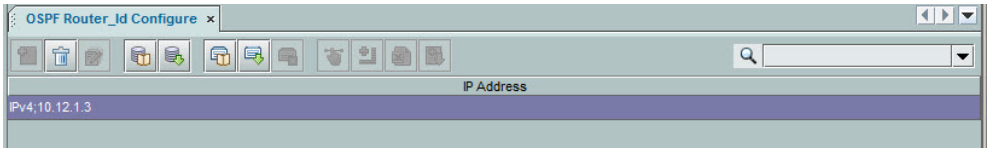


Figure 11-11 Configuring the OSPF Router ID

11.2.1.7 Configuring the OSPF Network Advertisement

Configure the AN6001-G16 as the OSPF router to perform LSA (Link State Advertisement) and inform other equipment in the LSA area that it belongs to, of its link, interface, overhead and neighbor information.

Planning Data

Item	Description	Example	
IP Address	The network segment advertised by OSPF network	10.1.1.0/255.255.255.0	10.98.1.0/255.255.255.0
Area_ID	Configure this item according to the network planning of the operator.	1.0.0.1	

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→OSPF→OSPF Network Advertise** to open the **OSPF Network Advertise** tab.
4. Click **Add**, enter **2** in the displayed dialog box, and click **OK** to add two OSPF network advertisement configuration entries.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-12.

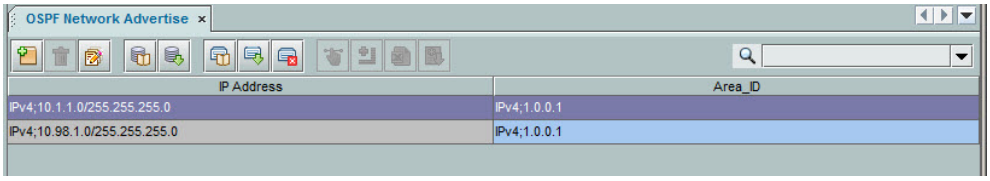


Figure 11-12 The OSPF Network Advertisement

11.2.1.8 Configuring the OSPF Area

Configure the area ID and area type of the OSPF area.

Planning Data

Item	Description	Example
Area ID	Configure this item according to the network planning of the operator.	1.0.0.1
Area Type	Configure this item according to the network planning of the operator.	STUB
No-Summary	The function that prevents the ABR from sending Summary LSA to the Stub area. Selecting the check box in this field means enabling the "No-Summary" function.	-
Translator Role	It is a read-only item, indicating the translator role in the NSSA.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→OSPF→OSPF Area** to open the **OSPF Area** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add an OSPF area configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-13.

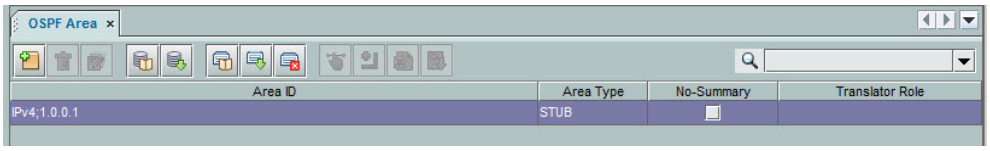


Figure 11-13 Configuring the OSPF Area

11.2.1.9 Configuring Basic Parameters of the OSPF

Configure parameters related to the OSPF routing protocol, including Hello packet interval and re-transmission interval of LSA.

Planning Data

Item	Description	Example	
VLAN ID	The Super VLAN ID.	1	2
IP Address	The IP address of Super VLAN.	10.1.1.1	10.98.1.254
Dead-interval (s)	Configure this item according to the network planning of the operator.	40	
Hello-interval (s)	Configure this item according to the network planning of the operator.	10	
Retransmit-interval (s)	Configure this item according to the network planning of the operator.	5	
Transmit-delay (s)	Configure this item according to the network planning of the operator.	1	
Network Type	Configure this item according to the network planning of the operator.	Broadcast	
Cost	Configure this item according to the network planning of the operator.	10	
MTU	Configure this item according to the network planning of the operator.	1500	
Priority	Configure this item according to the network planning of the operator.	1	

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→OSPF→OSPF Parameter Config** to open the **OSPF Parameter Config** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-14.

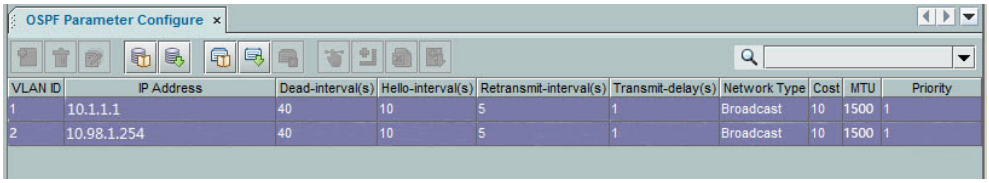


Figure 11-14 Configuring OSPF Basic Parameters

11.2.1.10 Configuration Result

As the OSPF router, the AN6001-G16 establishes the link state database by transmitting the LSA within the announced area. Taking itself as the root node, the equipment works out the shortest path tree, so as to support cross-segment network access of the connected users via this path tree.

11.3 Configuring the DHCP Function

The following introduces how to configure the DHCP function of the AN6001-G16.

11.3.1 Configuration Rules

The rules for configuring the DHCP service for the AN6001-G16 are as follows:

- When the AN6001-G16 serves as the DHCP Relay, it can either be the DHCP proxy only or be both the DHCP proxy and the gateway. Under both conditions, the Super VLAN interface should be added as the Layer 3 interface, so as to convert the users' DHCP broadcast messages into the unicast messages and forward the messages to the designated DHCP server.
  - Super VLAN: a virtual routing interface, also known as VLAN aggregation. A Super VLAN contains multiple Sub VLANs.
  - Sub VLAN: a subsidiary VLAN of the Super VLAN. The relationship between the Super VLAN and the Sub VLAN is master and slave.
- The AN6001-G16 can be configured with up to 16 Super VLANs. Each Super VLAN can be added with four Sub VLANs at most.

- The IP address bound to the downlink Super VLAN should be in the same network segment with the IP address of the DHCP Client which uses the DHCP proxy function of this Super VLAN.
- The VLAN IDs set for the Super VLANs and the Sub VLANs range from 1 to 4085.
- When the AN6001-G16 is used as DHCP proxy only, static routing should be configured. The DHCP request is forwarded to the DHCP server via the network gateway.
- When the DHCP Snooping function is enabled for the AN6001-G16, DHCP broadcast packets need not be processed. However, when trusted ports have been configured for the DHCP Snooping, only the trusted ports can normally receive and forward the DHCP request messages, while the DHCP response messages from the untrusted ports and the untrusted DHCP request messages from users are filtered. In this way, the client end can only obtain the IP address from a legal DHCP server.
- When serving as the DHCP Server and having received the DHCP broadcast messages from a user, the AN6001-G16 searches for an undistributed IP address from the address pool and sends the PING packets to check whether the IP address is occupied. After confirming the IP address is available, it allocates the IP address to the user.

11.3.2 Network Scenario

Background Information

The AN6001-G16 supports abundant DHCP functions, which can be deployed flexible to meet varied service demands.

- When serving as the DHCP proxy only, the AN6001-G16 converts the broadcast DHCP request messages received from the DHCP Client into the unicast messages, and modifies the message parameters such as source MAC address, destination MAC address, source IP address and destination IP address. Then, it forwards the messages to the DHCP Server via an external gateway.

- When serving as the DHCP proxy and gateway, the AN6001-G16 converts the broadcast DHCP request messages received from the DHCP Client into unicast messages, replaces the gateway IP address of the messages with the IP address of the downlink Super VLAN, and forwards the unicast messages to the DHCP Server in a different network segment.
- The AN6001-G16 provides the DHCP Option 60 authentication function. Thus, the Option 60 character authentication can be implemented for PC1 and PC2 users. Two Super VLANs are provided at the AN6001-G16 and bound to Sub VLANs. Then, the authentication service can be provided by proxy forwarding and character identification.
- When serving as the DHCP server and having received the broadcast DHCP request messages from the DHCP client, the AN6001-G16 directly allocates the IP address in the IP address pool to the user.
- After the DHCP Snooping function is enabled for it, the AN6001-G16 transmits the broadcast DHCP request messages received from the DHCP Client to the DHCP server, and prevents the DHCP server spoofing by filtering the response packets transmitted by the DHCP server.

Network Diagram

The network diagram for the DHCP service carried by the AN6001-G16 is shown in Figure 11-15.

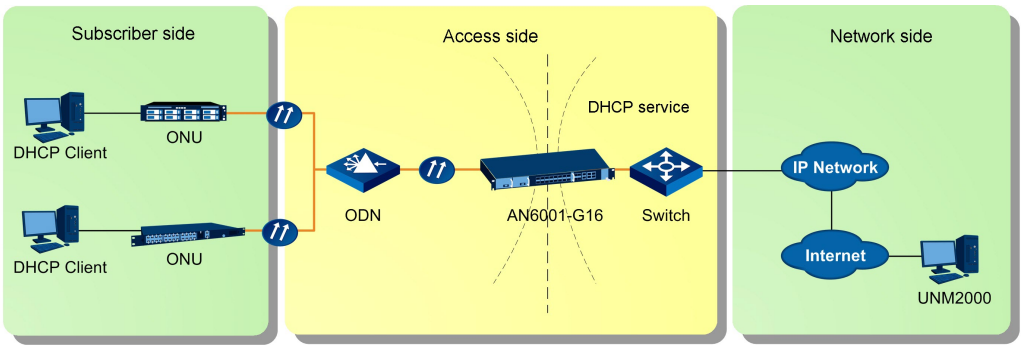


Figure 11-15 DHCP Service Network

11.3.3 Configuration Flow

Prerequisites

The VLAN service channel has been created. Please refer to Basic Configurations for the creation method.

Configuration Flow

Figure 11-16 shows the flow of configuring the DHCP service.

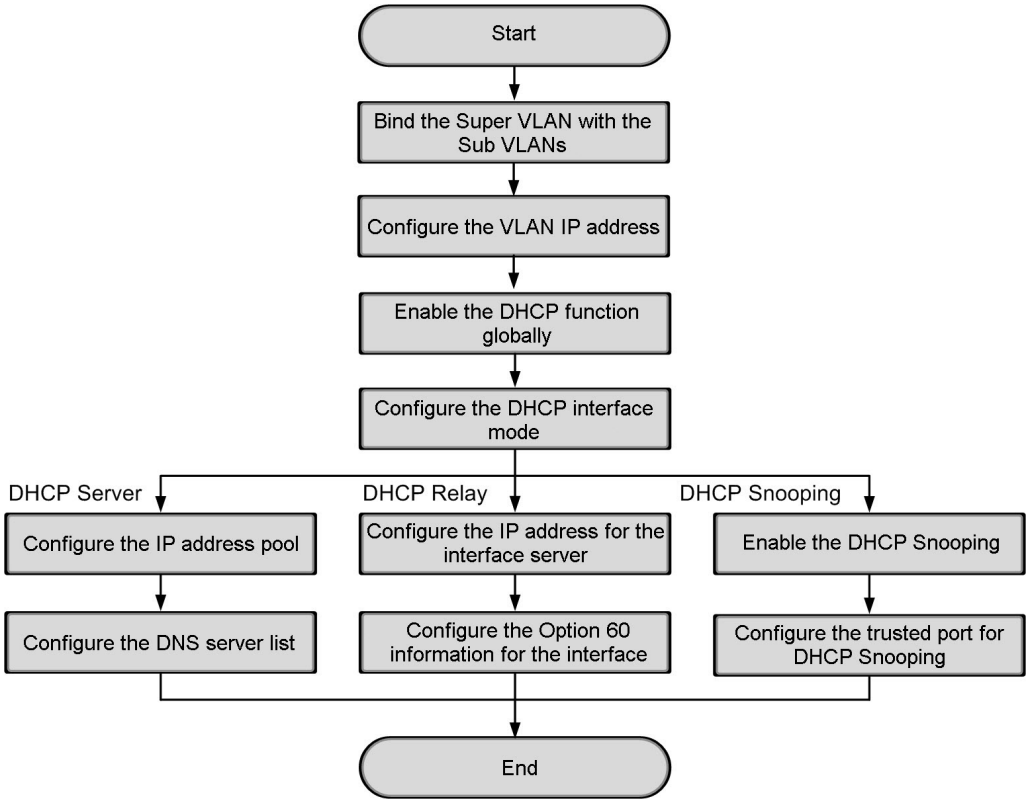


Figure 11-16 Flow of Configuring the DHCP Service

11.3.4 Binding the Super VLAN with the Sub VLANs

Refer to Binding the Super VLAN with the Sub VLANs for how to bind Super VLAN with Sub VLANs.

11.3.5 Configuring the VLAN IP Address

Please refer to Configuring the VLAN IP Address for the procedures of configuring the VLAN IP address.

11.3.6 Configuring the DHCP Global Switch

Enable the DHCP Layer 3 function for the AN6001-G16.

Planning Data

Item	Description	Example
DHCP Global Switch	Enable the DHCP function globally.	Enable
Ping Function (Times)	Enable the Ping function and set the operation times.	2
Ping Interval (ms)	Configure the time interval between two Pinging operations.	500

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Global→ DHCP Global Switch** to open the **DHCP Global Switch** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-17.

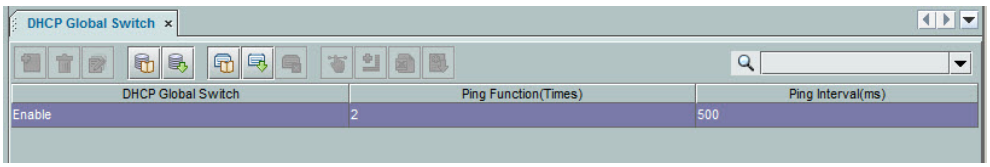


Figure 11-17 DHCP Global Switch

11.3.7 Configuring the DHCP Interface Mode

Set the Layer 3 interface of the AN6001-G16 to the required DHCP service interface mode.

Planning Data

Item	Description	Example
Super VLAN ID	The Super VLAN ID.	1
DHCP Interface Mode	Select the Server mode or Relay mode.	Relay Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Global→Set DHCP Interface Mode** to open the **Set DHCP Interface Mode** tab.
4. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a DHCP interface mode configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-18.

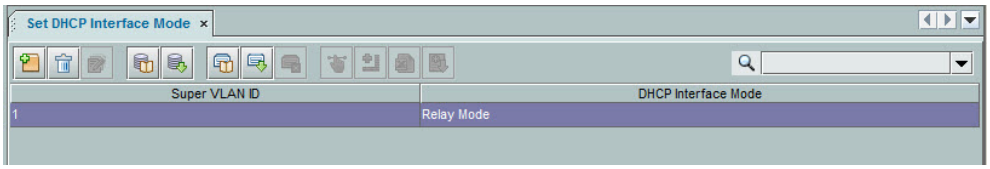


Figure 11-18 Configuring the DHCP Interface Mode

11.3.8 Configuring the DHCP Server

The operation described in this section is only required for configuring the DHCP Server service.

11.3.8.1 Configuring the IP Address Pool

Configure the IP address pool to allocate IP addresses to users.

Planning Data

Item	Description	Example
Pool ID	Configure this item according to the network planning of the operator.	1
Begin IP	The starting IP address available to users.	IPv4:192.168.1.1/255.255.255.0
End IP	The ending IP address available to users.	IPv4:192.168.1.20/255.255.255.0
Gateway	The default gateway corresponding to the IP address.	192.168.1.254
Lease (s)	The lease period of the IP address. Configure this item according to the network planning of the operator.	001 00:01:00

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Server→IP Pool Config** to open the **IP Pool Config** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add an IP address pool configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-19.

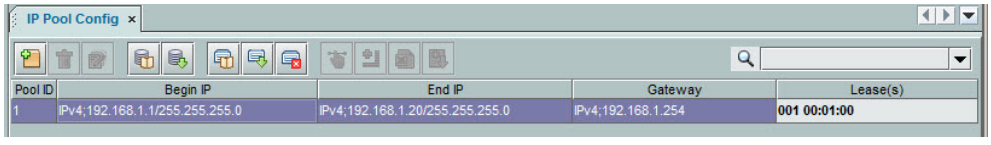


Figure 11-19 Configuring the IP Address Pool

11.3.8.2 Configuring the DNS Server List

Provide the address and domain name mapping for the DHCP client by configuring the DNS domain name server.

Planning Data

Item	Description	Example
Pool ID	Select the address pool ID configured in **Configuring the IP Address Pool**.	1
DNS Server Address	The DNS server address allocated to the user.	10.19.8.10
Operation Type	Select **Set**, which means adding.	Set

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Server→Set DNS Server Address List** to open the **Set DNS Server Address List** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add an IP address pool configuration entry.
5. Select the right pane. Click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a DNS server configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-20.

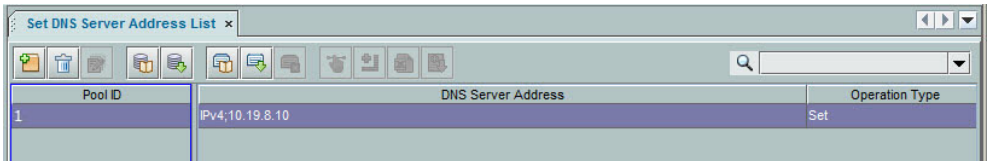


Figure 11-20 Configuring the DNS Server List

11.3.9 Configuring the DHCP Relay

The operation described in this section is only required for configuring the DHCP Relay service.

11.3.9.1 Configuring the Interface Server Address

Configure the IP address of the DHCP server corresponding to the Layer 3 interfaces of the AN6001-G16.

Planning Data

Item	Description	Example
Server IP Address	The IP address of the DHCP server	2.2.2.5
Super VLAN ID	Select the Super VLAN ID.	1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Relay→Set Port's DHCP Server IP** to open the **Set Port's DHCP Server IP** tab.
4. Select the left pane, click **Add**, enter **1** in the dialog box that appears, and then click **OK** to add a Super VLAN ID configuration entry.
5. Select the right pane. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a server IP address configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-21.

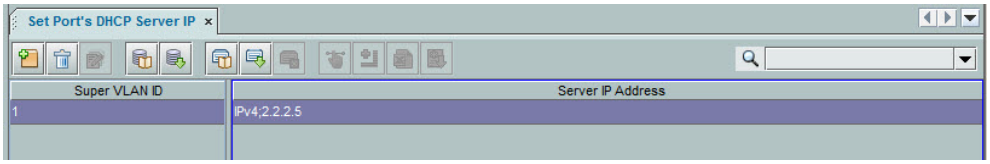


Figure 11-21 Configuring the Interface Server Address

11.3.9.2 Configuring Option 60 Information for the Port

Configure the Option 60 information corresponding to the port.

Planning Data

Item	Description	Example
Super VLAN ID	Select the Super VLAN ID.	1
Relay IP address	Select the IP address of the DHCP client end.	IPv4:1.1.1.1
Option 60 information	Enter the Option 60 information for the DHCP client end. The text entered can contain 128 characters at most.	aaaa
operation type	Available operation types include **Set** and **Delete**. ◆ **Set** means adding. ◆ **Delete** means deleting.	Set

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Relay→Set Port's DHCP Option 60 Information** to open the **Set Port's DHCP Option 60 Information** tab.
4. Select the left pane, click **Add**, enter **1** in the dialog box that appears, and then click **OK** to add a Super VLAN ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a Super VLAN interface IP address configuration entry.
6. Configure the parameters according to the planning data.

7. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-22.

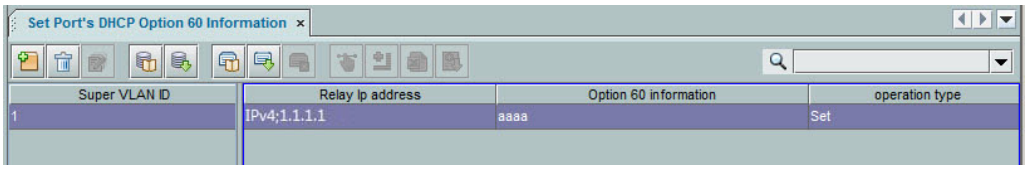


Figure 11-22 Configuring Option 60 Information for the Port

11.3.10 Configuring DHCP Snooping

The operation described in this section is only required for configuring the DHCP Snooping service.

11.3.10.1 Enabling the DHCP Snooping Function

Enable the DHCP Snooping function for the AN6001-G16.

Planning Data

Item	Description	Example
Switch	Enable the DHCP Snooping function.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP→DHCP Snooping Switch** to open the **DHCP Snooping Switch** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-23.

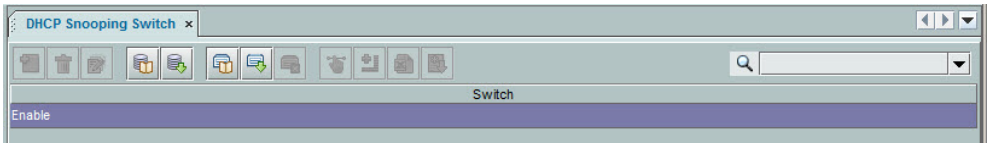


Figure 11-23 DHCP Snooping Switch

11.3.10.2 Configuring the DHCP Snooping Trusted Port

Configure the uplink trusted port of the DHCP Snooping, so as to receive and forward the DHCP Offer messages normally.

Planning Data

Item	Description	Example
Uplink Port No.	The number of the uplink port actually used.	19:SFP+1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Function→ DHCP Snooping Trusted Ports** to open the **DHCP Snooping Trusted Ports** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add an uplink interface configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 11-24.

Figure 11-24 DHCP Snooping Trusted Ports

12 Configuring Network Protection

- ☑ Configuring the MSTP Service
- ☑ Configuring the LACP
- ☑ Configuring the ERPS

12.1 Configuring the MSTP Service

The following introduces how to configure the MSTP services for the equipment.

12.1.1 Network Scenario

Service Planning

The AN6001-G16 and two switches make up an MSTP network. Two spanning trees corresponding to different VLAN IDs are configured.

Network Diagram

Figure 12-1 shows the network diagram for the MSTP services.

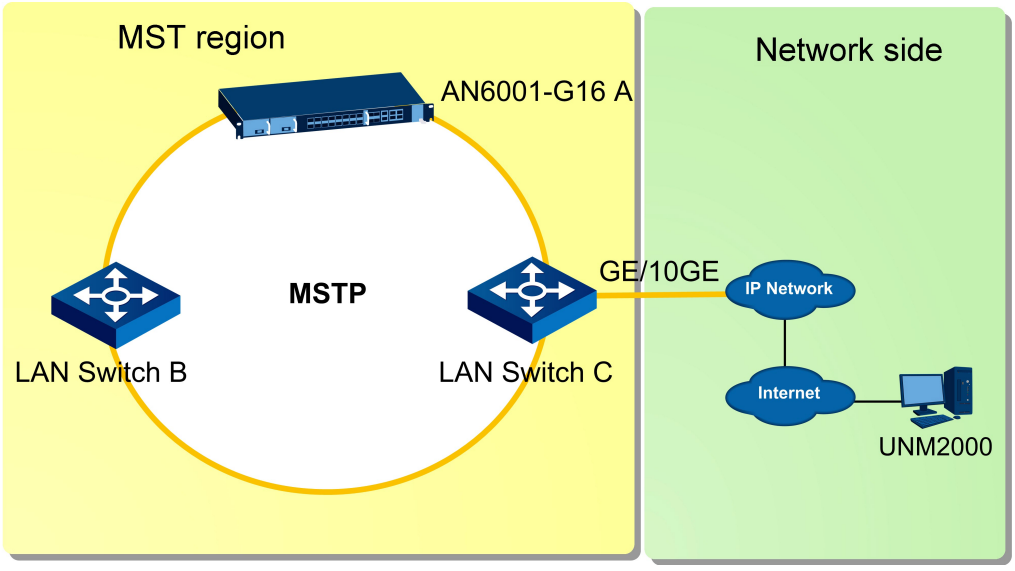


Figure 12-1 Network Diagram for the MSTP Service

Equipment A in the MST region is the AN6001-G16 with the MSTP function enabled; Equipment B and C are the switches, with C serving as the region root.

Each MST region can have multiple spanning trees (MST), and each spanning tree corresponds to a spanning tree instance. Accordingly, an MST region may have multiple spanning tree instances (MSTI). In this example, VLAN 10 is mapped to MST1, while other VLANs are mapped to MST0.

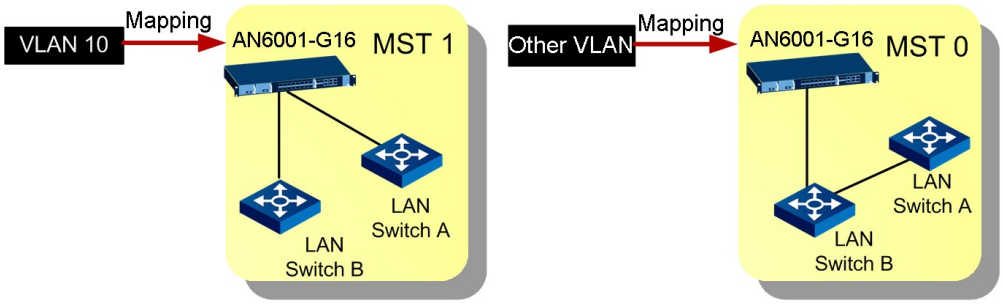


Figure 12-2 Mappings Between Spanning Trees and VLANs

12.1.2 Configuration Flow

See Figure 12-3 for the MSTP service configuration flow.

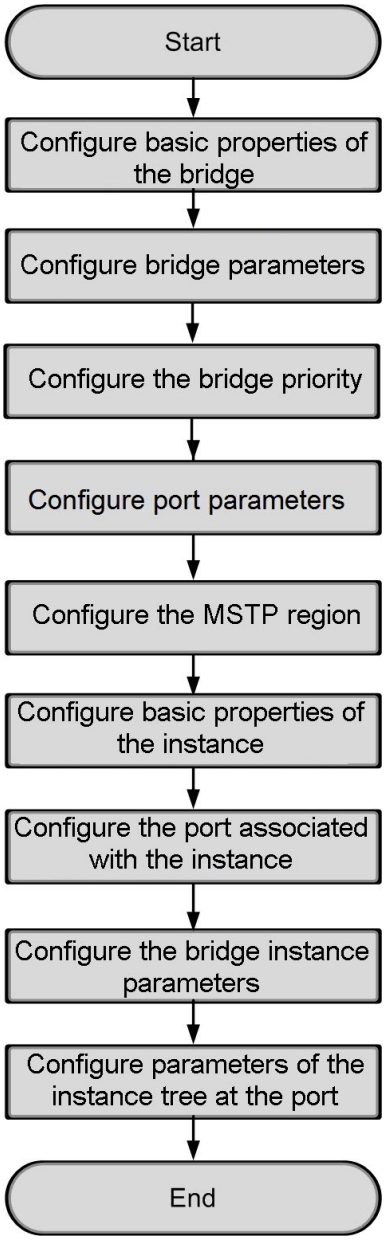


Figure 12-3 Flow of Configuring the MSTP Service

12.1.3 Configuring Basic Properties of the Bridge

Configure the basic properties of the bridge, and enable the MSTP function of the port.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Read-only.	1
Bridge Name	The name of the equipment. Read-only.	1
Protocol	Enable / disable the MSTP function.	MSTP
Slot No./Trunk Group No.	The number of the slot accommodating the uplink card actually used or the number of the Trunk group requiring the MSTP function.	19
Uplink Port No.	The number of the uplink card port actually used.	1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Bridge Basic Properties** to open the **Bridge Basic Properties** tab.
4. Select the right pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a port configuration entry with the MSTP function enabled.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-4.

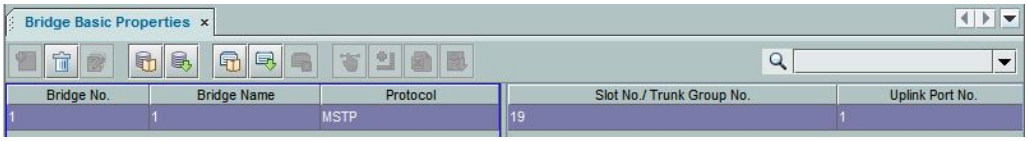


Figure 12-4 Basic Properties of the Bridge

12.1.4 Configuring Bridge Parameters

Configure the bridge parameters, including Forward-Time(s), Hello-Time(s), etc.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Set it to 1.	1
Forward-Time(s)	When the bridge port status changes, the messages need to be forwarded after a delay. The value ranges from 4 to 30.	15
Hello-Time (s)	The interval of transmitting Hello messages that are used to detect whether the link is faulty. The equipment sends Hello messages to other equipment periodically. The value ranges from 1 to 10.	2
Max-Age (s)	Used to set the time-out duration for the BPDU messages. The value ranges from 6 to 40.	20
Max_Hops	Used to restrict the scale of the MST region. Starting from the root bridge of the spanning tree in the MST region, the number of hops is reduced by 1 each time the BPDU messages are forwarded by a equipment set. The value ranges from 1 to 40.	20

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Bridge Parameter** to open the **Bridge Parameter** tab.
4. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to add a bridge parameter configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-5.

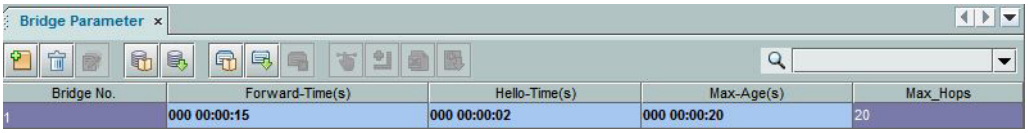


Figure 12-5 Bridge Parameters

12.1.5 Configuring Bridge Priority

Configure the bridge priority for electing the CIST.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Set it to 1.	1
Priority	Set the bridge priority for electing the CIST. The value should be an integral multiplex of 4096, and range between 0 and 61440. The default value is 32768.	32768

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Bridge Priority** to open the **Bridge Priority** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-6.

Figure 12-6 The Bridge Priority

12.1.6 Configuring Port Parameters

Configure the port parameters, including Port-Auto / Edge and Link Type.

Planning Data

Item	Description	Example
Slot No./Trunk Group No.	The number of the slot accommodating the uplink card actually used or the number of the Trunk group requiring the MSTP function.	19
Uplink Port No.	The number of the uplink card port actually used.	1
Port-Auto/Edge	Used to set whether the port is an edge port. The options available are **Auto Edge** and **Edge port**.	Auto Edge
Link Type	Set the type of link where the port resides in the network. **Point-to-point** and **Shared** are supported.	Point-to-point

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→Port Parameter** to open the **Port Parameter** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-7.

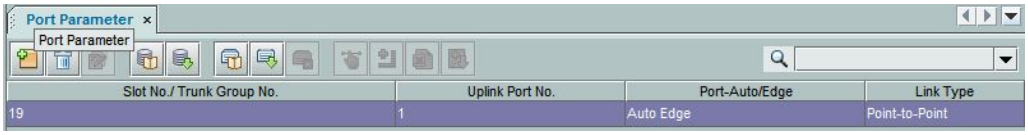


Figure 12-7 Port Parameters

12.1.7 Configuring the MST Region

Configure the region name and version (revision level) of the multiple spanning tree region containing the equipment. The equipment sets in the same region have the same region name and version.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Set it to 1.	1
Version	All the equipment in the same MST region has the same version (edition). The value ranges from 0 to 65535.	0
Region	Set the MST region that the equipment belongs to. All the equipment in the same MST region has the same domain name. The default setting is the MAC address of the equipment.	MST1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→MSTP Region** to open the **MSTP Region** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-8.

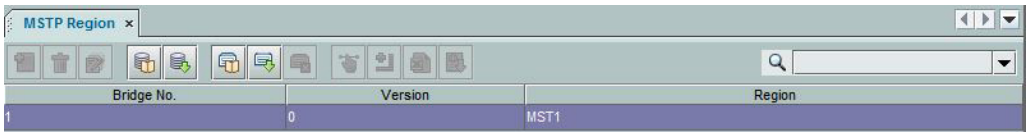


Figure 12-8 The MST Region

12.1.8 Configuring Basic Properties of the Instance

Configure basic properties of the instance, and set up the binding relationship between the multiple spanning tree instance and the VLAN.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Set it to 1.	1
Instance ID	The ID of the spanning tree instance. The value ranges from 1 to 64.	1
VLAN ID	The VLAN ID bound to the spanning tree instance. The value ranges from 1 to 4094.	10

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Instance Basic Properties** to open the **Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a bridge instance configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-9.

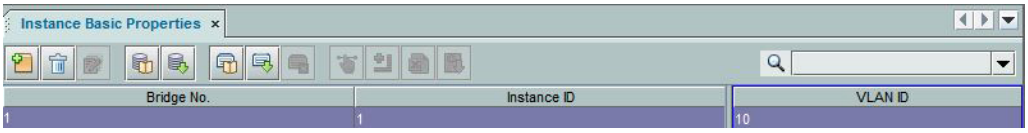


Figure 12-9 Basic Properties of the Instance

12.1.9 Configuring the Port Associated with the Instance

Configure the ports associated with the MST instance to set up the mappings between the instance and the ports.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Set it to 1.	1
Instance ID	The ID of the spanning tree instance. The value ranges from 1 to 64.	1
Slot No./Trunk Group No.	The number of the slot accommodating the uplink card actually used or the number of the Trunk group requiring the MSTP function.	19
Uplink Port No.	The number of the uplink card port actually used.	1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Instance Associate Port** to open the **Instance Associate Port** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a bridge instance configuration entry.
5. Select the right pane, click **Add**, enter **1** in the dialog box that appears, and then click **OK** to add a port configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-10.

Figure 12-10 The Port Associated with the Instance

12.1.10 Configuring Parameters of the Bridge Instance

Configure the priority of the multiple spanning tree instance, which is used in election of the multiple spanning tree instance.

Planning Data

Item	Description	Example
Bridge No.	The number of the equipment. Set it to 1.	1
Instance ID	The ID of the spanning tree instance. The value ranges from 1 to 64.	1
Priority	Set the bridge priority in the instance for electing the MSTI. The value should be an integral multiplex of 4096, and range between 0 and 61440. The default value is 32768.	32768

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Bridge Instance Parameter** to open the **Bridge Instance Parameter** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-11.

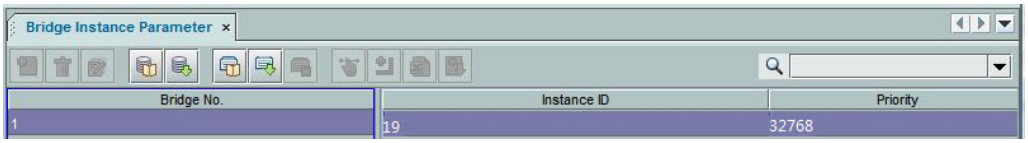


Figure 12-11 Parameters of the Bridge Instance

12.1.11 Configuring Instance Tree Parameters for the Port

Configure the instance tree parameters for the specified port, including the Instance ID, Path-Cost and Priority, etc.

Planning Data

Item	Description	Example
Slot No./Trunk Group No.	The number of the slot accommodating the uplink card actually used or the number of the Trunk group requiring the MSTP function.	19
Uplink Port No.	The number of the uplink card port actually used.	1
Instance ID	The ID of the spanning tree instance. The value ranges from 1 to 64.	1
Path-Cost	Set the path cost of the port in the instance. The value ranges between 1 and 200000000. The default value is 200000000/port rate (the rate unit is kbps).	2000
Priority	Set the port priority in the instance. The value should be an integral multiplex of 16, and range between 0 and 240. The default value is 128.	128

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→MSTP Config→ Interface Instance Parameter** to open the **Interface Instance Parameter** tab.

4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-12.

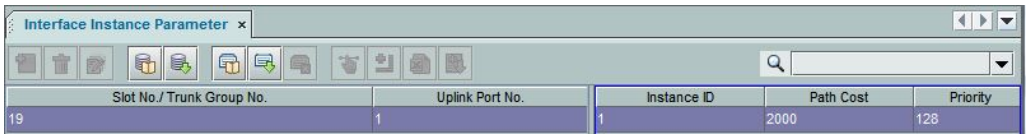


Figure 12-12 Configuring the Instance Tree at the Port

12.1.12 Configuration Result

- In the physical loop composed of equipment sets A, B, and C, multiple logical tree links are formed based on MSTP, so as to avoid infinite loop of packets in the loop network.
- The data from VLAN 10 and other VLANs are transmitted via different links to share data load.

12.2 Configuring the LACP

The following introduces how to configure the LACP for the equipment.

12.2.1 Background Knowledge

Link aggregation means binding two or more physical interfaces together to form a logical data link based on software configuration. The logical link has higher bandwidth and more throughput since bandwidth of the physical interfaces is combined. When a link is faulty, the service data can be automatically switched to another link, which provides higher reliability of data links. Two switches or one switch and one router can be deployed on the two ends of the link.

The LACP protocol based on the IEEE802.3ad standard is a protocol that implements dynamic link aggregation. The LACP protocol exchanges information with the far end via the link aggregation control protocol data unit (LACPDU). After being enabled with the LACP protocol, a port sends the LACPDU to notify the far end of its information such as system priority, system MAC address, port priority, port number and operation key. After receiving the information, the far end compares it with the information of other ports, and selects the ports that can be aggregated. In this way, both ends agree on the ports to join or leave a dynamic aggregation group.

The ports enabled with the LACP can work in two modes: **passive** and **active**.

- In the passive mode, the port does not send the LACPDU messages proactively. After receiving the LACP messages from the far end, the port comes into the protocol computation status.
- In the active mode, the port proactively sends the LACPDU messages to the far end, and makes LACP computations.

The LACP can be classified into static LACP and dynamic LACP in the application layer. Here we focus on the static LACP. The static LACP aggregation group is created by the user. When creating the group, the user designates some specific ports and has the LACP protocol run on them. The link aggregation group then comes into being through negotiation between these designated ports and the ports connected to them on the far end. Namely, members of an aggregation group must be limited to the designated ports. When the link at a member port is interrupted or the port is in the duplex mode, the rate parameters of the port will be inconsistent with those of other ports. In this case, the member port will leave the aggregation group. When conditions are met, the port will rejoin the aggregation group. To delete a member from an aggregation group, manual operation of the user is required.

12.2.2 Example of Configuring the LACP

The following gives an example to introduce how to configure the LACP function. In this example, the static LACP is configured.

12.2.2.1 Network Scenario

Service Planning

Set the three uplink ports of the AN6001-G16 as the member ports of the LACP protection group to enable link backup. Port 1 is used as the master port, and the other two ports as the slave ports.

Network Diagram

The network diagram of the LACP function is as shown in Figure 12-13.

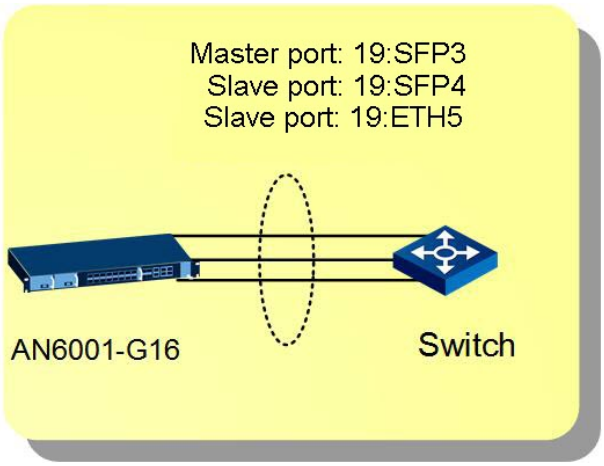


Figure 12-13 Network Diagram for the LACP Function

12.2.2.2 Configuration Flow

Figure 12-14 shows the flow of configuring the LACP function.

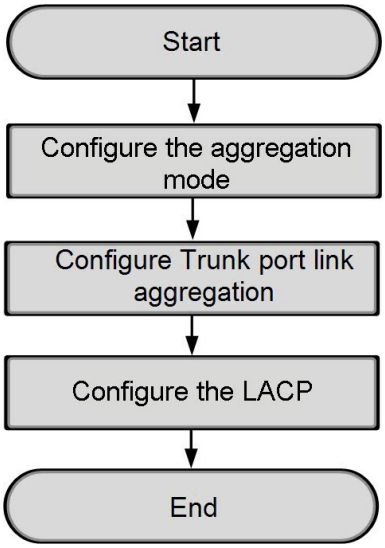


Figure 12-14 Flow of Configuring LACP

12.2.2.3 Configuring the Aggregation Mode

Configure the aggregation mode of the uplink port. Users can select either the manual aggregation or the static LACP mode.

Precautions

- The AN6001-G16 supports two aggregation modes: manual aggregation and static LACP.
- Before configuring the LACP, make sure the settings of the properties such as the rate, duplex type, MTU value and uplink mode of the ports to be configured are consistent.
- Before configuring the LACP, make sure that the member ports are not configured with service VLANs.

Planning Data

Item	Description	Example
Group No.	Configure this item according to the network planning of the operator.	1
Mode	Configure this item according to the network planning of the operator.	Static Lacp

Item	Description	Example
Trunk load balancing criteria	Configure this item according to the network planning of the operator.	SA and DA MAC
member max-num	Configure this item according to the network planning of the operator. The value range is 0 to 6.	6

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Aggregation→ Aggregation Mode Config** to open the **Aggregation Mode Config** tab.
4. Click the **Add** button, enter **1** in the dialog box that appears, and click **OK** to create a new aggregation group mode.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 12-15.

Figure 12-15 Configuring the Aggregation Mode

12.2.2.4 Configuring Trunk Port Link Aggregation

Precautions

For a Trunk group, you can configure only one master port but multiple member ports.

Planning Data

Item	Description	Example
TRUNK Group No.	The group number configured in the aggregation mode.	1
TRUNK Group Master Port	Configure this item according to the network planning of the operator.	19:SFP3
TRUNK Group Member Port	Configure this item according to the network planning of the operator.	19:SFP4, 19:ETH5

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Aggregation→TRUNK Link Aggregation** to open the **TRUNK Link Aggregation** tab.
4. Click the **Add** button, enter **1** in the dialog box that appears, and click **OK** to create a TRUNK group.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 12-16.

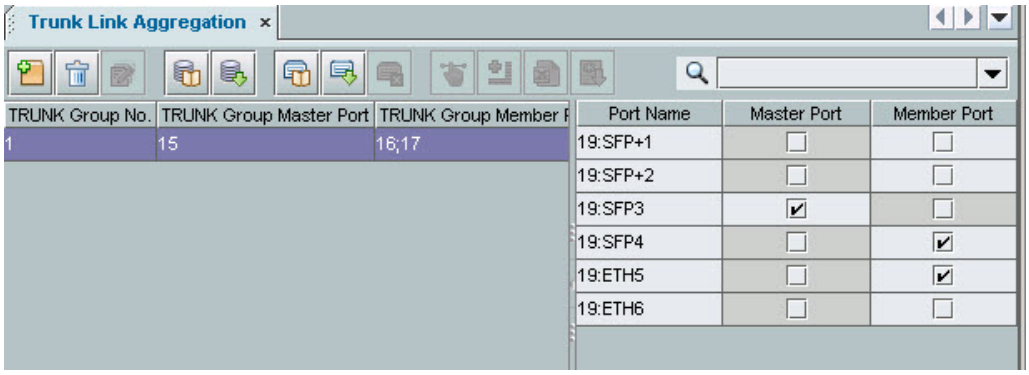


Figure 12-16 Configuring Trunk Port Link Aggregation

12.2.2.5 Configuring the LACP

Configure the LACP protocol switch and system priority.

Planning Data

Item	Description	Example
LACP Switch	The LACP function enable switch. Configure this item according to the network planning of the operator.	Enable
System Priority	Configure this item according to the network planning of the operator. The value range is 0 to 65534.	0

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→LACP→LACP Config** to open the **LACP Config** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 12-17.

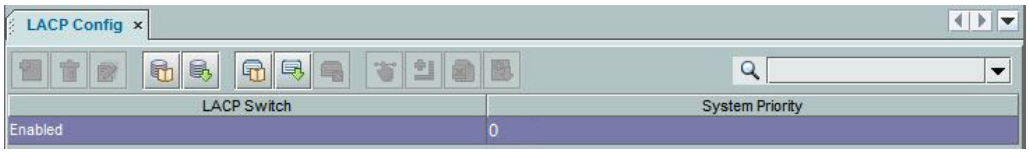


Figure 12-17 Configuring LACP

12.2.2.6 Configuration Result

The LACP function is configured. The ports 19:SFP3, 19:SFP4 and 19:SFP5 constitute a static LACP aggregation group to balance load among member ports in the group and provide more reliable connection in the system.

12.3 Configuring the ERPS

The following introduces how to configure the ERPS function of the AN6001-G16.

12.3.1 Background Knowledge

The Ethernet Ring Protection Switching (ERPS) is an Ethernet ring protection technology defined in the ITU-T G.8032 protocol. The fast switching mechanism and universality of the protocol can protect the link efficiently and guarantee the operation quality of the service.

Components of the ERPS Ring

At the physical layer, all the equipment (such as the AN6001-G16) on the ring nodes should have the ERPS function enabled and constitute one or more physical rings to use the ERPS protocol. The ports on the ring are called ring ports. The ERPS protocol controls connection and disconnection of the ring ports to form link redundancy and handle faults.

At the logical layer, ERPS instances should be created for the equipment on the ring nodes to run the ERPS function. Besides, each ERPS ring needs to be assigned with an exclusive signaling VLAN as a channel for transmitting protocol messages (R-APS message).

Several instances can be created for a physical ring, so that the link can be used in several ERPS rings.

Port Role and Status

There are two types of ring ports on the ERPS ring: RPL owner port and common port.

- RPL owner port: Each ERPS ring has only one RPL owner port. When the link is in normal status, the port is blocked (discarded) to prevent link loops. When the link is faulty, the port is unblocked to forward service messages. When the fault is cleared, the port is blocked again, and the updated status of the port is announced to other ports.

- Common port: The common port forwards service messages, monitors the status of the link directly connected with it, and announces its status to the ports on other nodes. When detecting a fault, the common port triggers the ERPS link protection mechanism to enable the backup link.

The link that is disconnected as the RPL owner port is blocked becomes the ring protection link (RPL).

The ERPS ring port has two statuses:

- A port in the discarding status (being blocked) cannot forward any service messages, but can forward R-APS messages and other Ethernet link protection protocol messages (such as CFM defined in IEEE 802.3ag).
- A port in the forwarding status (being unblocked) can forward service and protocol messages normally.

R-APS Message

As defined by the ITU-T G.8032 standard, the ring automatic protection switching (R-APS) messages are used to inform the ring node equipment of the change in connection status of the links on the ring.

Message Name	Generation Time	Meaning
R-APS (SF)	The link is faulty.	SF means signal failure, indicating that the link signal is lost. The message is sent by the port detecting the link fault. When receiving the SF message, the RPL Owner node will unblock the RPL Owner port .
R-APS (NR)	The link is normal.	NR means no request, indicating that the link is normal and there is no need for requiring change of the port status.
R-APS (NR, NB)	The link returns to normal and the RPL Owner port is blocked again.	It is similar to R-APS (NR), but can only be sent by the RPL Owner port, indicating that the port is blocked again.

Timer

The ITU-T G.8032 protocol defines multiple timers, which are used as the buffer time for the protocol to control the link status changes. This helps avoid the link flapping caused by the port misjudgment on the link status, as a result of delay in transmitting signaling messages or fault correction.

The names, starting time and functions of the timers are described as follows:

Timer Name	Starting Time	Function
WTR timer	It is started when the RPL Owner port receives R-APS (NR) messages.	Reserve the buffer time, and do not block the RPL Owner port until the physical and logical statuses of all ports and links return to normal.
Guard timer	It is started when a faulty node detects that the fault is cleared.	When the guard timer is running, the port does not receive any R-APS (SF) messages from other ports. In this way, the guard timer can prevent the port from receiving or forwarding outdated R-APS (SF) messages. Receiving or forwarding of these outdated R-APS messages may result in further change of the whole link status.
Hold-off timer	It is started when a ring node is faulty.	The hold-off timer holds off the transmission of R-APS (SF) messages. In the set period, the fault will not be detected by the ERPS protocol. If the fault persists at the expiration of the hold-off time, link protection will be implemented based on the ERPS protocol.

12.3.2 Configuration Rules

- Only one RPL owner port needs to be configured on an ERPS ring.
- While configuring tangent rings, make sure the RPL owner port is configured on the equipment at a non-tangent point.

12.3.3 Configuring Single-Ring Single-Instance Protection

The following gives an example to introduce how to configure the single-ring single-instance ERPS protection.

12.3.3.1 Network Scenario

Service Planning

Three AN6001-G16s make up an ERPS protection ring. The link between Equipment 1 and 2 is an RPL link. This ERPS ring protects a single service via one ring instance. The service VLAN ID is 200, and the signaling VLAN ID on the ring is 100.

Network Diagram

The network for the single-ring single-instance ERPS is shown in Figure 12-18.

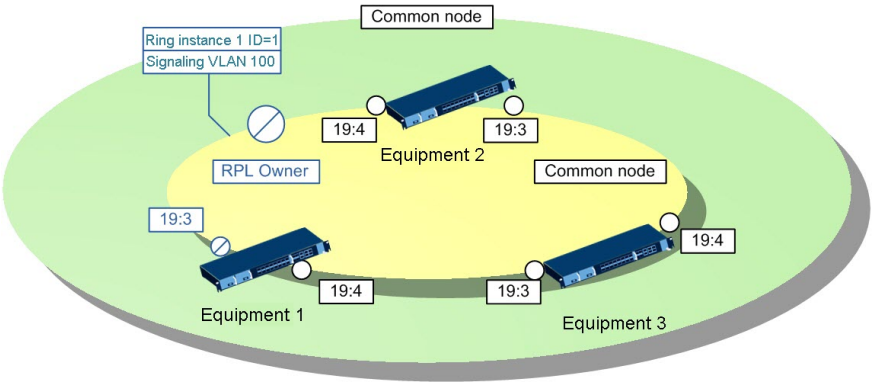


Figure 12-18 ERPS Network - Single Ring and Single Instance

Equipment 1 serves as the RPL Owner of the ERPS ring. Port 19:3 of Equipment 1 serves as the RPL Port and is blocked.

- When the network is normal, the service flow is forwarded in the direction of **Equipment 1→Equipment 3→Equipment 2**.
- When the network between Equipment 1 and Equipment 3 is faulty, the blocked RPL port will be unblocked, so that the service flow can be forwarded in the direction of **Equipment 1→Equipment 2→Equipment 3**. When the fault is cleared and the RPL owner has confirmed the link status, the RPL port will be blocked again, and the service flow will be switched back to the original direction.

12.3.3.2 Configuration Flow

Figure 12-19 shows the flow of configuring the single-ring single-instance ERPS.

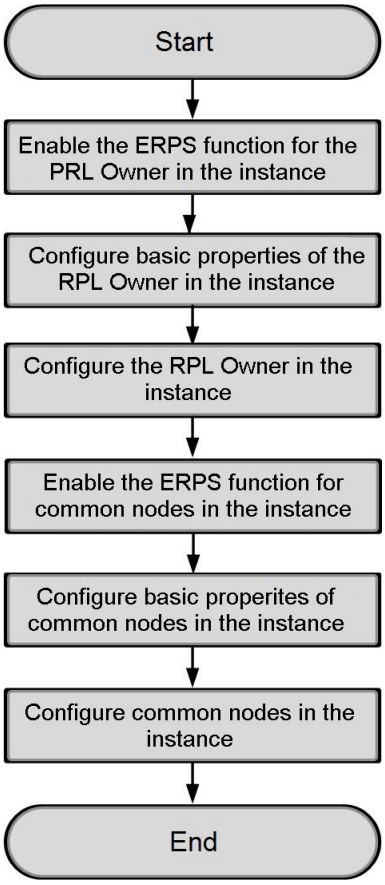


Figure 12-19 Flow of Configuring ERPS - Single Ring and Single Instance

12.3.3.3 Enabling the ERPS Function for the RPL Owner in the Instance

Enable ERPS function of the RPL Owner equipment.

Planning Data

Item	Description	Example
erps switch	Enable or disable the ERPS function.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Configuration Information** to open the **Erps Configuration Information** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-20.

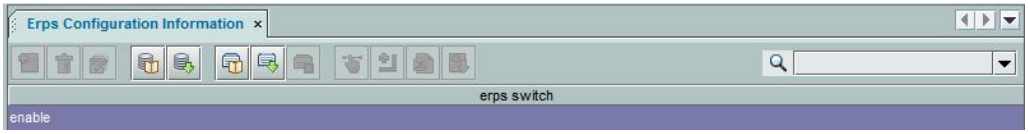


Figure 12-20 ERPS Global Configuration Information

12.3.3.4 Configuring Basic Properties of the RPL Owner in the Instance

Configure the instance ID and the corresponding service VLAN ID on the RPL Owner equipment.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	1
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	200

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.

4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-21.

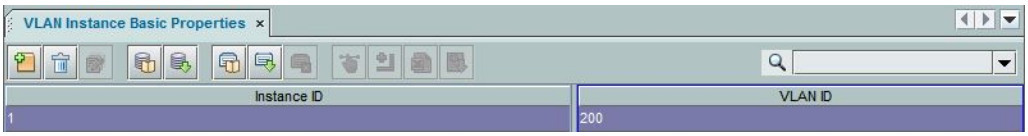


Figure 12-21 Basic Properties of the VLAN Instance - RPL Owner

12.3.3.5 Configuring the RPL Owner in the Instance

Configure ERPS function parameters for the RPL Owner equipment.

Planning Data

Item	Description	Example
Ring ID	The user-defined ID of the ERPS ring.	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	100
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7
Protected Instance	The identifier for the instance to be configured.	1
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	rpl owner
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500

Item	Description	Example
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5
Primary Slot No./Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3
Primary Port_Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	rpl port
Second Slot No./Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port
Virtual Channel	Reserved.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-22.

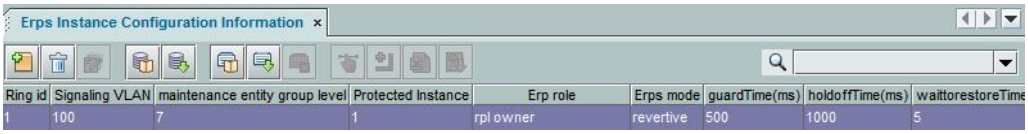


Figure 12-22 ERPS Instance Configuration Information - RPL Owner

12.3.3.6 Enabling the ERPS Function for Common Nodes in the Instance

Enable ERPS function for Equipment 2 and 3.

Planning Data

Item	Description	Example
erps switch	Enable or disable the ERPS function.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Configuration Information** to open the **Erps Configuration Information** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-23.

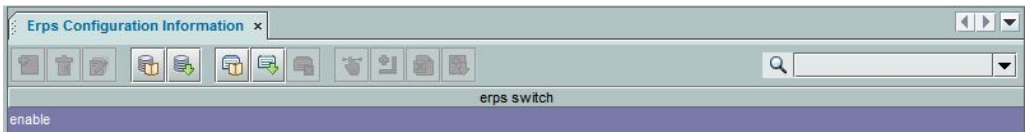


Figure 12-23 ERPS Global Configuration Information

12.3.3.7 Configuring Basic Properties of Common Nodes in the Instance

Configure the instance ID and the corresponding service VLAN ID on Equipment 2 and 3.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	1
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	200

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-24.

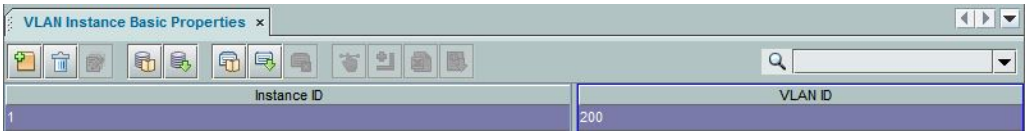


Figure 12-24 Basic Properties of the VLAN Instance - Common Node

12.3.3.8 Configuring Common Nodes in the Instance

Configure the ERPS function parameters for Equipment 2 and 3.

Planning Data

Item	Description	Example
Ring ID	The user-defined ID of the ERPS ring.	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	100
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7
Protected Instance	The identifier for the instance to be configured.	1
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	common node
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5
Primary Slot No./Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3
Primary Port_Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	common port
Second Slot No./Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19

Item	Description	Example
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port
Virtual Channel	Reserved.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-25.

Figure 12-25 ERPS Instance Configuration Information - Common Node

12.3.4 Configuring Single-Ring Multi-Instance Protection

The following gives an example to introduce how to configure the single-ring multi-instance ERPS protection.

12.3.4.1 Network Scenario

Service Planning

Three AN6001-G16s make up an ERPS protection ring. Two ERPS ring instances are created for the ring to protect different services.

Network Diagram

Figure 12-26 shows the network for single-ring multi-instance ERPS.

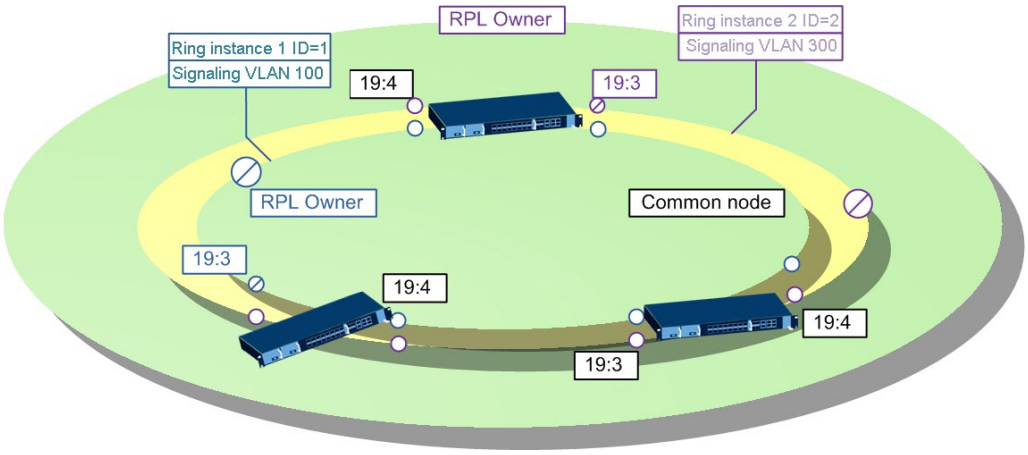


Figure 12-26 ERPS Network - Single Ring and Multiple Instances

The configuration in this example covers two parts: Ring Instance 1 and Ring Instance 2.

- Ring Instance 1 here is configured in the same way as that in the single-ring single-instance application. Equipment 1 serves as the RPL owner in Ring Instance 1; Port 19:3 servers as the RPL port and is blocked. The signaling VLAN ID for Ring Instance 1 is 100.
- In Ring Instance 2, Equipment 2 serves as the RPL owner; Port 19:3 servers as the RPL port and is blocked. The signaling VLAN ID for Ring Instance 2 is 300.

A physical port can be used in different ring instances logically. However, the role of the port is specific to ring instance. That is, the role of the port in one ring instance will not affect the role or message forwarding of the port in other ring instances.

12.3.4.2 Configuration Flow

Figure 12-27 shows the flow of configuring any single instance in the single-ring multi-instance application.

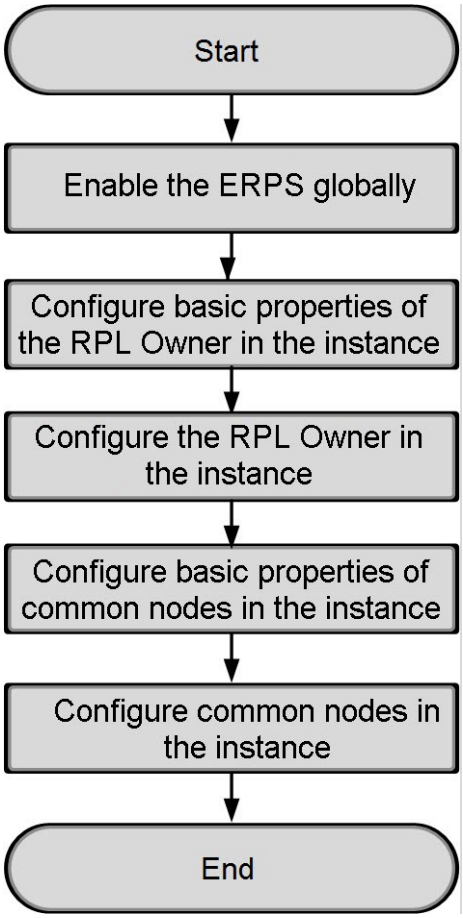


Figure 12-27 Flow of Configuring ERPS - Single Ring and Multiple Instances

12.3.4.3 Enabling the ERPS Globally

Enable the ERPS function for all the equipment in the system.

Planning Data

Item	Description	Example
erps switch	Enable or disable the ERPS function.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Configuration Information** to open the **Erps Configuration Information** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-28.

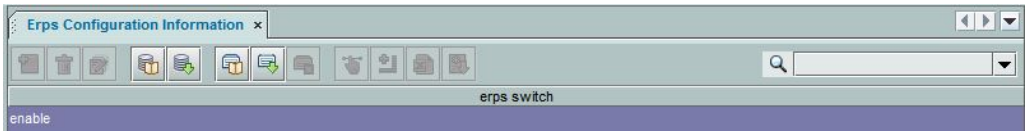


Figure 12-28 ERPS Global Configuration Information

12.3.4.4 Configuring Basic Properties of the RPL Owner in Instance One

On **Equipment 1**, configure instance ID and corresponding service VLAN ID for **Instance One**.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	1
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	200

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-29.

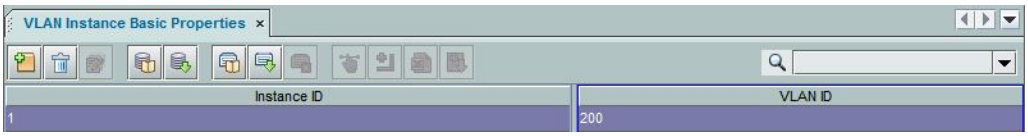


Figure 12-29 Basic Properties of the VLAN Instance - RPL Owner in Instance One

12.3.4.5 Configuring the RPL Owner in Instance One

On **Equipment 1**, configure the ERPS function parameters for **Instance One**, such as port number, port type, signaling VLAN, and timer duration.

Planning Data

Item	Description	Example
Ring ID	The user-defined ID of the ERPS ring.	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	100
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7
Protected Instance	The identifier for the instance to be configured.	1
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	rpl owner
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive

Item	Description	Example
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3
Primary Port_Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	rpl port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port
Virtual Channel	Reserved.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-30.

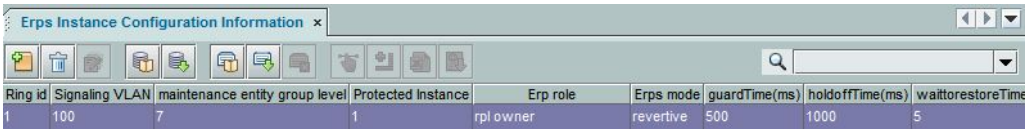


Figure 12-30 ERPS Instance Configuration Information - RPL Owner in Instance One

12.3.4.6 Configuring Basic Properties of Common Nodes in Instance One

Configure instance ID and corresponding service VLAN ID for **Instance One** on **Equipment 2 and 3**.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	1
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	200

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-31.

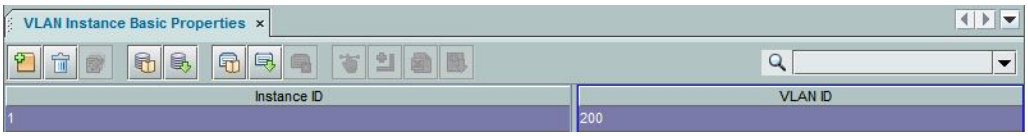


Figure 12-31 Basic Properties of the VLAN Instance - Common Node in Instance One

12.3.4.7 Configuring Common Nodes in Instance One

On **Equipment 2 and 3**, configure the ERPS function parameters for **Instance One**, such as port number, port type, signaling VLAN, and timer duration.

Planning Data

Item	Description	Example
Ring ID	The user-defined ID of the ERPS ring.	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	100
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7
Protected Instance	The identifier for the instance to be configured.	1
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	common node
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive

Item	Description	Example
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3
Primary Port_Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	common port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port
Virtual Channel	Reserved.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-32.

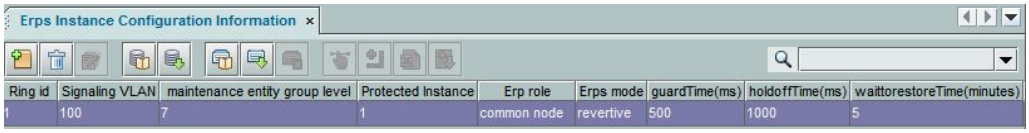


Figure 12-32 ERPS Instance Configuration Information - Common Node in Instance One

12.3.4.8 Configuring Basic Properties of the RPL Owner in Instance Two

On **Equipment 2**, configure instance ID and corresponding service VLAN ID for **Instance Two**.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	2
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	2000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-33.

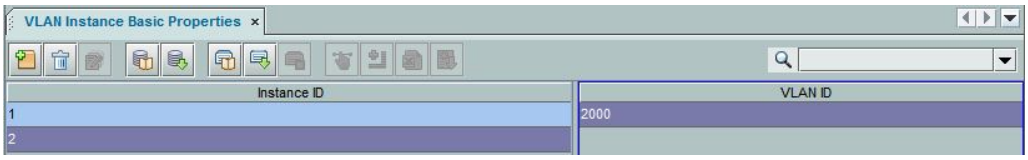


Figure 12-33 Basic Properties of the VLAN Instance - RPL Owner in Instance 2

12.3.4.9 Configuring the RPL Owner in Instance Two

On **Equipment 2**, configure the ERPS function parameters for **Instance Two**, such as port number, port type, signaling VLAN, and timer duration.

Planning Data

Item	Description	Example
Ring ID	The user-defined ID of the ERPS ring.	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	300
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7
Protected Instance	The identifier for the instance to be configured.	2
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	rpl owner
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive

Item	Description	Example
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3
Primary Port_Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	rpl port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port
Virtual Channel	Reserved.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add** to create a configuration entry.
5. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-34.

Figure 12-34 ERPS Instance Configuration Information - RPL Owner in Instance 2

12.3.4.10 Configuring Basic Properties of Common Nodes in Instance Two

Configure instance ID and corresponding service VLAN ID for **Instance Two** on **Equipment 1 and 3**.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	2
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	2000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-35.

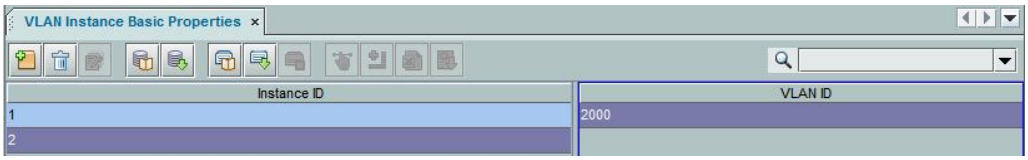


Figure 12-35 Basic Properties of the VLAN Instance - Common Node in Instance 2

12.3.4.11 Configuring Common Nodes in Instance Two

On **Equipment 1 and 3**, configure the ERPS function parameters for **Instance Two**, such as port number, port type, signaling VLAN, and timer duration.

Planning Data

Item	Description	Example
Ring ID	The user-defined ID of the ERPS ring.	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	300
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7
Protected Instance	The identifier for the instance to be configured.	2
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	common node

Item	Description	Example
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3
Primary Port_Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	common port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port
Virtual Channel	Reserved.	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration for Equipment 1 and 3, as shown in Figure 12-36 and Figure 12-37 respectively.

Figure 12-36 ERPS Instance Configuration Information - Common Equipment 1 in Instance 2

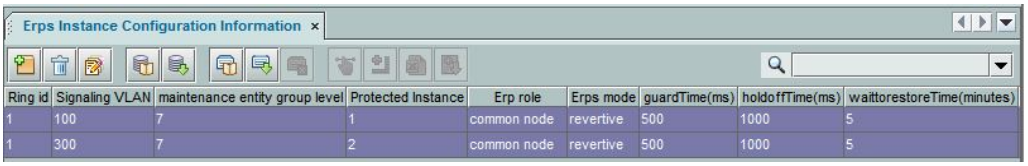


Figure 12-37 ERPS Instance Configuration Information - Common Equipment 3 in Instance 2

12.3.5 Configuring Tangent Ring Protection

The following gives an example to introduce how to configure the tangent-ring ERPS protection.

12.3.5.1 Network Scenario

Service Planning

Five AN6001-G16s constitute two tangent ERPS protection rings. Each ring corresponds to an ERPS instance, and the two instances protect different services.

Network Diagram

Figure 12-38 shows the network for tangent-ring ERPS.

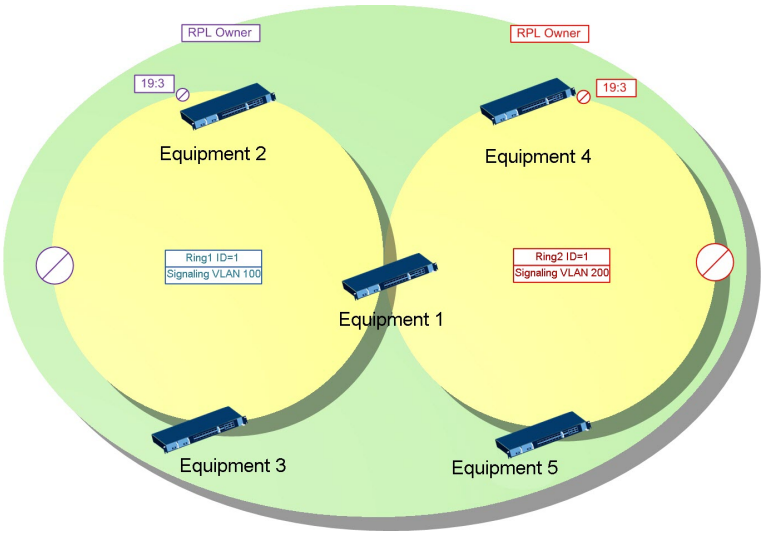


Figure 12-38 Network Diagram for ERPS in the Tangent Ring Mode

The configuration in this example covers three parts: the equipment at the non-tangent points of Ring 1 (including Equipment 2 and 3), the equipment at the non-tangent points of Ring 2 (including Equipment 4 and 5), and the equipment at the tangent point (Equipment 1).

- Ring 1: Equipment 2 acts as the RPL Owner, and Port 19:3 as the RPL port which is blocked. With the signaling VLAN ID 100 and the ring ID 1, the ring protects the service with the VLAN ID 1000.
- Ring 2: Equipment 4 acts as the RPL owner, and Port 19:3 as the RPL port which is blocked. With the signaling VLAN ID 200 and the ring ID 2, the ring protects the service with the VLAN ID 2000.

- Equipment at the tangent point: Equipment 1 acts as the tangent point of the two rings. Two instances need to be created for the equipment to correspond to the signaling transmission for the two rings respectively.

Table 12-1 shows the mappings between the ERPS instances on the equipment and rings in the example.

Table 12-1 Mappings between Equipment Role, ERPS Instance and Ring

Equipment Name	Equipment Role	Ring Corresponding to Instance 1	Ring Corresponding to Instance 2
Equipment 1	Equipment at the tangent point	Ring 1	Ring 2
Equipment 2	RPL owner of Ring 1	Ring 1	N/A
Equipment 3	Common node of Ring 1	Ring 1	N/A
Equipment 4	RPL owner of Ring 2	N/A	Ring 2
Equipment 5	Common node of Ring 2	N/A	Ring 2

12.3.5.2 Configuration Flow

Figure 12-39 shows the flow of configuring ERPS in the tangent-ring mode.

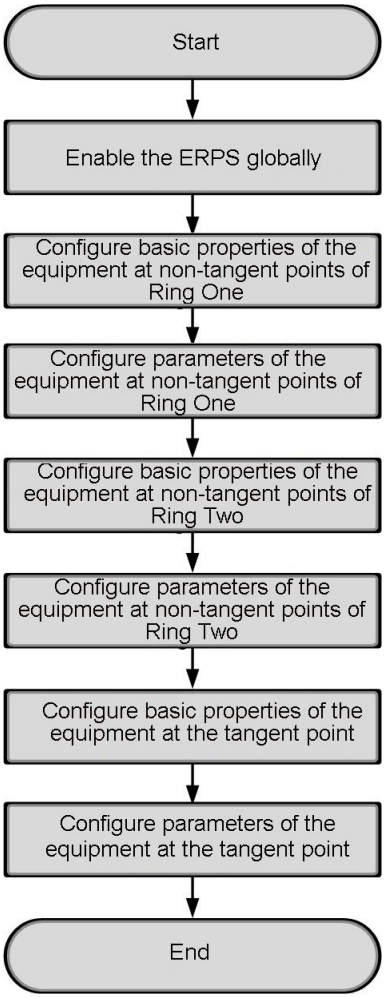


Figure 12-39 Flow of Configuring ERPS in the Tangent Ring Mode

12.3.5.3 Enabling the ERPS Globally

Enable the ERPS function for all the equipment in the system.

Planning Data

Item	Description	Example
erps switch	Enable or disable the ERPS function.	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Configuration Information** to open the **Erps Configuration Information** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-40.

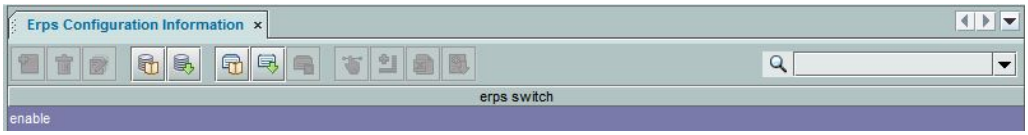


Figure 12-40 ERPS Global Configuration Information

12.3.5.4 Configuring Basic Properties of the Equipment at Non-Tangent Points of Ring One

On **Equipment 2 and 3**, configure the instance ID and corresponding service VLAN ID for **Ring One**.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	1
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	1000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-41.

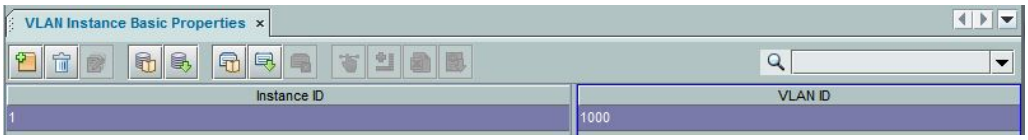


Figure 12-41 Basic Properties of the VLAN Instance - Non-tangent Point of Ring 1

12.3.5.5 Configuring Parameters of the Equipment at Non-Tangent Points of Ring One

On **Equipment 2 and 3**, configure the ERPS function parameters for **Ring One**, such as port number, port type, signaling VLAN, and timer duration.

Planning Data

Item	Description	Example	
		Equipment 2	Equipment 3
Ring ID	The user-defined ID of the ERPS ring.	1	1
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	100	100
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7	7
Protected Instance	The identifier for the instance to be configured.	1	1

Item	Description	Example	
		Equipment 2	Equipment 3
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	rpl owner	common node
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive	revertive
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3	3
Primary Port_ Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	rpl port	common port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4	4

Item	Description	Example	
		Equipment 2	Equipment 3
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port	common port
Virtual Channel	Reserved.	-	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration for Equipment 2 and 3, as shown in Figure 12-42 and Figure 12-43.

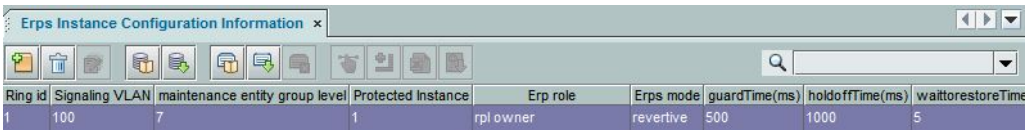


Figure 12-42 ERPS Instance Configuration Information - RPL Owner Equipment 2 at Non-tangent Point of Ring 1

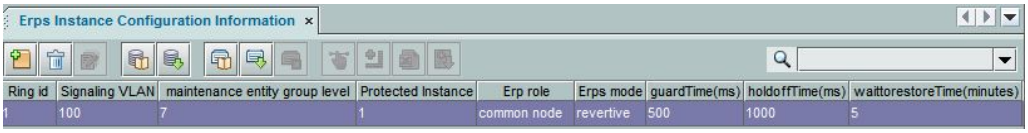


Figure 12-43 ERPS Instance Configuration Information - Common Equipment 3 at Non-tangent Point of Ring 1

12.3.5.6 Configuring Basic Properties of the Equipment at Non-Tangent Points of Ring Two

On **Equipment 4 and 5**, configure the instance ID and corresponding service VLAN ID for **Ring Two**.

Planning Data

Item	Description	Example
Instance ID	The ID of the ERPS instance, which is designated by the user.	1
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	2000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-44.

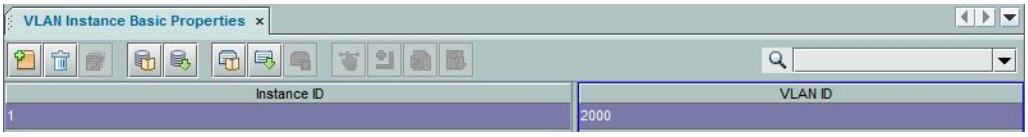


Figure 12-44 Basic Properties of the VLAN Instance - Non-tangent Point of Ring 2

12.3.5.7 Configuring Parameters for the Equipment at Non-Tangent Points of Ring Two

On **Equipment 4 and 5**, configure the ERPS function parameters for **Ring Two**, such as port number, port type, signaling VLAN, and timer duration.

Planning Data

Item	Description	Example	
		Equipment 4	Equipment 5
Ring ID	The user-defined ID of the ERPS ring.	2	2
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	200	200
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7	7
Protected Instance	The identifier for the instance to be configured.	1	1
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	rpl owner	common node
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive	revertive
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000	1000

Item	Description	Example	
		Equipment 4	Equipment 5
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3	3
Primary Port_ Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	rpl port	common port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4	4
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port	common port
Virtual Channel	Reserved.	-	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration for Equipment 4 and 5, as shown in Figure 12-45 and Figure 12-46.

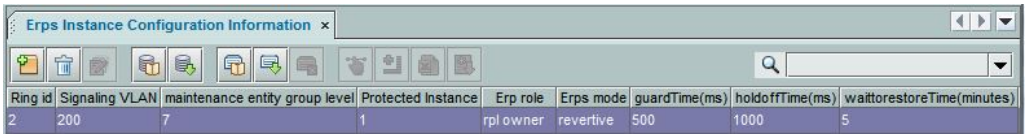


Figure 12-45 ERPS Instance Configuration Information - RPL Owner Equipment 4 at Non-tangent Point of Ring 2

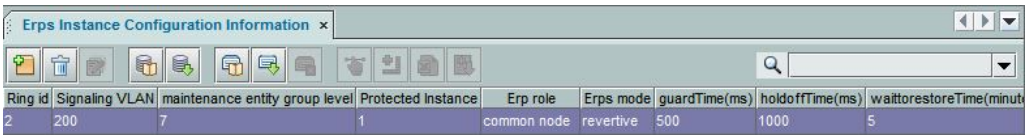


Figure 12-46 ERPS Instance Configuration Information - Common Equipment 5 at Non-tangent Point of Ring 2

12.3.5.8 Configuring Basic Properties of the Equipment at the Tangent Point

Create ERPS instances for **Ring One** and **Ring Two** on **Equipment 1**, and set up the mappings between the ERPS instances and service VLAN IDs.

Planning Data

Item	Description	Example	
		Ring 1	Ring 2
Instance ID	The ID of the ERPS instance, which is designated by the user.	1	2
VLAN ID	The VLAN ID of the services protected by the ERPS. The value ranges from 1 to 4094.	1000	2000

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→VLAN Instance Basic Properties** to open the **VLAN Instance Basic Properties** tab.

4. Select the left pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add an instance ID configuration entry.
5. Select the right pane, click **Add**, enter **1** in the displayed dialog box and then click **OK** to add a VLAN ID configuration entry.
6. Configure the parameters according to the planning data for **Ring One**.
7. Follow the steps 4 to 6 and configure the parameters according to the planning data for **Ring Two**.
8. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-47.

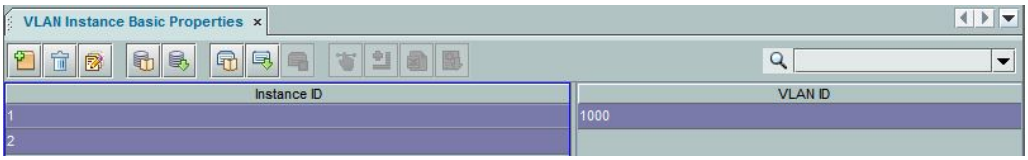


Figure 12-47 Basic Properties of the VLAN Instance - Tangent Point

12.3.5.9 Configuring Parameters of the Equipment at the Tangent Point

Configure functional parameters for the two ERPS instances on **Equipment 1**, such as port number, port type, signaling VLAN and timer duration.

Planning Data

Item	Description	Example	
		Ring 1	Ring 2
Ring ID	The user-defined ID of the ERPS ring.	1	2
Signaling VLAN	The VLAN ID used for transmitting ERPS signaling.	100	200
Maintenance entity group level	Configure the MEL value in the R-APS message. The value ranges from 0 to 7, and the default value is 7 (the highest level).	7	7
Protected Instance	The identifier for the instance to be configured.	1	2

Item	Description	Example	
		Ring 1	Ring 2
Erp role	The role of the equipment on the ERPS ring: RPL Owner or Common Node. A ring instance can be configured with only one RPL Owner.	common node	common node
Erps mode	Configure whether it is allowed to switch to another fault detection mode after the fault is cleared in the network.	revertive	revertive
Guard Time (ms)	The guard timer is a type of R-APS timers and is used to prevent ring nodes from receiving outdated R-APS messages and mistakenly unblocking the port, so to avoid the network loop. When the guard timer is running, the ring node discards the R-APS message that arrives. When the guard timer expires, the received R-APS message is forwarded.	500	500
Holdoff Time (ms)	Configure the delay time from the fault occurrence to the status switching (from blocked to unblocked) at the RPL owner port. When the hold-off timer is running, the fault is not reported to the ERPS scheme for processing.	1000	1000
Wait-to-restore Time (minutes)	Configure the time waited for the RPL Owner port to restore to the blocking status after the fault is cleared.	5	5
Primary Slot No. /Trunk Group No.	The slot number or Trunk group number of the first uplink port for the equipment on the ERPS ring.	Slot:19	Slot:19
Primary Uplink Port No.	The number of the first uplink port for the equipment on the ERPS ring.	3	3
Primary Port_ Role	The role of the uplink port: RPL Port or Common Port. An ERPS ring can be configured with only one RPL Port.	common port	common port
Second Slot No. /Trunk Group No.	The slot number or Trunk group number of another uplink port for the equipment on the ERPS ring.	Slot:19	Slot:19
Second Uplink Port No.	The number of another uplink port for the equipment on the ERPS ring.	4	4

Item	Description	Example	
		Ring 1	Ring 2
Secondary Port	The role of the uplink port: RPL Port or Common Port.	common port	common port
Virtual Channel	Reserved.	-	-

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→Erps Config→Erps Instance Configuration Information** to open the **Erps Instance Configuration Information** tab.
4. Click **Add**, enter **2** in the dialog box that appears, and click **OK** to add two configuration entries.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 12-48.

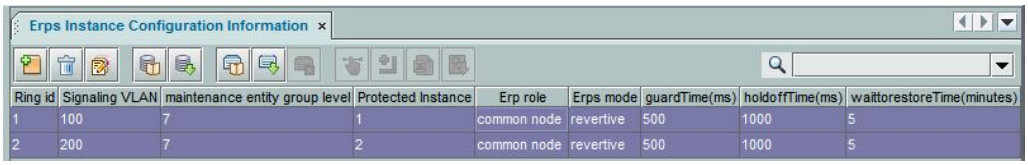


Figure 12-48 ERPS Instance Configuration Information - Tangent Point

13 Configuring Traffic Classification

The following introduces the traffic classification configuration example.

- Configuration Example for Traffic Classification Based on the L4 Source Port
- Configuration Example for Traffic Classification Based on the SVLAN

13.1 Configuration Example for Traffic Classification Based on the L4 Source Port

The following introduces the traffic classification configuration example based on L4 source port.

13.1.1 Configuration Flow

Figure 13-1 shows the flow of configuring traffic classification based on the L4 source port.

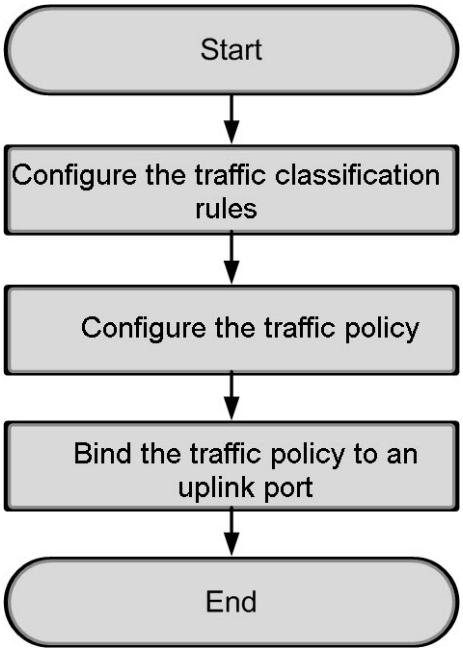


Figure 13-1 Flow of Configuring Traffic Classification Based on the L4 Source Port

13.1.2 Configuring the Traffic Classification Rules

Configure the traffic classification rules. When a traffic flow complies with the configured rules, the equipment will react according to the set rules.

Precautions

- When the traffic classification object is an uplink port, only the downlink traffic policy and downlink rule are valid.

- When the traffic classification object is a main card port, only the uplink traffic policy and uplink rule are valid.
- When the traffic classification object is an ONU port, both the uplink and downlink traffic policies and the uplink and downlink rules are valid.

Planning Data

Item	Description	Example
Rule Name	Set the name of the rule.	Rule1
Rule Type	Set the type of the rule, e.g., the object to be based on for matching.	L4 SA Port
Operator	Set the logical conditions for rule matching.	=
Rule Domain Value	Set the rule matching value.	111

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **QoS Config→Flow Classification Rule** to open the **Flow Classification Rule** tab.
4. Click **Add**, and enter **1** in the dialog box that appears. Click **OK** to create a new traffic classification rule.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 13-2.

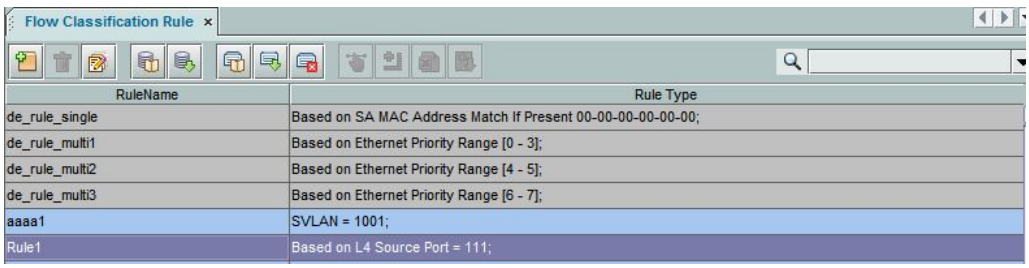


Figure 13-2 Traffic Classification Rule Based on the L4 Source Port

13.1.3 Configuring the Traffic Policy

Configure the traffic policy, and the equipment will take corresponding forwarding action on the traffic based on the rule matching condition.

Planning Data

Item	Description	Example
Policy Name	Set the name of the policy.	Policy1
Precedence	Set the priority of the policy.	1
ACL Enable	Enable the ACL function.	Enable
Forward	Configure this item according to the network planning of the operator.	Forbidden, Matched streams would be dropped.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **QoS Config→Flow Policy** to bring up the **Flow Policy** tab.
4. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to create a traffic policy.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 13-3.

Figure 13-3 Traffic Policy Based on the L4 Source Port

13.1.4 Binding the Traffic Policy to an Uplink Port

Bind the traffic policy to a designated uplink port so as to apply the policy to the port.

Planning Data

Item	Description	Example
Object Type	The type of the object to be bound	Uplink Port
Slot No.	Set the slot number of the uplink card.	19
Port No.	Set the uplink port number.	2
Egress Policy ID	Set the traffic policy to be bound.	Policy1
Egress Rule ID	Set the flow rule to be bound.	Rule1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **QoS Config→Flow Policy Binding** to bring up the **Flow Policy Binding** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to create an object configuration entry.
5. Select the right pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to create a configuration entry for binding traffic policy.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 13-4.

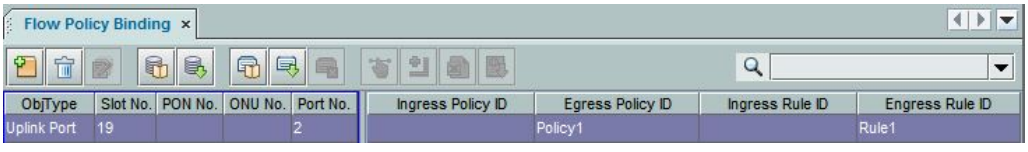


Figure 13-4 Binding the Traffic Policy Based on the L4 Source Port

13.1.5 Configuration Result

The AN6001-G16 can process data traffic of different types according to the set rules.

13.2 Configuration Example for Traffic Classification Based on the SVLAN

The following introduces the traffic classification configuration example based on SVLAN.

13.2.1 Configuration Flow

Figure 13-5 shows the flow of configuring traffic classification based on the SVLAN source port.

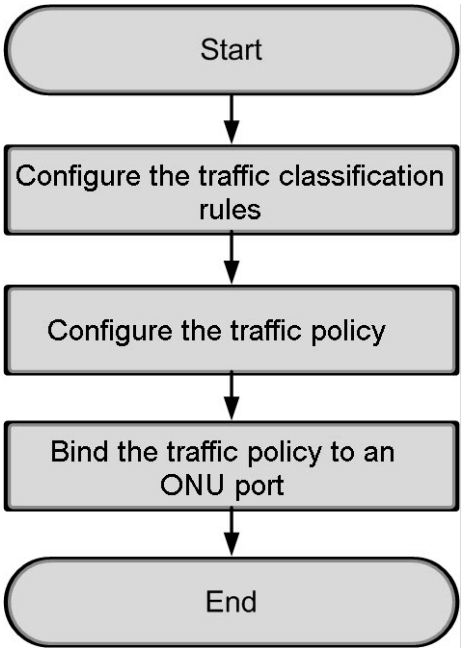


Figure 13-5 Flow of Configuring Traffic Classification Based on the SVLAN

13.2.2 Configuring the Traffic Classification Rules

Configure the traffic classification rules. When a traffic flow complies with the configured rules, the equipment will react according to the set rules.

Precautions

- When the traffic classification object is an uplink port, only the downlink traffic policy and downlink rule are valid.
- When the traffic classification object is a main card port, only the uplink traffic policy and uplink rule are valid.
- When the traffic classification object is an ONU port, both the uplink and downlink traffic policies and the uplink and downlink rules are valid.

Planning Data

Item	Description	Example
Rule Name	Set the name of the rule.	Rule2
Rule Type	Set the type of the rule, e.g., the object to be based on for matching.	SVLAN
Operator	Set the logical conditions for rule matching.	=
Rule Domain Value	Set the rule matching value.	100

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **QoS Config→Flow Classification Rule** to open the **Flow Classification Rule** tab.
4. Click **Add**, and enter **1** in the dialog box that appears. Click **OK** to create a new traffic classification rule.
5. Configure the parameters according to the planning data.

6. Click the **Create on Device** button to complete the configuration, as shown in Figure 13-6.

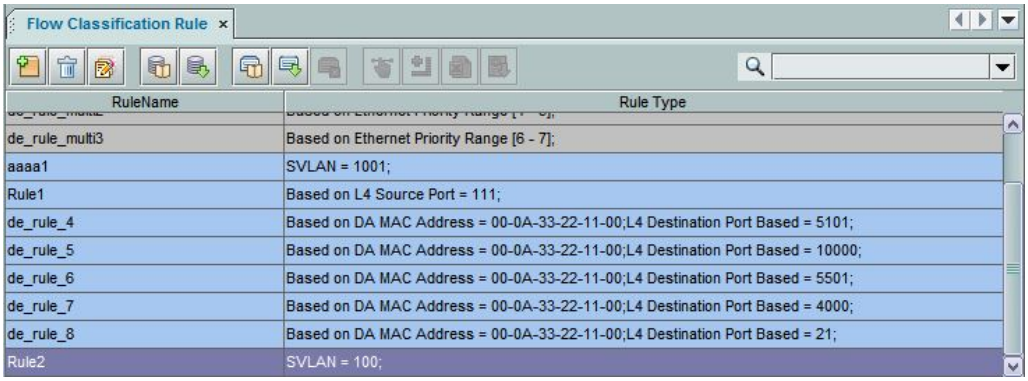


Figure 13-6 Traffic Classification Rule Based on SVLAN

13.2.3 Configuring the Traffic Policy

Configure the traffic policy, and the equipment will take corresponding forwarding action on the traffic based on the rule matching condition.

Planning Data

Item	Description	Example
Policy Name	Set the name of the policy.	Policy2
Precedence	Set the priority of the policy.	1
ACL Enable	Enable the ACL function.	Enable
Forward	Configure this item according to the network planning of the operator.	Forbidden, Matched streams would be dropped.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **QoS Config→Flow Policy** to bring up the **Flow Policy** tab.

4. Click **Add**, enter **1** in the dialog box that appears, and click **OK** to create a traffic policy.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 13-7.

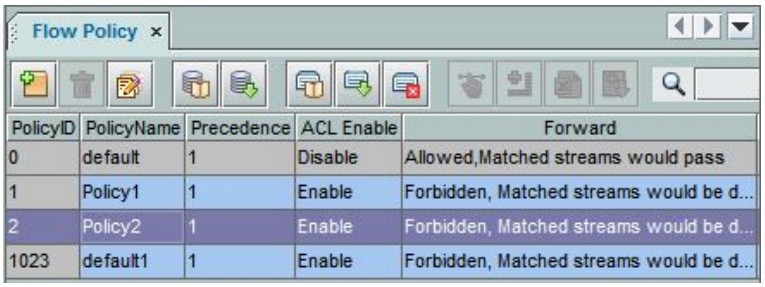


Figure 13-7 Traffic Policy Based on SVLAN

13.2.4 Binding the Traffic Policy to an ONU Port

Bind the traffic policy to a designated ONU port so that the policy can be applied to the port.

Planning Data

Item	Description	Example
Object Type	Select the type of the object to be bound.	ONU Port
Slot No.	Select the slot housing the card connected to the ONU.	1
PON No.	Select the number of the PON port connected to the ONU.	1
ONU No.	Enter the authorization number of the ONU.	1
Port No.	Enter the number of the ONU port.	1
Egress Policy ID	Select the traffic policy to be bound.	Policy2
Egress Rule ID	Select the flow rule to be bound.	Rule2

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **QoS Config→Flow Policy Binding** to bring up the **Flow Policy Binding** tab.
4. Select the left pane, click **Add**, enter **1** in the displayed dialog box, and click **OK** to create an object configuration entry.
5. Select the right pane, click **Add**, enter **1** in the dialog box that appears, and click **OK** to create a configuration entry for binding traffic policy.
6. Configure the parameters according to the planning data.
7. Click the **Create on Device** button to complete the configuration, as shown in Figure 13-8.

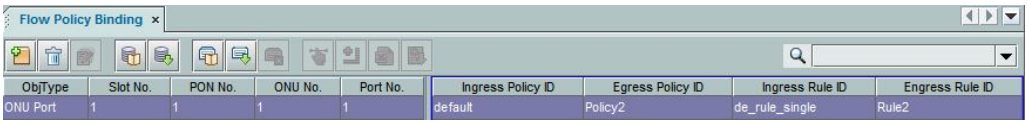


Figure 13-8 Binding the Traffic Policy Based on SVLAN

13.2.5 Configuration Result

The AN6001-G16 can process data traffic of different types according to the set rules.

14 Configuring Subscriber Line Identifiers

The following introduces how to configure the subscriber line identifier for the equipment.

☑ Background Knowledge

☑ Configuration Rules

☑ Example of Configuring Subscriber Line Identifiers

14.1 Background Knowledge

Figure 14-1 illustrates the signal flow of the subscriber line identifier.

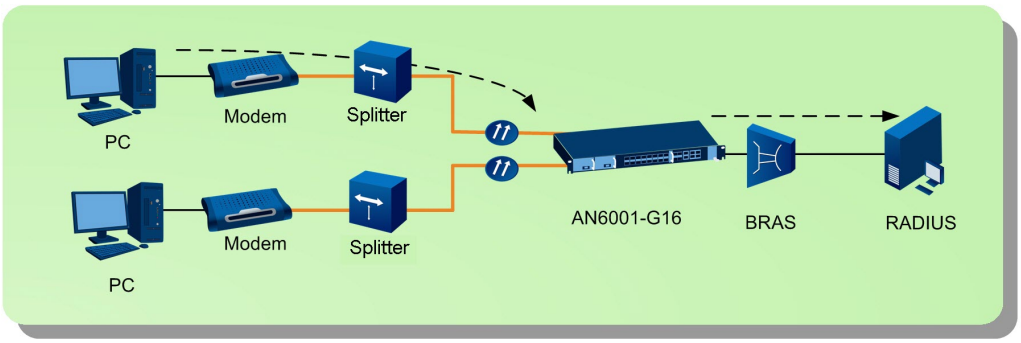


Figure 14-1 Signal Flow of the Subscriber Line Identifier

1. The AN6001-G16 system captures specific messages (DHCP DISCOVER, DHCP REQUEST, PADI and PADR) in the uplink direction and adds the line identifier information to the messages based on the configured format. The identifier information is the physical information of the subscribers sending the messages.
2. The AN6001-G16 forwards the messages inserted with the identifier information to the broadband remote access server (BRAS). After receiving the messages, the BRAS adds the line information to the messages and forwards them to the remote authentication dial-in user service (RADIUS) server.
3. The RADIUS server performs the authentication, authorization and accounting (AAA) function based on the identifier information.

Note:

The background knowledge mentioned above is based on the protocol DHCP in the IPv4 environment.

14.2 Configuration Rules

See below for details about custom line identifiers.

- The system defines some custom identifier variables. You can use these variables in different combinations to enhance flexibility of the identification function. Table 14-1 lists the custom identifier variables defined by the system.

Table 14-1 Custom Identifier Variables

Identifier	Meaning	Identifier	Meaning
%s	SVLAN	%o	ONU Authorization Number
%c	CVLAN	%n	ONU Type
%a	Access Node ID	%T	MDU ONU Slot No.
%r	Access Node Rack No.	%M	MDU ONU Sub-slot No.
%f	Access Node Shelf No.	%P	MSAN UNI Port No.
%S	Access Node Slot No.	%t	ONU User End Port Type
%p	Access Node PON Port No.	%X	Port VPI or SVLAN
%m	Access Node ONU ID (MAC)	%x	Port VCI or CVLAN
%u	Uplink Port Type	%I	IAD IP Address
%L	Service Card Type	%A	IAD MAC Address
%O	OLT Management VLAN	%B	Access Node Type: OLT, DSL or LAN

- The custom format is subject to the following restrictions.
  - In the custom format, a variable identifier must be separated from the subsequent character string or variable by a delimiter. The delimiter should be one of the characters listed in Table 14-2.

Table 14-2 List of Delimiters

Separator	Meaning
	Space
.	Decimal point
/	Slash
;	Semicolon
:	Colon
{	Open curly bracket
}	Close curly bracket
<	Open angle bracket
>	Close angle bracket
[	Open square bracket
]	Close square bracket

- The character string in the custom format should contain no more than 256 characters.
- The aforesaid delimiters are not allowed in the values of variables.

14.3 Example of Configuring Subscriber Line Identifiers

The following gives an example to introduce how to configure subscriber line identifier.

14.3.1 Configuration Flow

Figure 14-2 shows the flow of configuring the subscriber line identifier.

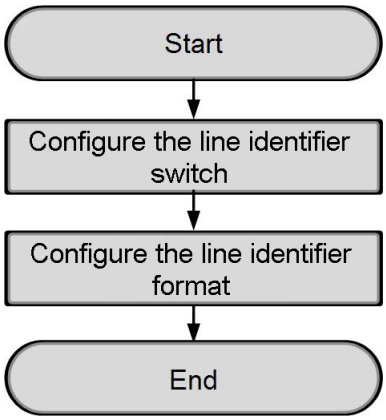


Figure 14-2 Flow of Configuring the Subscriber Line Identifier Management

14.3.2 Configuring the Line Identifier Switch

Configure parameters relevant to the line identifier. Select the access node identifier mode for the AN6001-G16 and add the rack number and shelf number into the DHCP or PPPoE request message.

Precautions

The AN6001-G16 supports three identifier modes: DHCP Option82, DHCP Option18 and PPPoE+.

Planning Data

Item	Description	Example
Option82 Switch	Configure this item according to the network condition.	Enable
Option18 Switch	Configure this item according to the network condition.	Enable
PPPoE+ Switch	Configure this item according to the network condition.	Enable
Access Node Identifier	Configure this item according to the planning of the operator.	AN6001-G16
ANI_rack	Configure this item according to the planning of the operator.	1
ANI_frame	Configure this item according to the planning of the operator.	1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Function→ Line Identifier Management** to bring up the **Line Identifier Management** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 14-3.

Figure 14-3 Line Identifier Management

14.3.3 Configuring the Line Identifier Format

Configure the format of line identifier, and add the user information and equipment information into the data packet to facilitate management of the upper-level BRAS equipment.

Precautions

The AN6001-G16 supports the user-defined identifier format.

Planning Data

Item	Description	Example
Use CTC Format / Use CNC Format / Custom Format	Configure this item according to the network condition.	Use CTC Format
Custom Character String	Configure this item according to the planning of the operator. Applicable only to the custom format.	-
Line Identifier Variable	Configure this item according to the planning of the operator. Applicable only to the custom format.	SVLAN
		CVLAN
		Access Node ID
		Access Node Rack No.
		Access Node Shelf No.
		Access Node Slot No.
		Access Node PON Port No.
		Access Node ONU ID (MAC)
		MDU ONU UNI Port Number

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Ethernet Config→DHCP Function→ Circuit ID Format** to bring up the **Circuit ID Format** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 14-4.

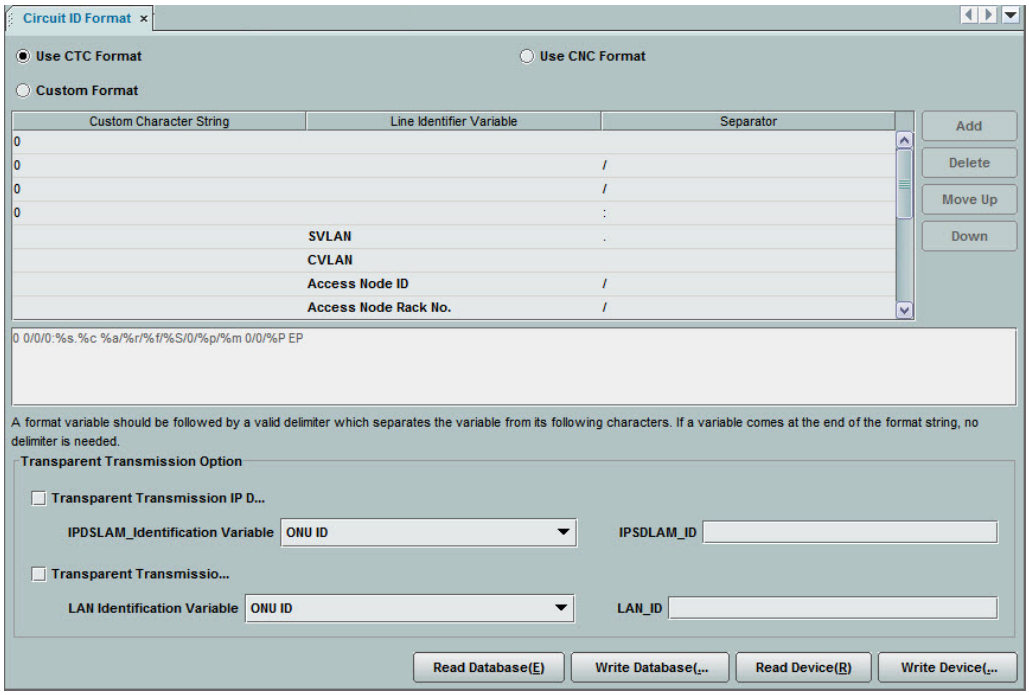


Figure 14-4 Line Identifier Format

14.3.4 Configuration Result

The line identifier of the user equipment can be resolved successfully by the packet capture software.

15 Configuring TACACS+

The following introduces how to configure the Tacacs+ function.

☑ Background Knowledge

☑ Example of Configuring Tacacs+

15.1 Background Knowledge

The Tacacs+ (Terminal Access Controller Access-Control System Plus) protocol is a user access control protocol based on the C-S mode. The protocol is mainly used for user authentication, authorization and accounting (i.e., the AAA function). The protocol is based on TCP for service transmission and uses Port 49 for communication.

The AAA function is a network security management mechanism integrating three functions: authentication, authorization and accounting. The following describes each function in details.

- Authentication: confirms whether the user's identity is valid.
- Authorization: assigns varied access authorities to different users, restricting the operations and services available to them.
- Accounting: records the user operation information such as the types of services used by the user, the destination address of the access, the access duration and the flow statistics, and calculates the charges based on the aforesaid records.

In the aforesaid application, the AN6001-G16 serves as the access equipment for the communication between users and the Tacacs+ server. It authenticates, authorizes and accounts the user access according to the user information on the Tacacs+ server to implement the user access control function based on the Tacacs+ protocol.

15.2 Example of Configuring Tacacs+

The following gives an example to introduce how to get authenticated and login using the Tacacs+ protocol.

15.2.1 Configuration Flow

Figure 15-1 shows the flow of configuring the Tacacs+ function.

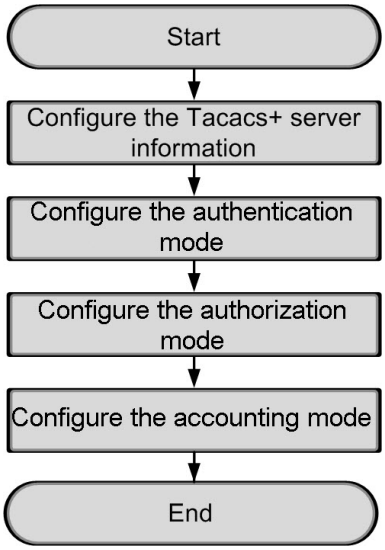


Figure 15-1 Flow of Configuring Tacacs+

15.2.2 Configuring Information about the Tacacs+ Server

Configure the communication mode of the Tacacs+ server.

Planning Data

Item	Description	Example	
IP Address	Set the VLAN ID of Super VLAN.	10.99.110.10	10.99.110.11
Server Port	The TCP port number. Port 49 is used by default.	49	
Key	The password for the user to log in.	123	
Timeout (s)	The time threshold set to ascertain whether the connection between the user and the server times out.	5	

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Common Config→Tacacs+ Server Information** to open the **Tacacs+ Server Information** tab.
4. Click **Add**, enter **2** in the dialog box that appears, and then **OK** to add two Tacacs+ server configuration entries.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 15-2.

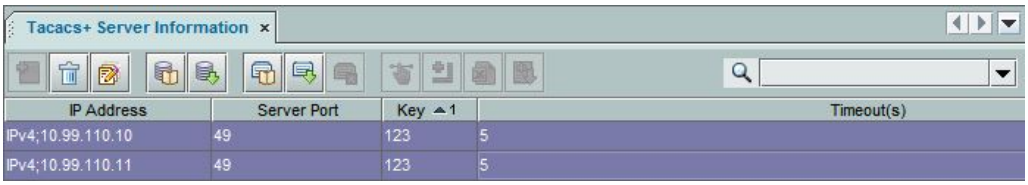


Figure 15-2 Tacacs+ Server Information

15.2.3 Configuring the Authentication Mode

Configure the user authentication mode.

Planning Data

Item	Description	Example
Authentication Mode	The options include "Local Mode", "Radius Mode" and "Tacacs+ Mode".	Tacacs+ Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Common Config→Authentication** to bring up the **Authentication** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 15-3.

Figure 15-3 Authentication - Tacacs+

15.2.4 Configuring the Authorization Mode

Enable the user authority and set the command line authorization mode.

Planning Data

Item	Description	Example
Get User Privilege Mode	Enable or disable the function. Select "Enable" in this example.	Enable
Command Line Authorization Mode	The options include "None" and "Tacacs+ Mode". Select "Tacacs+ Mode" in this example to obtain the command line authorization information.	Tacacs+ Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Common Config→Authorization** to bring up the **Authorization** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 15-4.

Figure 15-4 Authorization

15.2.5 Configuring the Accounting Mode

Configure whether to enable accounting and set the accounting mode.

Planning Data

Item	Description	Example
Record User Information Mode	The options include "None" and "Tacacs+ Mode". Select "Tacacs+ Mode" in this example to record the user information.	Tacacs+ Mode
Command Line Accounting Mode	The options include "None" and "Tacacs+ Mode". Select "Tacacs+ Mode" in this example for accounting.	Tacacs+ Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Common Config→Accounting** to bring up the **Accounting** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 15-5.

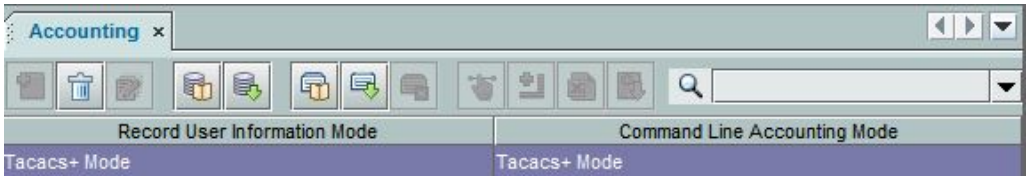


Figure 15-5 Accounting

15.2.6 Configuration Result

After completing the configuration, users can log in with the configured key. Since authentication is implemented in the Tacacs+ mode, users cannot log in with local user name and password.

- Below is the echo information when the login fails.

  ```
  Login:GEPON Password:***** Bad UserName or Bad Password,
  Login Failed. Please retry Login:
  ```

- Below is the echo information when the login succeeds.

  ```
  Login: GEPON Password: ***** Admin#
  ```

After logging into the system successfully, users can perform the command line operations in the allowed range of their authority. The users' operations will be recorded and accounted by the Tacacs+ server.

16 Configuring RADIUS

The following introduces how to configure the RADIUS function.

☑ Background Knowledge

☑ Example of Configuring RADIUS

16.1 Background Knowledge

The AN6001-G16 serves as the RADIUS client end to provide access service for remote access users and enables their interaction with the RADIUS server. The RADIUS server stores the identity and authorization information of the users and records their access operations to provide the user authentication, authorization and accounting (AAA) services.

Generally, when the RADIUS server authenticates a user, the equipment proxy authentication functions such as NAS will be used. The RADIUS client and server authenticate the interactive information between them by sharing the key. The user password is transmitted over the network in the form of cipher text which enhances the security. The RADIUS protocol combines the authentication and authorization processes. Namely, the response messages carry the authorization information as well.

The interaction procedures are as follows:

1. The user enters the user name and password.
2. The RADIUS client end, based on the user name and password obtained, sends the access-request packets to the RADIUS server.
3. The RADIUS server compares the user information received with the information stored in the user database. If the authentication succeeds, the RADIUS server will send the user's authority information to the RADIUS client end via the access-accept packets. If the authentication fails, the RADIUS server will return the access-reject response packets.
4. The RADIUS client end accepts or rejects the user based on the authentication result received. If the user is accepted, the RADIUS client end sends the accounting-request packets to the RADIUS server for starting accounting, and the "status-type" becomes "start".
5. The RADIUS server returns the accounting-response packets for starting accounting.
6. The RADIUS client end sends the accounting-request packets to the RADIUS server for stopping accounting, and the "status-type" becomes "stop".
7. The RADIUS server returns the accounting-response packets for stopping accounting.

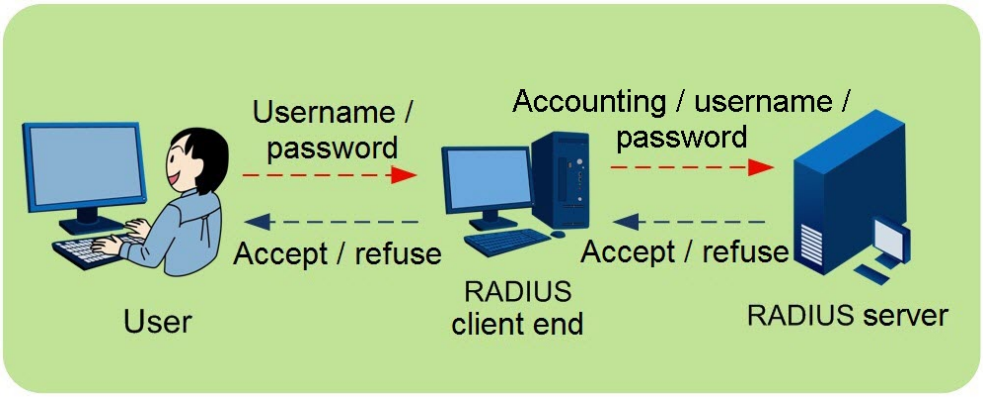


Figure 16-1 Principle of RADIUS Protocol Interaction

16.2 Example of Configuring RADIUS

The following gives an example to introduce how to configure the RADIUS function.

16.2.1 Configuration Flow

Figure 16-2 shows the flow of configuring RADIUS.

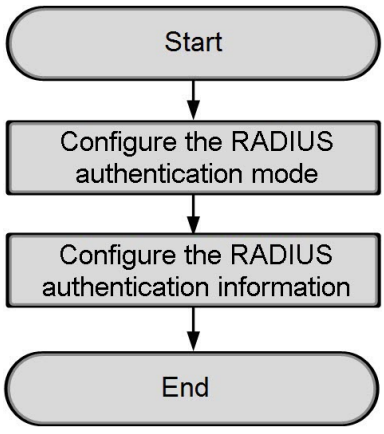


Figure 16-2 Flow of Configuring RADIUS

16.2.2 Configuring the RADIUS Authentication Mode

Planning Data

Item	Description	Example
Authentication Mode	Select RADIUS mode.	Radius Mode

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Common Config→Authentication** to bring up the **Authentication** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 16-3.

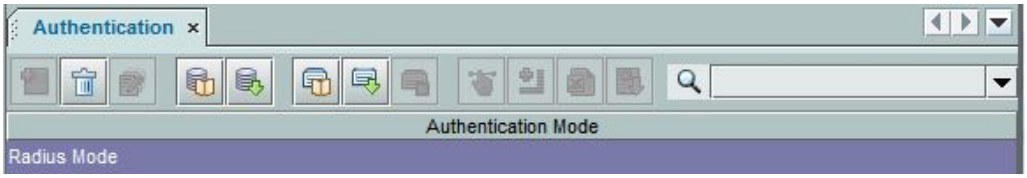


Figure 16-3 Authentication - RADIUS

16.2.3 Configuring the RADIUS Authentication Information

Planning Data

Item	Description	Example
IP Address	Configure the authentication server IP address and key of the equipment. The key should be consistent with that configured in the server.	IPv4:10.190.44.19
Authen Port	The port used for connecting to the authentication server.	1812
Server Port	The port used for connecting to the accounting server.	1813

Item	Description	Example
Key	Configure the authentication server IP address and key of the equipment. The key should be consistent with that configured in the server.	123
Timeout (s)	Configure the timeout duration for retransmission on the RADIUS client. The value ranges from 3 to 10, and the default value is 3.	3
retransmit	Set the retransmission times. The value ranges from 1 to 5, and the default value is 3.	3

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Common Config→RADIUS Server Information** to open the **RADIUS Server Information** tab.
4. Click **Add**, enter **1** in the displayed dialog box, and click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button on the toolbar to complete the configuration, as shown in Figure 16-4.

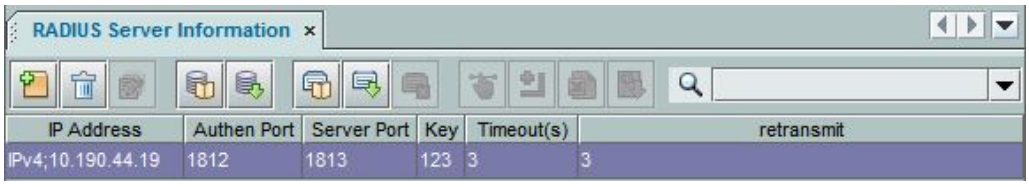


Figure 16-4 RADIUS Server Information

16.2.4 Configuration Result

After RADIUS is configured, enter the correct user name and password, and you will log in successfully.

17 Configuring Power Supply and Environment Monitoring

- ☑ Configuring Environment Monitoring
- ☑ Configuring the Discharge Test
- ☑ Configuring Environment Monitoring Parameters
- ☑ Configuring the Charging Mode
- ☑ Enabling the Rectifier Module
- ☑ Checking the Power Supply Status
- ☑ Viewing the Current Performance of the HCU Card
- ☑ Viewing the Current Alarms of the HCU Card
- ☑ Viewing the Alarm History of the HCU Card

17.1 Configuring Environment Monitoring

The AN6001-G16 can monitor environment variables such as temperature, humidity, power supply and security via the environment monitoring unit. The following introduces how to configure environment monitoring.

17.1.1 Alarm List

The following lists the alarms relevant with environment monitoring:

Alarm Code	Alarm Level	Alarm Type
AC_FAIL	Critical alarm	Communication quality
Battery Fail	Major alarm	Communication quality
ISSUE_ALM	Critical alarm	Environmental alarm
SYSMINALM	Critical alarm	Environmental alarm
HUM_DOWN	Critical alarm	Environmental alarm
ENV_TEMP_DOWN	Critical alarm	Environmental alarm
ACVOLOVER	Critical alarm	Environmental alarm
ACVOLDOWN	Critical alarm	Environmental alarm
DCVOLOVER	Critical alarm	Environmental alarm
DCVOLDOWN	Critical alarm	Environmental alarm
HUM_OVER	Critical alarm	Environmental alarm
ENV_TEMP_OVER	Critical alarm	Environmental alarm
ARRESTBRK	Critical alarm	Environmental alarm
FIRE_ALM	Critical alarm	Environmental alarm
DOOR_ALM	Critical alarm	Environmental alarm
BFUSEBRK	Critical alarm	Environmental alarm
LOADFUSE	Critical alarm	Environmental alarm
ACBRKOPEN	Critical alarm	Environmental alarm
LVDS_ALM	Critical alarm	Environmental alarm
FANFAIL	Critical alarm	Environmental alarm
HEATFAIL	Critical alarm	Environmental alarm
SHAKE	Critical alarm	Environmental alarm
INFRARED	Critical alarm	Environmental alarm
INUNDATION	Critical alarm	Environmental alarm
SMOKE	Critical alarm	Environmental alarm
AIRCONDITION	Critical alarm	Environmental alarm

Alarm Code	Alarm Level	Alarm Type
PALM	Critical alarm	Environmental alarm
BATTERY_TEMPERATURE_OVER_THRESHOLD_ALARM	Critical alarm	Environmental alarm
Battery_Charging	Warning alarm	Environmental alarm
Battery_Discharging	Critical alarm	Environmental alarm
BATTERY_TEMPERATURE_LOW_THRESHOLD_ALARM	Critical alarm	Environmental alarm
BATTERY_HUM_OVER	Critical alarm	Environmental alarm
BATTERY_HUM_DOWN	Critical alarm	Environmental alarm
Battery bunker door alarm	Critical alarm	Environmental alarm
HCU card is not on line alarm	Critical alarm	Environmental alarm
DCVOLDOWN	Major alarm	Equipment failure
DCVOLOVER_WARNING	Warning alarm	Environmental alarm
DCVOLDOWN_WARNING	Warning alarm	Environmental alarm
ENV_TEMP_OVER_WARNING	Warning alarm	Environmental alarm
ENV_TEMP_DOWN_WARNING	Warning alarm	Environmental alarm
BATTERY_TEMPRATURE_OVER_THRESHOLD_WARNING	Warning alarm	Environmental alarm
BATTERY_TEMPRATURE_LOW_THRESHOLD_WARNING	Warning alarm	Environmental alarm
Battery recharge Over Volt level	Critical alarm	Environmental alarm
Battery discharge Down Volt level	Critical alarm	Environmental alarm
Battery recharge Over current level	Critical alarm	Environmental alarm
Battery capacity too low	Critical alarm	Environmental alarm
Battery temperature sensor breakdown	Critical alarm	Environmental alarm
Battery volt sensor breakdown	Critical alarm	Environmental alarm
Battery current sensor breakdown	Critical alarm	Environmental alarm
Battery Cell temperature over	Critical alarm	Environmental alarm

Alarm Code	Alarm Level	Alarm Type
Battery Cell recharge volt over	Critical alarm	Environmental alarm
Battery Cell discharge volt down	Critical alarm	Environmental alarm
Battery Cell recharge current over	Critical alarm	Environmental alarm
Battery Cell discharge current over	Critical alarm	Environmental alarm

17.1.2 Configuration Flow

Figure 17-1 shows the flow of configuring environment monitoring.

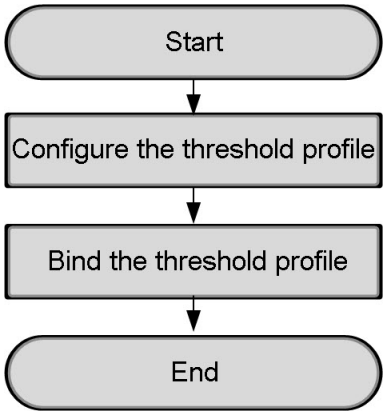


Figure 17-1 Flow of Configuring Environment Monitoring

17.1.3 Configuring the Threshold Profile

This command is used to configure the alarm codes and the threshold values for clearing and reporting the alarms of the threshold profile. When the profile is bound to a card or a port, the threshold alarming function will be enabled.

Note:

A bound threshold profile cannot be deleted unless being unbound first.

Planning Data

Item	Description	Example
Profile ID	Read only.	-
Profile Name	Configure this item according to the network planning of the operator. It contains no more than 20 characters. The acceptable character collection is 0 to 9, a to z, A to Z and the underline.	test1
Object Class	Configure this item according to the network planning of the operator. The options available are "Board", "Port", "ONU", "ONU Port" and "None". For the configuration of the equipment power supply and environment monitoring, only two options are valid: "Board" and "Port".	Board
Object Type	Configure this item according to the network planning of the operator. Select "HCU-OLT" when the "Object Class" is set to "Board".	HCU-OLT
Alarm Code	Configure this item according to the planning of the operator.	ACVOLOVER
Alarm Threshold Switch	Configure this item according to the network planning of the operator. Select **Enable** or **Disable**. ◆ When it is set to "Enable", the UNM2000 will deliver the threshold profile parameters configured by the users to the equipment. ◆ When it is set to "Disable", the UNM2000 will deliver the default settings of the threshold profile to the equipment.	Enable
Alarm Report Threshold	◆ For an alarm code indicating an overhigh performance value, the UNM2000 reports the alarm when the performance value of the card or port is higher than the set value. ◆ For an alarm code indicating an overlow performance value, the UNM2000 reports the alarm when the performance value of the card or port is lower than the set value.	250.00
Alarm Report Threshold Range	Read-only. The set alarm report threshold should be within this range.	[250.00,289.90]

Item	Description	Example
Clearing Alarm Threshold	◆ For an alarm code indicating an overhigh performance value, the UNM2000 clears the alarm when the performance value of the card or port is lower than the set value. The value of the "Clearing Alarm Threshold" should be smaller than or equal to the value of "Alarm Report Threshold" in this case. ◆ For an alarm code indicating an overlow performance value, the UNM2000 clears the alarm when the performance value of the card or port is higher than the set value. The value of the "Clearing Alarm Threshold" should be higher than or equal to the value of "Alarm Report Threshold" in this case.	250.00
Clearing Alarm Threshold Range	Read-only. The set clearing alarm threshold should be within this range.	[250.00,289.90]

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the NE to be configured and select **Performance Management→Threshold Profile and Bind→PM Threshold Profile** from the shortcut menu that appears to bring up the **PM Threshold Profile** tab.
3. Configure the parameters according to the planning data.
4. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-2.

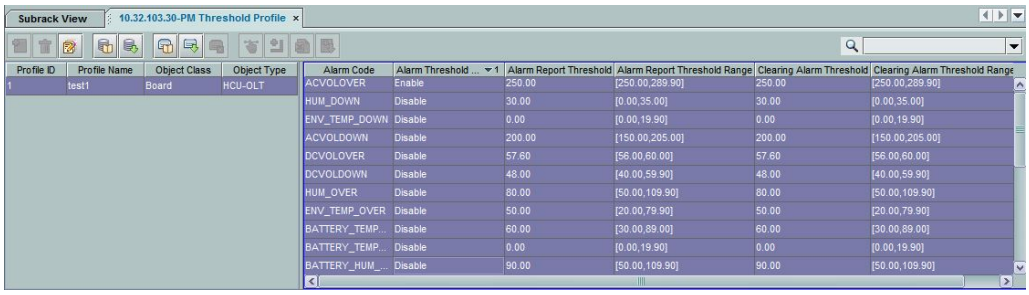


Figure 17-2 The Performance Threshold Configuration Profile

17.1.4 Binding the Threshold Profile

This command is used to bind a threshold profile to a card or a port on the card to be monitored to enable the threshold-crossing alarm reporting function. The following uses the HCU-OLT card as an example.

Precautions

A card or a port on the card can be bound to only one threshold profile, while a threshold profile can be bound to multiple ports.

Planning Data

Item	Description	Example
Object Name	Select the object card.	HCU-OLT[801]
Object Type	Set this object to a card or a port.	HCU-OLT
Profile Name	Select an exiting threshold profile. For a bound threshold profile, you can select **Unbind** from the drop-down list to unbind it from a card or port.	test1

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the NE to be configured and select **Performance Management→ Threshold Profile and Bind→PM Threshold Profile Bind** from the shortcut menu that appears to bring up the **PM Threshold Profile Bind** tab.
3. Configure the parameters according to the planning data.
4. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-3.

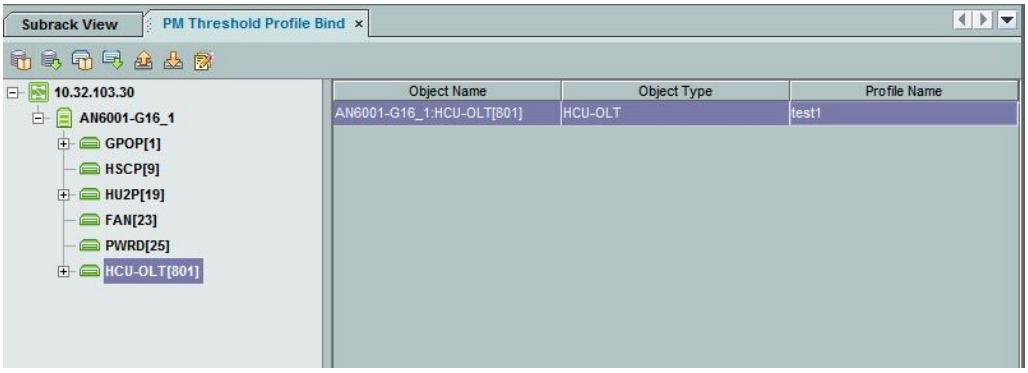


Figure 17-3 Binding the Performance Threshold Profile

17.1.5 Configuration Result

A threshold profile with the alarm code set to ACVOLOVER (AC voltage overhigh) is configured and bound to the HCU-OLT card. When the AC voltage of the card is higher than the set alarm report threshold, the AN6001-G16 will report the alarm. When the AC voltage of the card is lower than the set clearing alarm threshold, the alarm will be cleared.

17.2 Configuring the Discharge Test

The discharge test is used to measure the power supply capability of storage batteries. The following introduces how to configure the storage battery discharge test .

17.2.1 Configuration Flow

The flow of configuring the discharge test is shown in Figure 17-4.

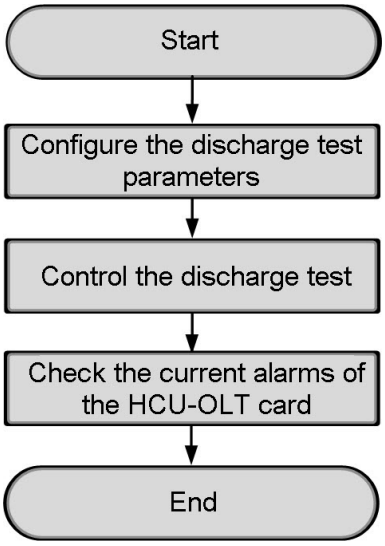


Figure 17-4 Flow of the Discharge Test

17.2.2 Configuring the Discharge Test Parameters

Configure the parameters for the storage battery discharge test.

Planning Data

Item	Description	Example
Discharge End Voltage (V)	The battery will stop discharging when its voltage is reduced to the "Discharge End Voltage". Configure this item according to the network planning. The value ranges from 45.1 to 52.0. The default value is 48.0, and the unit is V.	48
Discharge Time (minute)	The discharge duration time. When the discharge time expires, the battery stops discharging. Configure this item according to the network planning. The value ranges from 1 to 300. The default value is 60, and the unit is minute.	60

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select**Common Config→Discharge Test Para Config** to bring up the **Discharge Test Para Config** tab.
4. Click **Add**, enter **1** in the dialog box that appears and then click **OK** to add a configuration entry.
5. Configure the parameters according to the planning data.
6. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-5.

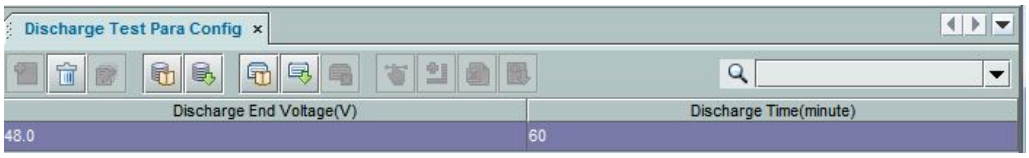


Figure 17-5 Configuring the Discharge Test Parameters

17.2.3 Controlling the Discharge Test

Configure starting / stopping a discharge test for storage batteries.

Planning Data

Item	Description	Example
Enable/Disable	Configure this item according to the network planning of the operator. Two options are available: "Start" and "End". ◆ When "Start" is selected, the discharge test is conducted immediately. The batteries ascertain the conditions for terminate the test according to the set test parameters. When any of the conditions is met, the discharge test is terminated. ◆ When "End" is selected, the discharge test is terminated immediately.	Start

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.

2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select**Common Config→Discharge Control** to bring up the **Discharge Control** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-6.

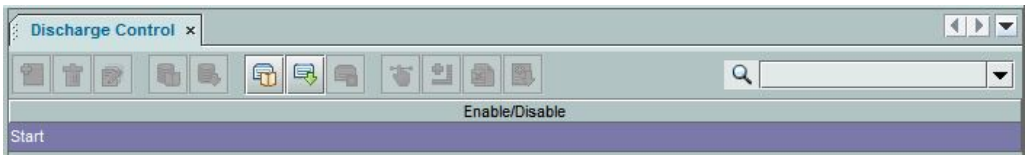


Figure 17-6 Controlling the Discharge Test

17.2.4 Viewing the Current Alarms of the HCU Card

This command is used to check whether the storage battery can discharge normally in the discharge test.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the HCU-OLT card in the **Device Tree**, and select **Current Alarm** from the shortcut menu that appears to bring up the **Current Alarm** tab and check the alarms currently existing on the HCU card.
3. Check whether the alarm list includes the **BATTERY_DISCHARGE** alarm.
   - If yes, the storage battery is discharging normally.
   - If no, the storage battery cannot provide power supply.

17.2.5 Configuration Result

After the configuration for the discharge test is completed, the equipment starts to test the power supply capability of the storage battery in the HCU-OLT card immediately according to the set discharge test parameters. When the test is completed, users can terminate the test in the **Discharge control** tab.

17.3 Configuring Environment Monitoring Parameters

Configure the parameters for the power system of the HCU-OLT card to ensure normal operation of the power system.

Planning Data

Item	Description	Example
Slot No.	Read-only. The HCU-OLT card is managed as a special card with a dedicated slot number 801 in the network management system.	801
Battery Fill Back Coefficient Value	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.9, and the default value is 0.0.	0.0
Battery Fill Value	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.9, and the default value is 0.0.	0.0
Battery Fill Limit Current Value (A)	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0. The default value is 19.0, and the unit is A.	19.0
Battery Fill Circle Value (H)	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0. The default value is 0.0, and the unit is H.	0.0
Battery Fill Time Value (H)	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0. The default value is 0.0, and the unit is H.	0.0
Battery Fill Time Stoptime (H)	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0. The default value is 0.0, and the unit is H.	0.0
Temperature_Compensate_ Coefficient	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0, and the default value is 0.0.	0.0

Item	Description	Example
Temperature Battery Fill Basic (℃)	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 39.0. The default value is 20.0, and the unit is ℃.	20.0
Volt Fill Adjust Value	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0, and the default value is 0.0.	0.0
Temperature Fill Adjust Value	Configure this item according to the network planning of the operator. The value ranges from 0.0 to 999.0, and the default value is 0.0.	0.0
Communte Float Charge Volt (V)	Configure this item according to the network planning of the operator. The value ranges from 43.0 to 56.0. The default value is 54.0, and the unit is V.	54.0
Communte Squal Charge Volt (V)	Configure this item according to the network planning of the operator. The value ranges from 43.0 to 57.0. The default value is 55.0, and the unit is V.	55.0
Communte Num	Configure this item according to the network planning of the operator. The value ranges from 0 to 60, and the default value is 2.	2
Battery Capacity (AH)	Configure this item according to the network planning of the operator. The value ranges from 0 to 999. The default value is 100. 0, and the unit is AH.	100.0
Sound Alarm Switch	Configure this item according to the planning of the operator. The options include "ON" and "OFF".	ON
Battery Switch Volt (V)	Configure this item according to the network planning of the operator. The value ranges from 40 to 52. The default value is 43, and the unit is V.	43.0
Load Switch Volt (V)	Configure this item according to the network planning of the operator. The value ranges from 40 to 52. The default value is 45, and the unit is V.	45.0
Communte Limit_Current Value (A)	Configure this item according to the network planning of the operator. The value ranges from 2.0 to 55.0. The default value is 0. 0, and the unit is A.	0.0
Battery Discharge Turn to Equal Charge Volt (V)	Configure this item according to the network planning of the operator. The value ranges from 43.0 to 51.0. The default value is 48.0, and the unit is V.	48.0
Battery Discharge Turn to Equal Charge Time (min)	Configure this item according to the network planning of the operator. The value ranges from 30.0 to 600.0. The default value is 30.0, and the unit is min.	30.0

Item	Description	Example
Battery Discharge Turn to Equal Charge Capacity (%)	Configure this item according to the network planning of the operator. The value ranges from 10.0 to 90.0. The default value is 60.0, and the unit is %.	60.0
Battery Type	Configure this item according to the network planning of the operator. The options available include "phosphoric acid battery" and "lead switch battery".	phosphoric acid battery

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select**Common Config→HCU Para Config** to open the **HCU Para Config** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-7.

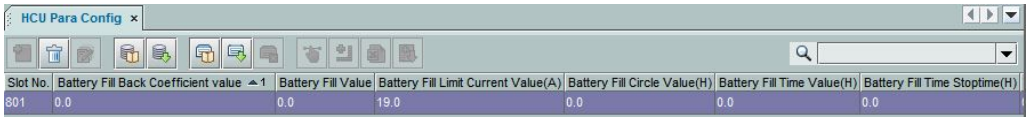


Figure 17-7 Configuring Environment Monitoring Parameters

17.4 Configuring the Charging Mode

Planning Data

Item	Description	Example
Charging Mode	Configure the charge mode for the AC power supply to charge the storage battery via the rectifying module. The options include "equal charge" and "float charge".	float charge

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select**Common Config→Charging Mode** to bring up the **Charging Mode** tab.
4. Select the desired charging mode.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-8.

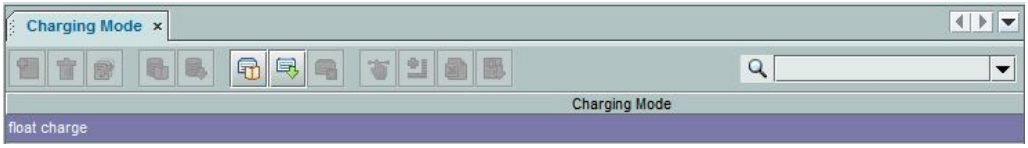


Figure 17-8 The Charging Mode

17.5 Enabling the Rectifier Module

Enable the rectifier module. When the rectifier module is enabled, the rectification function will be enabled for the rectifier module as well.

Planning Data

Item	Description	Example
Module No.	Configure this item according to the network planning of the operator. The value range is 1 to 60.	1
Enable	Select "Enable" or "Disable".	Enable

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.

3. In the **Operational Tree** pane, select **Common Config→Rectifier Module Enable** to bring up the **Rectifier Module Enable** tab.
4. Configure the parameters according to the planning data.
5. Click the **Create on Device** button to complete the configuration, as shown in Figure 17-9.

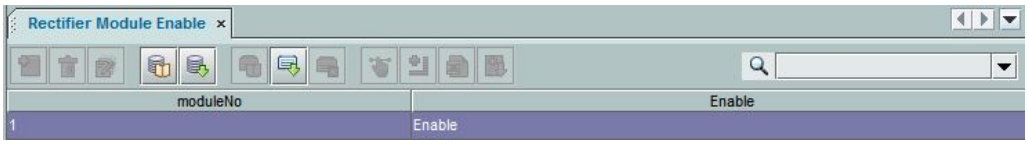


Figure 17-9 Enabling the Rectifier Module

17.6 Checking the Power Supply Status

This command is used to query the power supply status of the current storage battery.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the HCU-OLT card in the **Device Tree**, and select **Card Service Config** from the shortcut menu that appears to bring up the **Card Service Config** tab.
3. In the **Operational Tree** pane, select **Get Information→Power Supply Status** to bring up the **Power Supply Status** tab and check the power supply status of the current storage battery, as shown in Figure 17-10.

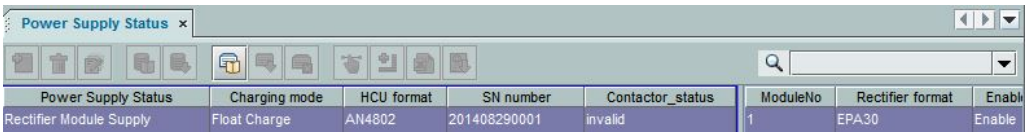


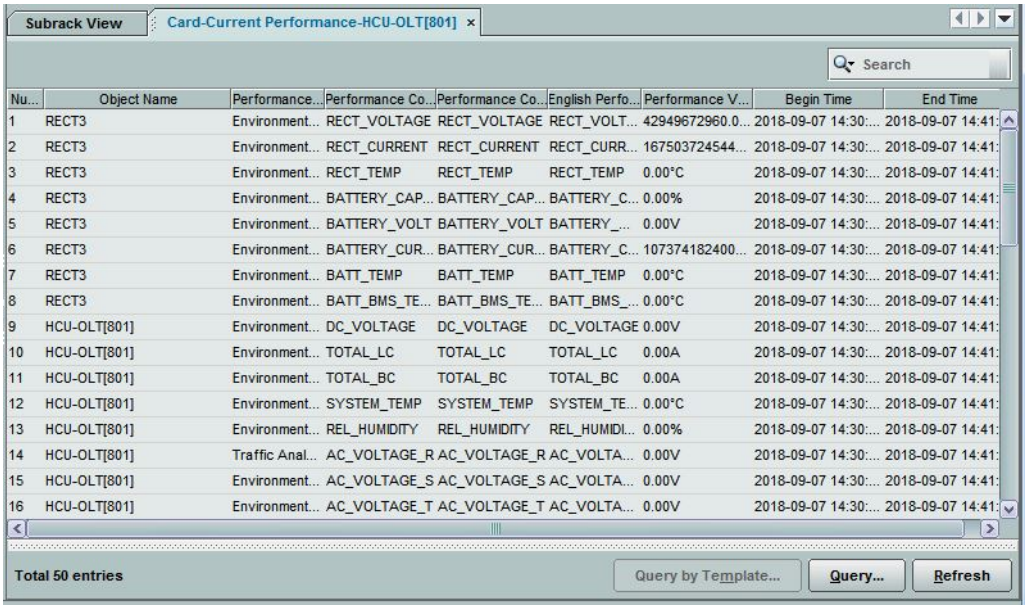
Figure 17-10 The HCU Device Status

17.7 Viewing the Current Performance of the HCU Card

This command is used to query the current performance of the HCU-OLT card.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the HCU-OLT card in the **Device Tree**, and select **Current Performance** from the shortcut menu that appears to bring up the **Card-Current Performance-HCU-OLT[801]** tab. Then you can check the instant performance of the current HCU card, as shown in Figure 17-11.



Nu...	Object Name	Performance...	Performance Co...	Performance Co...	English Perfo...	Performance V...	Begin Time	End Time
1	RECT3	Environment...	RECT_VOLTAGE	RECT_VOLTAGE	RECT_VOLT...	42949672960.0...	2018-09-07 14:30:...	2018-09-07 14:41:
2	RECT3	Environment...	RECT_CURRENT	RECT_CURRENT	RECT_CURR...	167503724544...	2018-09-07 14:30:...	2018-09-07 14:41:
3	RECT3	Environment...	RECT_TEMP	RECT_TEMP	RECT_TEMP	0.00°C	2018-09-07 14:30:...	2018-09-07 14:41:
4	RECT3	Environment...	BATTERY_CAP...	BATTERY_CAP...	BATTERY_C...	0.00%	2018-09-07 14:30:...	2018-09-07 14:41:
5	RECT3	Environment...	BATTERY_VOLT	BATTERY_VOLT	BATTERY_...	0.00V	2018-09-07 14:30:...	2018-09-07 14:41:
6	RECT3	Environment...	BATTERY_CUR...	BATTERY_CUR...	BATTERY_C...	107374182400...	2018-09-07 14:30:...	2018-09-07 14:41:
7	RECT3	Environment...	BATT_TEMP	BATT_TEMP	BATT_TEMP	0.00°C	2018-09-07 14:30:...	2018-09-07 14:41:
8	RECT3	Environment...	BATT_BMS_TE...	BATT_BMS_TE...	BATT_BMS_...	0.00°C	2018-09-07 14:30:...	2018-09-07 14:41:
9	HCU-OLT[801]	Environment...	DC_VOLTAGE	DC_VOLTAGE	DC_VOLTAGE	0.00V	2018-09-07 14:30:...	2018-09-07 14:41:
10	HCU-OLT[801]	Environment...	TOTAL_LC	TOTAL_LC	TOTAL_LC	0.00A	2018-09-07 14:30:...	2018-09-07 14:41:
11	HCU-OLT[801]	Environment...	TOTAL_BC	TOTAL_BC	TOTAL_BC	0.00A	2018-09-07 14:30:...	2018-09-07 14:41:
12	HCU-OLT[801]	Environment...	SYSTEM_TEMP	SYSTEM_TEMP	SYSTEM_TE...	0.00°C	2018-09-07 14:30:...	2018-09-07 14:41:
13	HCU-OLT[801]	Environment...	REL_HUMIDITY	REL_HUMIDITY	REL_HUMIDI...	0.00%	2018-09-07 14:30:...	2018-09-07 14:41:
14	HCU-OLT[801]	Traffic Anal...	AC_VOLTAGE_R	AC_VOLTAGE_R	AC_VOLTA...	0.00V	2018-09-07 14:30:...	2018-09-07 14:41:
15	HCU-OLT[801]	Environment...	AC_VOLTAGE_S	AC_VOLTAGE_S	AC_VOLTA...	0.00V	2018-09-07 14:30:...	2018-09-07 14:41:
16	HCU-OLT[801]	Environment...	AC_VOLTAGE_T	AC_VOLTAGE_T	AC_VOLTA...	0.00V	2018-09-07 14:30:...	2018-09-07 14:41:

Figure 17-11 Card-Current Performance-HCU-OLT[801]

17.8 Viewing the Current Alarms of the HCU Card

This command is used to query the current alarms of the HCU-OLT card.

Current Alarm: The alarms that currently exist in the equipment and are not ended yet.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the HCU-OLT card in the **Device Tree**, and select **Current Alarm** from the shortcut menu that appears to bring up the **Card-Current Alarm-HCU-OLT[801]** tab. Then you can check the alarms currently existing on the HCU card, as shown in Figure 17-12.

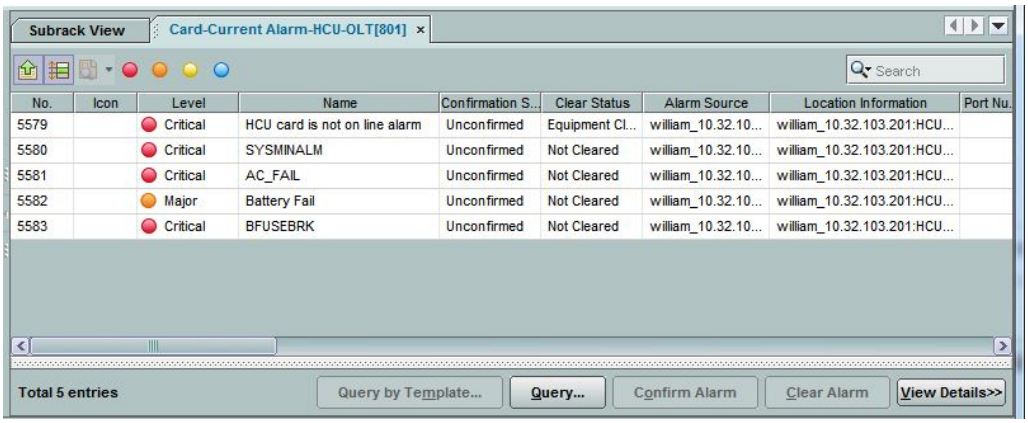


Figure 17-12 Card-Current Alarm-HCU-OLT[801]

17.9 Viewing the Alarm History of the HCU Card

This command is used to query the alarm history of the HCU-OLT card.

History alarms: The alarms that have ever appeared but now ended.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Right-click the HCU-OLT card in the **Device Tree**, and select **History Alarm** from the shortcut menu that appears to bring up the **Card-History Alarm-HCU-OLT[801]** tab. Then you can check the alarm history of the HCU card, as shown in Figure 17-13.

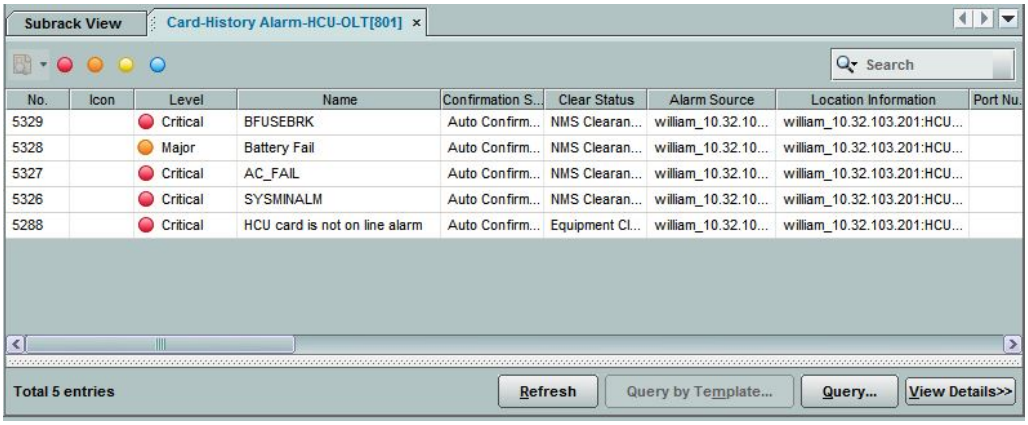


Figure 17-13 Card-History Alarm-HCU-OLT[801]

18 Detecting the Optical Power

The following introduces how to detect the optical power.

☑ Viewing Optical Module Parameter Information of a GPON Interface Card

☑ Viewing Optical Module Parameter Information of a PON ONU

18.1 Viewing Optical Module Parameter Information of a GPON Interface Card

The following introduces how to view optical module parameter information of a PON interface card.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Select **Configuration→Local Service Configuration** from the menu bar to open the **Local Service Configuration** tab.
3. In the **Operational Tree** pane, select **Get Information→Opt Module Para Information**, and choose the PON interface card on the **Select Object (Opt Module Para Information)** tab that appears. Click **OK** to access the **Opt Module Para Information** tab.
4. Enter the number of the PON port to be viewed in the **PON No.** field. In this example, enter **1**.
5. Click the **Read from Device** button in the toolbar to read the parameters of the optical module at this PON port, as shown in Figure 18-1.

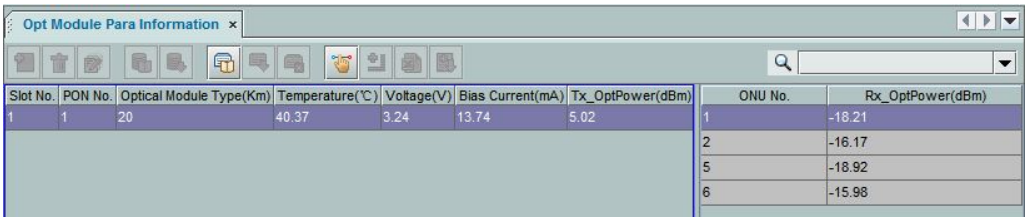


Figure 18-1 Optical Module Parameters of the PON Interface Card

18.2 Viewing Optical Module Parameter Information of a PON ONU

The following introduces how to view the optical module parameters of a PON ONU.

Procedure

1. Double-click the NE to be configured in **Main Topology** to open the **NE Manager**.
2. Click the **ONU List** button to open the **ONU List** tab.
3. Right-click an ONU and select **Service Configuration** from the menu.
4. In the **Operational Tree** pane, select **Get Information→Opt Module Para Information** to open the **Opt Module Para Information** tab.
5. View the parameter information of the optical module at the PON port. See Figure 18-2.

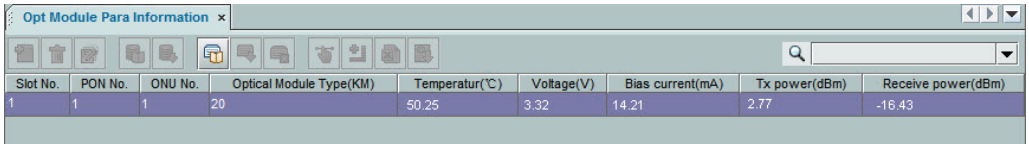


Figure 18-2 Optical Module Parameters of the PON ONU

19 FTP Operation Guide

The following introduces the FTP function and how to configure it.

☑ Function Overview

☑ Procedure

19.1 Function Overview

Connect the computer with the equipment using the network cable, and set up the FTP server end on the computer; that is, install the WFTP software.

- During equipment upgrade, the equipment obtains the upgrade package from the FTP server in the FTP mode.
- During equipment backup, the equipment exports the backup files to the FTP server end in the FTP mode.

19.2 Procedure

Note:

Here we use WFTP as an example of FTP software.

1. Create the directory d:\ftp for saving the upgrade / backup packet on the FTP server end.
2. Open the WFTP window, as shown in Figure 19-1.

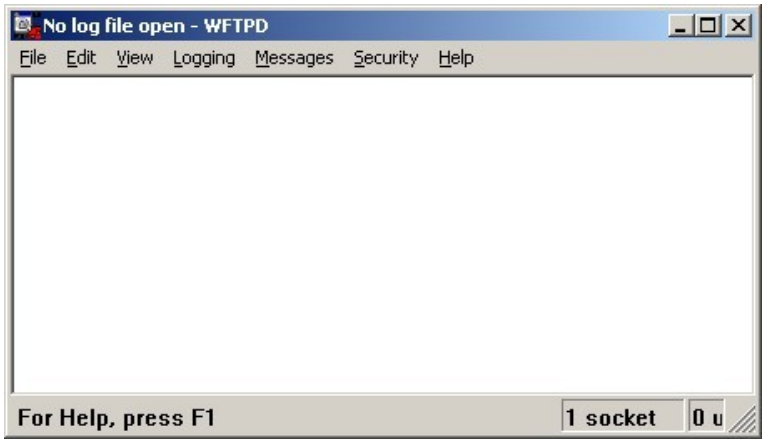


Figure 19-1 Opening the WFTP

3. Click **Security→Users/Rights** in the menu bar to open the **User/Rights Security Dialog** dialog box, as shown in Figure 19-2.

Figure 19-2 User Settings

4. Click the **New User** button to add a new FTP user. This user will be used in upgrade and backup. Enter the user name **1**, as shown in Figure 19-3.

Note:

Click the **Delete** button to delete an existing user, or select an existing user and click the **Change Password** button to modify the user's password.

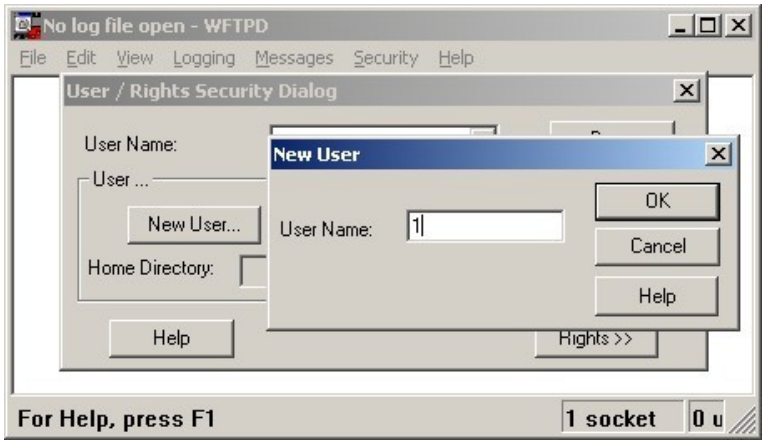


Figure 19-3 Creating a New User

5. Click the **OK** button, enter the password **1**, and click **OK** to create a user, as shown in Figure 19-4.

Figure 19-4 Creation of the New User Account Completed

6. In the **User/Rights Security Dialog** dialog box, enter the directory where the upgrade or backup package is saved, i.e. **d:\ftp**, as shown in Figure 19-5.

Figure 19-5 Setting the Path

7. Click **Done** to complete the settings.
8. Click **Logging→Log Options** in the **No log file open** window to set the log function of the WFTP tool, as shown in Figure 19-6.

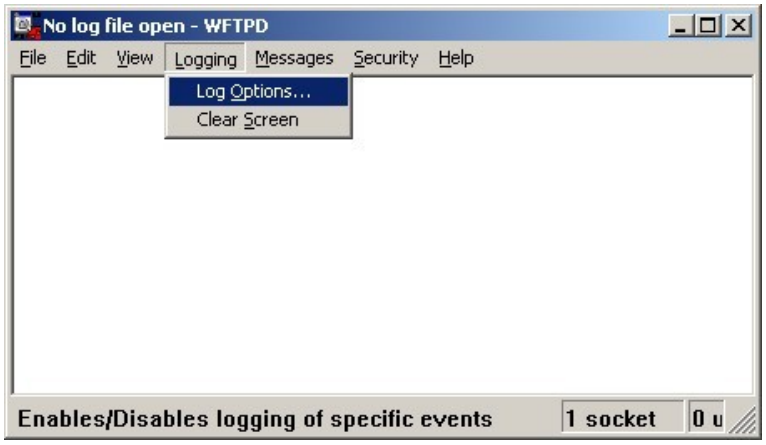


Figure 19-6 Setting the Log Function of the WFTP Tool

9. Select the check boxes **Enable Logging**, **Gets**, **Logins**, **Commands**, **Warnings**, **Puts** and **Anon.Logins** in the **Logging Options** dialog box, as shown in Figure 19-7.

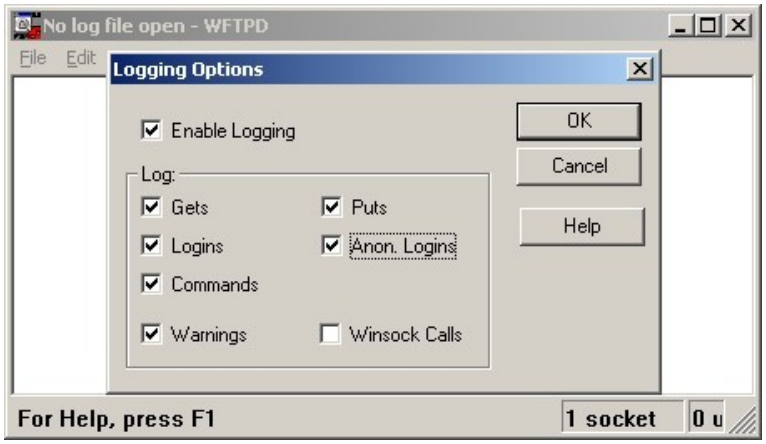


Figure 19-7 Selecting the Log Information

10. Click **OK**, the system then displays the logs. Users can isolate the faults by viewing the log information and determine whether the "Gets" or "Puts" operation is successful according to the log in the WFTP window.

Now the WFTP configuration is completed.

Product Documentation Customer Satisfaction Survey

Thank you for reading and using the product documentation provided by FiberHome. Please take a moment to complete this survey. Your answers will help us to improve the documentation and better suit your needs. Your responses will be confidential and given serious consideration. The personal information requested is used for no other purposes than to respond to your feedback.

Name	
Phone Number	
Email Address	
Company	

To help us better understand your needs, please focus your answers on a single documentation or a complete documentation set.

Documentation Name	
Code and Version	

Usage of the product documentation:

1. How often do you use the documentation?

☐ Frequently ☐ Rarely ☐ Never ☐ Other (please specify) _____

2. When do you use the documentation?

☐ in starting up a project ☐ in installing the product ☐ in daily maintenance ☐ in trouble shooting ☐ Other (please specify) _____

3. What is the percentage of the operations on the product for which you can get instruction from the documentation?

☐ 100% ☐ 80% ☐ 50% ☐ 0% ☐ Other (please specify) _____

4. Are you satisfied with the promptness with which we update the documentation?

☐ Satisfied ☐ Unsatisfied (your advice) _____

5. Which documentation form do you prefer?

☐ Print edition ☐ Electronic edition ☐ Other (please specify) _____

Quality of the product documentation:

1. Is the information organized and presented clearly?

☐ Very ☐ Somewhat ☐ Not at all (your advice) _____

2. How do you like the language style of the documentation?

☐ Good ☐ Normal ☐ Poor (please specify) _____

3. Are any contents in the documentation inconsistent with the product?

_____

4. Is the information complete in the documentation?

☐ Yes

☐ No (Please specify) _____

5. Are the product working principles and the relevant technologies covered in the documentation sufficient for you to get known and use the product?

☐ Yes

☐ No (Please specify) _____

6. Can you successfully implement a task following the operation steps given in the documentation?

☐ Yes (Please give an example) _____

☐ No (Please specify the reason) _____

7. Which parts of the documentation are you satisfied with?

_____

8. Which parts of the documentation are you unsatisfied with?Why?

_____

9. What is your opinion on the Figures in the documentation?

☐ Beautiful ☐ Unbeautiful (your advice) _____

☐ Practical ☐ Unpractical (your advice) _____

10. What is your opinion on the layout of the documentation?

☐ Beautiful ☐ Unbeautiful (your advice) _____

11. Thinking of the documentations you have ever read offered by other companies, how would you compare our documentation to them?

Product documentations from other companies:_____

Satisfied (please specify) _____

Unsatisfied (please specify) _____

12. Additional comments about our documentation or suggestions on how we can improve:

_____

_____

Thank you for your assistance. Please fax or send the completed survey to us at the contact information included in the documentation. If you have any questions or concerns about this survey please email at edit@fiberhome.com