AN6001-G16

Optical Line Terminal Equipment

CLI Configuration Guide

Version: B

Code: MN000003551

FiberHome Telecommunication Technologies Co., Ltd.

March 2021

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.fiberhome.com

Legal Notice

烽火通信® 烽火® FiberHome®

GONST® FONST® e-Fim®

CiTRANS® E-jet® IBAS®

Freelink® FonsWeaver®

OTNPlanner® SmartWeaver®

FitServer®

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.

Contents

1 Documentation Guide

Document Orientation

CLI Configuration Guide introduces how to start and configure services for the AN6001-G16 in the CLI mode.

Intended Readers

- Commissioning engineers
- Operation and maintenance engineers

Version Information

Version	Description
A	Initial version, applicable to the V1R1 version of the AN6001-G16.
B	Adds contents about configurations of Layer 3 functions and time & clock functions.

2 Logging into the Device

- Login Through Hyper Terminal
- Login Through Telnet

2.1 Login Through Hyper Terminal

Properly connect the PC to the CONSOLE port of the main control service card with the serial port line. Log into the AN6001-G16 through the hyper terminal. Follow the steps below:

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

Note:

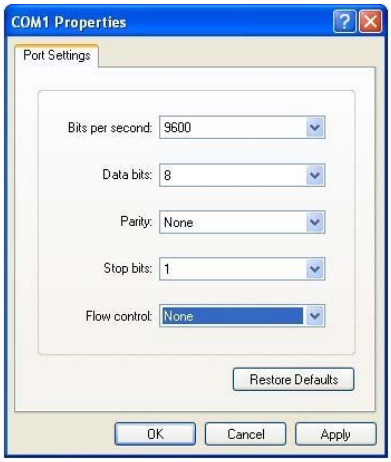
The Windows XP operating system is used as an example here.

2. In the **Connection Description** dialog box, enter the name of the object to be connected and select an icon for it.

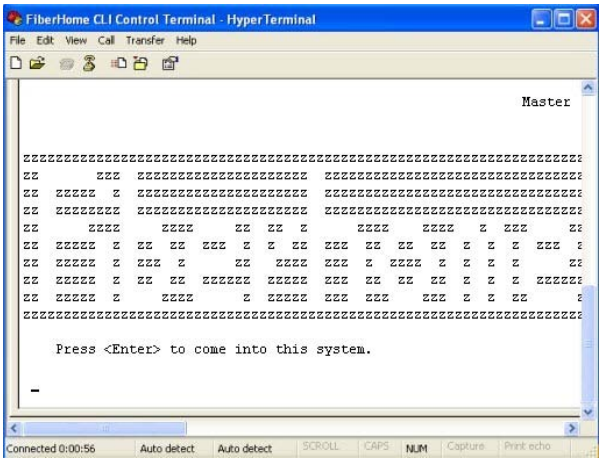
3. Click **OK**, and the **Connect To** dialog box appears.
4. In the **Connect To** dialog box, select the computer's **COM1** port to be connected to the **CONSOLE** port of the main control service card through the serial port line.

5. Click **OK**, and the **COM1 Properties** dialog box appears.

6. In the **COM1 Properties** dialog box, click the **Restore Defaults** button.



7. Click **OK** to start up the CONSOLE.



8. Press the <Enter> key, and enter the user name and password to log into the CLI network management system.

```
Login:GEPON
// The default user is the administrator user, and the user name is "GEPON".

Password:*****
// The initial password is "GEPON".

User>enable
// In the read-only mode, use the "enable" command to enter the management mode.

Password:*****
// The initial password of the administrator user is "GEPON".

Admin#
// After the prompt "Admin#" appears, you can enter command lines to perform network management operations 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 is case sensitive.

Caution:

Users should memorize their passwords and keep them secret. Regularly changing passwords is recommended.

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

2.2 Login Through Telnet

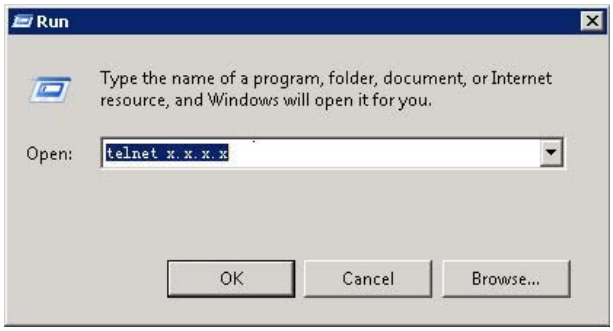
When logging into the equipment through a hyper terminal, you can configure the out-of-band management IP address and in-band management IP address for the equipment. After the aforesaid configuration, you can log into the equipment though Telnet. Follow the steps below:

1. Click the **Start** menu on the desktop, and select **Run** to bring up the **Run** dialog box.

Note:

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

2. Enter telnet x.x.x.x in the **Run** dialog box.



Note:

x.x.x.x is the out-of-band management IP address for the equipment (configured under the directory of Admin (config-if-meth-1)) or the in-band management IP address (the IP address of the management VLAN configured under the directory of Admin(config)).

3. Click **OK** to bring up the **Telnet x.x.x.x** window.

4. Enter the user name and the password to log into the CLI network management system.

```
Login:GEPON
// The default user is administrator, 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 is case sensitive.

Caution:

Users should memorize their passwords and keep them secret. Regularly changing passwords is recommended.

3 Overview of Command Lines

- Command Mode
- Syntax
- Interaction Feature

3.1 Command Mode

Command Mode (Directory)	Directory Name	Prompt Example	Access Command Example
Common user mode	user	`user>`	Common user login
Privileged user mode	admin	`Admin#`	`user>enable`
Global configuration mode	config	`Admin(config)#`	`Admin#config`
Protocol	config-dhcp	`Admin(config-dhcp)#`	`Admin(config)#dhcp`
	config-ospf	`Admin(config-ospf)#`	`Admin(config)#ospf`
	config-aaa	`Admin(config-aaa)#`	`Admin(config)#aaa`
	config-igmp	`Admin(config-igmp)#`	`Admin(config)#igmp`
Multicast VLAN and multicast configuration	config-mvlan**vlan_id**	`Admin(config-mvlan100)#`	`Admin(config)#multicast-vlan 100`
VLAN IF	config-vlanif-**vlanid**	`Admin(config-vlanif-200)#`	`Admin(config)#interface vlanif 200`
PON mode (slot / port)	config-if-pon-**frame/slot/pon**	`Admin(config-if-pon-1/1/2)#`	`Admin(config)#interface pon 1/1/2`
Ethernet mode (slot / port)	config-if-eth-**frame/slot/eth**	`Admin(config-if-eth-1/19/1)#`	`Admin(config)# interface eth 1/19/1`
Fan	config-if-fan-**frame/slot**	`Admin(config-if-fan-1/23)#`	`Admin(config)#interface fan 1/23` (Slot 23 is dedicated for the fan unit)
Maintenance network port	config-if-meth-**port**	`Admin(config-if-meth-1)#`	`Admin(config)#interface meth 1` (Port 1 is dedicated for the out-of-band management network port)
Debugging and diagnosis	diagnose	`Admin(diagnose)#`	`Admin#diagnose`

3.2 Syntax

Command Format

A command consist of a command name followed by an argument field.

A complete command comprises command name(s) and argument(s). A valid command may contain one or more command names and argument fields. An argument field consists of two parts: the flag and the argument. For an argument with a flag, enter the flag first, and then the argument; for an argument without flag, enter the argument only.

Format	Meaning
< >	Indicates that the content in **< >** is the argument (parameter) value.
<a/b/...>	Indicates that all the parameter values in **< >** should be configured.
[ ]	Indicates that the parameter in **[ ]** is mandatory.
[a|b|...]	Indicates that one of the mandatory parameters in **[ ]** should be selected.
{ }	Indicates that the parameter in **{ }** is optional.
{ }* (1 ~ n)	Indicates that the optional parameter in **{ }** can be configured for one to n times.

3.3 Interaction Feature

Intelligent Match

Intelligent match allows you to type only the first one or several letters of a command keyword plus the Tab key. If a unique keyword starting with the letters entered is found, the CLI network management system will replace the letters you have entered with the complete keyword and display it in the next line, with a space between the cursor and the keyword. This helps simplify the work for typing long keywords. For example, to use the **enable** command, you only need to type **en** or **ena**.

Edition Function

Key	Function
Common key	If the edition buffer area is not filled, pressing the key will insert the key content to the current cursor position, and the cursor will moves rightward accordingly.
Backspace	Presses this key to delete the character before the cursor and move the cursor backwards. When reaching the beginning of the command, the cursor stops.
Tab	Typeaheads the keyword of the command.
Left arrow key ← or Ctrl + B	Moves the cursor to the left of one character.

Key	Function
Right arrow key → or Ctrl + F	Moves the cursor to the right of one character.
Up/Down arrow key ↑ / ↓	Displays historical commands. For some display terminals that do not support the upward / downward arrow key, you can press Ctrl + P to select the previous historical command or press Ctrl + O to select the next historical command.
Ctrl + U	Deletes the characters before the current cursor and moves the cursor to the beginning of the line.
Ctrl + K	Deletes the characters that follow the current cursor and moves the cursor to the end of the line.
Ctrl + D	Deletes a character after the cursor.
Ctrl + A	Moves the cursor to the beginning of the line.
Ctrl + W	Deletes a word before the cursor.
Ctrl + C	Stops executing the current command.
Q	Goes back to the upper layer directory.
Any keys except Q	Displays the command output.
?	Displays the help information.

4 Configuring Management Information

- Configuring the IP Address for In-Band Management
- Configuring the IP Address for Out-of-Band Management
- Configuring Static Routing
- Configuring the SNMP Trap Receiver Address
- Configuring the SNMP Time System
- Synchronizing Time
- Saving Current Configuration to the Flash

4.1 Configuring the IP Address for In-Band Management

Command Format

Configure the management VLAN.

```
manage-vlan <name> svlan <svlan> {cvlan <cvlan>}*1
```

Configure the management IP address.

```
manage-vlan ipv4 <name> <A.B.C.D/M>
```

Add the management VLAN to the uplink port.

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

View the management VLAN.

```
show manage-vlan [<1-4085>|all]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the management VLAN	manage-vlan <name>	The name of the management VLAN	Mandatory	test
	svlan <svlan>	The outer management VLAN, ranging from 1 to 4085	Mandatory	1001
	{cvlan <cvlan>}*1	The inner management VLAN, ranging from 1 to 4085	Optional	2001
Configuring the management IP address	ipv4 <name>	The management IP address name	Mandatory	test
	<A.B.C.D/M>	The management IP address and the number of mask digits	Mandatory	10.90.40.123/24
Adding the management VLAN to the uplink port	vlan <vlanid>	The starting VLAN ID, ranging from 1 to 4085	Mandatory	1001
	{to <end-vlanid>}*1	The ending VLAN ID, ranging from 1 to 4085	Optional	-
	[tag|untag]	The mode of adding VLAN ◆ tag: retaining the tags ◆ untag: stripping the tags	Mandatory	tag
	<frameid/slotid>	The subrack No. / slot No.	Mandatory	1/19

Procedure	Parameter	Description	Attribute	Example
	<port-list>	The port number	Mandatory	3
Viewing the management VLAN	manage-vlan [<1-4085>|all]	The management VLAN ID, with "all" indicating all the management VLANs	Mandatory	all

Example

1. Configure the management VLAN.

```
Admin(config)#manage-vlan test svlan 1001 cvlan 2001
```

2. Configure the management IP address.

```
Admin(config)#manage-vlan ipv4 test 10.90.40.123/24
```

3. Add the management VLAN to the uplink port.

```
Admin(config)#port vlan 1001 tag 1/19 3
```

4. View the management VLAN.

```
Admin(config)#show manage-vlan all
---------------------------------
Manage name     : test
---------------------------------
Svlan           : 1001
Cvlan           : 2001
Port            : 19:3[T]
Device          : sub
Unit            : 1001
Ethernet address: 34:bf:90:56:bc:e7
Total protocols : 0
Inet            : 10.90.40.123
mask            : 255.255.255.0
RX packets      : 0
TX packets      : 6
RX bytes        : 0
TX bytes        : 506
MTU             : 1492
Admin(config)#
```

4.2 Configuring the IP Address for Out-of-Band Management

Command Format

Configure the IP address for out-of-band management.

```
ip address <A.B.C.D> mask <A.B.C.D>
```

View the IP address for out-of-band management.

```
show ip address
```

Planning Data

Parameter	Description	Attribute	Example
ip address <A.B.C.D>	The IP address for out-of-band management	Mandatory	10.182.24.120
mask <A.B.C.D>	Mask	Mandatory	255.255.248.0

Example

1. Set the IP address for out-of-band management to 10.182.24.120 and the mask to 255.255.248.0.

```
Admin(config-if-meth-1)#ip address 10.182.24.120 mask 255.255.248.0
```

2. View the IP address for out-of-band management.

```
Admin(config-if-meth-1)#show ip address
debugip 10.182.24.120 mask 255.255.248.0
Admin(config-if-meth-1)#
```

4.3 Configuring Static Routing

Command Format

```
static-route destination-ip <ipaddr> mask [<mask>|<mask-length>] nexthop
<ipaddr> {metric <metric>}*1
```

Planning Data

Parameter	Description	Attribute	Example
`destination-ip <ipaddr>`	The destination IP address identifying the destination IP address or destination network of the IP messages.	Mandatory	3.3.3.0
`mask [<mask>|<mask-length>]`	◆ <mask>: the subnet mask ◆ <mask-length>: the subnet mask length	Mandatory	255.255.255.0
`nexthop <ipaddr>`	The next-hop IP address of the designated route.	Mandatory	1.1.1.10
`{metric <metric>}*1`	The priority of the route. The system selects the route with the highest priority (the smallest value) to forward IP messages. The route priority ranges from 0 to 255.	Optional	-

Example

Configure a static route, setting the destination IP address to 3.3.3.0, the mask to 255.255.255.0, and the next-hop IP address of the designated route to 1.1.1.10.

```
Admin(config)#static-route destination-ip 3.3.3.0 mask 255.255.255.0 nexthop 1.1.1.10
Admin(config)#
```

4.4 Configuring the SNMP Trap Receiver Address

Command Format

Configure the SNMP Trap receiver address.

```
snmp-agent trap-reciever add ip <ip-address> {security-name <securityname>}*1 {[v1|v2c|v3]}*1
```

View the SNMP Trap receiver address.

```
show snmp-agent trap-receiver
```

Data Planning

Parameter	Description	Attribute	Example
ip <ip-address>	The IP address of the SNMP Trap receiver.	Mandatory	10.32.154.11
{security-name <securityname>}*1	The security name.	Optional	public
{[v1|v2c|v3]}*1	The SNMP version, including v1, v2c and v3.	Optional	v2c

Example

1. Set the IP address of the SNMP Trap receiver to "10.32.154.11", the security name to "public", and the SNMP version to "v2c".

```
Admin(config)#snmp-agent trap-receiver add ip 10.32.154.11 security-name public v2c
```

2. View the SNMP Trap receiver address.

```
Admin(config)#show snmp-agent trap-receiver
IPAddress        Port  Version SecurityName   SecurityLevel  SourceIP
10.190.40.140    162   v2c     public
10.32.103.18     162   v2c     public
10.32.154.11     162   v2c     public
Total 3 trap-receiver in system.
Admin(config)#
```

4.5 Configuring the SNMP Time System

Command Format

Configure the SNMP time management.

```
snmp-time interval <0-86400> servip [ipv4|ipv6|ipv4z|ipv6z|dns] <servip>
```

View the configuration of the SNMP time management.

```
show snmp-time
```

Planning Data

Parameter	Description	Attribute	Example
interval <0-86400>	The automatic time calibration interval (unit: s), ranging from 0 to 86 400. The default value is 600s.	Mandatory	3260
servip [ipv4|ipv6|ipv4z|ipv6z|dns]	The IP address type for time calibration.	Mandatory	ipv4
<servip>	The IP address of the calibration server.	Mandatory	10.32.135.102

Example

1. Configure the SNMP time management.

```
Admin(config)#snmp-time interval 3260 servip ipv4 10.32.135.102
Set ok!
Admin(config)#
```

2. View the configuration of the SNMP time management.

```
Admin(config)#show snmp-time
SNMP TIME CONFIG INTERVAL=3260 Server IP : 10.32.135.102
Admin(config)#
```

4.6 Synchronizing Time

Command Format

```
time <2012-2100> <1-12> <1-31> <HH:MM:SS>
show time
```

Planning Data

Parameter	Description	Attribute	Example
<2012-2100>	Year	Mandatory	2018
<1-12>	Month	Mandatory	08
<1-31>	Day	Mandatory	17
<HH:MM:SS>	Hour, minute and second	Mandatory	04:12:30

Example

1. Calibrate the time.

```
Admin(config)#time 2018 08 17 04:12:30
```

2. View the time.

```
Admin(config)#show time
Current Date is 2018-08-17
Current Time is 04:12:31
System running time is 0 day 04:11:53
Admin(config)#
```

4.7 Saving Current Configuration to the Flash

Command Format

```
save
```

Example

Save current configuration to the Flash.

```
Admin(config)#save
Trying save configuration to flash, please wait ......
Admin(config)#
```

5 Authorizing Cards and ONUs

- ☑ Authorizing a Card
- ☑ Authenticating and Authorizing an ONU
- ☑ Modifying the Authentication Mode and Re-authorizing an ONU
- ☑ Deauthorizing an ONU

5.1 Authorizing a Card

Command Format

Automatically authorize all the cards detected in the hardware test.

```
card auto-auth
```

Authorize a specified card.

```
card auth <frameid/slotid> <cardtype>
```

View the card authorization information.

```
show card info
```

Data Planning

Parameter	Description	Attribute	Example
<frameid/slotid>	Subrack No./slot No.	Mandatory	1/1
<cardtype>	Card name	Mandatory	GPOP

Example

1. Authorize all the cards automatically.

```
Admin(config)#card auto-auth
Success to set all detected card authed.
Admin(config)#
```

2. Authorize the GPOP card in Slot 1 of Subrack 1.

```
Admin(config)#card auth 1/1 GPOP
Success to set 1 slot as type GPOP.
Admin(config)#
```

3. View the card authorization information.

```
Admin(config)#show card info
--------------------AN6001-G16---------------
CARD   EXIST   CONFIG   DETECT    DETAIL
1      YES     GPOP     GPOP       MATCH
9      YES     HSCP     HSCP     MATCH/M
19      YES     HU2P     HU2P       MATCH
23      YES      FAN      FAN       MATCH
24      ---      ---      ---         ---
25      YES     PWRD     PWRD       MATCH
```

```
801     YES      HCU      HCU       MATCH
Current temperature is 42 C.
Power 2 is ON.
FAN 1 speed is 1.
Subframe type is G16.
Admin(config)#
```

5.2 Authenticating and Authorizing an ONU

5.2.1 Configuring the PON Port Authentication Mode

Command Format

```
port authentication-mode <frameid/slotid/portid> mode [phyid|phy-id+psw|
password|log-id|log-id+psw|no-auth|phy-id/psw|phy-id/log-id/psw|phy-id/
log-id+psw/psw]
```

Planning Data

Parameter	Description	Attribute	Example	
<frameid/slotid/portid>	Subrack No. / slot No. / PON port No.	Mandatory	1/1/1	1/1/2
mode [phyid|phy-id+psw|password|log-id|log-id+psw|no-auth|phy-id/psw|phy-id/log-id/psw|phy-id/log-id+psw/psw]	Authentication mode ◆ phyid: physical identifier authentication ◆ phy-id+psw: physical identifier plus password authentication ◆ password: password authentication ◆ log-id: logical identifier authentication (without password) ◆ log-id+psw: logical identifier plus password authentication ◆ no-auth: no authentication ◆ phy-id/psw: physical identifier / password hybrid authentication ◆ phy-id/log-id/psw: physical identifier / logical identifier (without password) / password hybrid authentication ◆ phy-id/log-id+psw/psw: physical identifier / logical identifier (with password) / password hybrid authentication	Mandatory	phyid	no-auth

Example

1. Set physical identifier authentication for PON Port 1 of the PON interface card in Slot 1 of Subrack 1.

```
Admin(config)#port authentication-mode 1/1/1 mode phyid
Command executes success.
Admin(config)#
```

2. Set no authentication for PON Port 2 of the PON interface card in Slot 1 of Subrack 1.

```
Admin(config)#port authentication-mode 1/1/2 mode no-auth
Command executes success.
Admin(config)#
```

5.2.2 Configuring a White List

Command Format

Configure a white list.

```
whitelist add [phy-id|logic-id|password] <sn> {[checkcode] <checkcode>}*1
{[type] <onutype>}*1 {[slot] <slotno> [pon] <ponno> [onuid] <onuid>}*1
```

View the white list.

```
show whitelist [phy-id|logic-id|password] {<frameid/slotid/portid>}*1
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring a white list	[phy-id|logic-id|password]	White list type ◆ phy-id: physical identifier authentication ◆ logic-id: logical identifier authentication ◆ password: password authentication	Mandatory	phy-id
	<sn>	◆ phy-id: physical identifier ◆ logic-id: logical identifier; ONU identifier ◆ password: physical password	Mandatory	8888888888-88
	{[checkcode] <checkcode>}*1	◆ phy-id: physical password ◆ logic-id: logical identifier; logical password	Optional	-
	{[type] <onutype>}*1	ONU type	Optional	HG260
	{[slot] <slotno> [pon] <ponno> [onuid] <onuid>}*1	Slot No., PON port No., and ONU authorization No.	Optional	1, 1, 1
Viewing the white list	[phy-id|logic-id|password]	White list type ◆ phy-id: physical identifier authentication ◆ logic-id: logical identifier authentication ◆ password: password authentication	Mandatory	phy-id

Procedure	Parameter	Description	Attribute	Example
	{<frameid/slo-tid/portid>}*1	Subrack No. / slot No. / PON port No.	Optional	1/1/1

Example

1. Configure a white list for ONU 1 connected to PON Port 1 in Slot 1, setting the physical identifier of the ONU to 888888888888, keeping the physical password empty, and setting the ONU type to HG260.

```
Admin(config)#whitelist add phy-id 888888888888 type HG260 slot 1 pon 1 onuid 1
Admin(config)#
```

2. View the physical white list for PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config)#show whitelist phy-id 1/1/1
----- Physical Address Whitelist -----
Slot  Pon   Onu   Onu-Type       Phy-ID       Phy-Pwd    Used
----- ----- ----- -------------- ------------ ---------- ----
1     1     1     HG260          888888888888            Y
--------------------------
slot 1  pon 1 item 1
Admin(config)#
```

5.3 Modifying the Authentication Mode and Re-authorizing an ONU

5.3.1 Switching the PON Port Authentication Mode

Command Format

```
port authentication-mode <frameid/slotid/portid> mode [phyid|phy-id+psw|
password|log-id|log-id+psw|no-auth|phy-id/psw|phy-id/log-id/psw|phy-id/
log-id+psw/psw]
```

Planning Data

Parameter	Description	Attribute	Example
<frameid/slotid/portid>	Subrack No. / slot No. / PON port No.	Mandatory	1/1/1
mode [phyid|phy-id+psw|password|log-id|log-id+psw|no-auth|phy-id/psw|phy-id/log-id/psw|phy-id/log-id+psw/psw]	Authentication mode ◆ phyid: physical identifier authentication ◆ phy-id+psw: physical identifier plus password authentication ◆ password: password authentication ◆ log-id: logical identifier authentication (without password) ◆ log-id+psw: logical identifier plus password authentication ◆ no-auth: no authentication ◆ phy-id/psw: physical identifier / password hybrid authentication ◆ phy-id/log-id/psw: physical identifier / logical identifier (without password) / password hybrid authentication ◆ phy-id/log-id+psw/psw: physical identifier / logical identifier (with password) / password hybrid authentication	Mandatory	phy-id/log-id+psw/psw

Example

Switch PON Port 1 of the PON interface card in Slot 1 of Subrack 1 from the physical authentication mode to the physical identifier / logical identifier (with password) / password hybrid authentication mode.

```
Admin(config)#port authentication-mode 1/1/1 mode phy-id/log-id+psw/psw
Command executes success.
Admin(config)#
```

5.3.2 Re-configuring a White List

Command Format

Configure a white list.

```
whitelist add [phy-id|logic-id|password] <sn> {[checkcode] <checkcode>}*1
{[type] <onutype>}*1 {[slot] <slotno> [pon] <ponno> [onuid] <onuid>}*1
```

View the white list.

```
show whitelist [phy-id|logic-id|password] {<frameid/slotid/portid>}*1
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring a white list	[phy-id|logic-id|password]	White list type ◆ phy-id: physical identifier authentication ◆ logic-id: logical identifier authentication ◆ password: password authentication	Mandatory	logic-id
	<sn>	◆ phy-id: physical identifier ◆ logic-id: logical identifier; ONU identifier ◆ password: physical password	Mandatory	8888888888
	[checkcode] <checkcode>	◆ phy-id: physical password ◆ logic-id: logical identifier; logical password	Optional	666666
	[type] <onutype>	ONU type	Optional	HG260
	[slot] <slotno> [pon] <ponno> [onuid] <onuid>	Slot No., PON port No., and ONU authorization No.	Optional	1, 1, 1
Viewing the white list	[phy-id|logic-id|password]	White list type ◆ phy-id: physical identifier authentication ◆ logic-id: logical identifier authentication ◆ password: password authentication	Mandatory	logic-id
	{<frameid/slotid/portid>}*1	Subrack No. / slot No. / PON port No.	Optional	1/1/1

Example

1. Configure a white list for ONU 1 connected to PON Port 1 in Slot 1, setting the logical identifier of the ONU to 888888888888, the logical password to 666666, and the ONU type to HG260.

```
Admin(config)#whitelist add logic-id 8888888888 checkcode 666666 type HG260 slot 1 pon 1 onuid 1
```

```
Admin(config)#
```

2. View the logical white list for PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config)#show whitelist logic-id 1/1/1
----- Logic SN Whitelist-----
Slot  Pon   Onu   Onu-Type  Logic-Id      Logic-Pwd    En Used
----- ----- ----- --------- ------------- ------------ -- ----
1     1     1     HG260     8888888888    666666       Y  Y
--------------------------
slot 1  pon 1 item 1
Admin(config)#
```

5.4 Deauthorizing an ONU

- When the no-authentication mode is configured for a PON port, deauthorize the ONU connected to the PON port using the command described in **Deauthorizing an ONU in the No-authentication Mode**.
- In other authentication modes, deauthorize the ONU using the command described in **Deleting the White List**.

5.4.1 Deauthorizing an ONU in the No-authentication Mode

Command Format

```
no authorize <frameid/slotid/portid> <onulist>
```

Planning Data

Parameter	Description	Attribute	Example
<frameid/slotid/portid>	Subrack No. / slot No. / PON port No.	Mandatory	1/1/1
<onulist>	ONU authorization No.	Mandatory	1

Example

De-authorize ONU 1 under PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config)#no authorize 1/1/1 1
Command executes success.
Admin(config)#
```

5.4.2 Deleting an ONU from the Physical Identifier White List

Command Format

```
no whitelist [phy-id|logic-id|password] <slotno> <ponno> <sn> {<checkcode>}*1
```

Planning Data

Parameter	Description	Attribute	Example
[phy-id|logic-id|password]	White list type ◆ phy-id: physical identifier authentication ◆ logic-id: logical identifier authentication ◆ password: password authentication	Mandatory	phy-id
<slotno>	Slot No.	Mandatory	1
<ponno>	PON port No.	Mandatory	1
<sn>	◆ phy-id: physical identifier ◆ logic-id: logical identifier; ONU identifier ◆ password: physical password	Mandatory	888888888888
{<checkcode>}*1	◆ phy-id: physical password ◆ logic-id: logical identifier; logical password	Optional	-

Example

Delete the physical white list for PON Port 1 in Slot 1 with the physical identifier 888888888888.

```
Admin(config)#no whitelist phy-id 1 1 888888888888
Admin(config)#
```

6 Basic Configurations

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

6.1 Configuring Local End Outer VLAN Data

Command Format

Configure local end outer VLAN data.

```
service-vlan <name> <vlanbegin> {[to]<vlanend>}*1 {[type]<value>}*1
```

View the configuration data of local end outer VLAN.

```
show service-vlan {<name>}
```

Planning Data

Parameter	Description	Attribute	Example	
`service-vlan <name>`	The service VLAN name. You can enter numbers, letters and underlines not exceeding 32 characters for the subscriber service name.	Mandatory	data1	ngn1
`<vlanbegin>`	The starting VLAN ID, ranging from 1 to 4085. The starting VLAN ID should not be larger than the ending VLAN ID.	Mandatory	500	300
`{[to]<vlanend>}*1`	The ending VLAN ID, ranging from 1 to 4085. The starting VLAN ID should not be larger than the ending VLAN ID.	Optional	-	-
`{[type]<value>}*1`	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. ◆ cnc: CNC service. ◆ system: system service.	Optional	data	ngn

Example

1. Set the service VLAN name to "data1", service VLAN ID to "500", and VLAN type to "data".

```
Admin(config)#service-vlan data1 500 type data
```

2. Set the service VLAN name to "ngn1", service VLAN ID to "300", and VLAN type to "ngn".

```
Admin(config)#service-vlan ngn1 300 type ngn
Admin(config)#
```

3. View the configuration data of local end outer VLAN.

```
Admin(config)#show service-vlan
servicevlan 101 :
name : data1,   type : data
vlan range: 500 #####end.
servicevlan 102 :
name : ngn1,   type : ngn
vlan range: 300 #####end.
Admin(config)#
```

6.2 Adding Ports to a VLAN

Command Format

Add the uplink port to a VLAN.

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

Add all the slots to the VLAN.

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

Planning Data

Parameter	Description	Attribute	Example
<vlanid>	VLAN ID	Mandatory	300
{to <end-vlanid>}*1	Ending VLAN ID	Optional	-

Parameter	Description	Attribute	Example
[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.	Mandatory	tag
<frameid/slotid>	Subrack No. / slot No.	Mandatory	1/19
<port-list>	Port number	Mandatory	4

Example

1. Add the uplink port to VLAN 300 in the tag mode.

```
Admin(config)#port vlan 300 tag 1/19 4
```

2. Add all the slots to VLAN 300.

```
Admin(config)#port vlan 300 allslot
Admin(config)#
```

6.3 Disabling Suppression of Multicast Packets at the Uplink Port

Command Format

```
no traffic-suppress <frameid/slotid/portid> [broadcast|multicast|unknown|
all]
```

Planning Data

Parameter	Description	Attribute	Example
<frameid/slotid/-portid>	Subrack No. / slot No. / port No.	Mandatory	1/19/3
[broadcast|multicast|unknown|all]	◆ broadcast ◆ multicast: multicast service ◆ unknown: unknown unicast packets ◆ all: all types of packets	Mandatory	multicast

Example

Disable multicast packet suppression for Port 3 in Slot 19 of Subrack 1.

```
Admin(config)#no traffic-suppress 1/19/3 multicast
Admin(config)#
```

7 Configuring TWAMP

This chapter introduces the background information, network scenarios, configuration flow, and configuration examples of TWAMP.

- Background
- Network Scenarios
- Configuration Flow
- Command Format
- Configuration Examples

7.1 Background

Definition

The Two-Way Active Measurement Protocol (TWAMP) is a technology that measures the round-trip performance of an IP network.

TWAMP uses UDP packets to collect statistics about the delay, jitter, and packet loss rate. In addition, TWAMP intelligently separates session control and traffic measurement to provide high security. Performance data about IP links between devices can be collected through the cooperation between the network devices deployed with TWAMP.

TWAMP uses the client-server communication mode.

- Client: Establishes, starts, and stops a TWAMP session; generates and maintains performance statistics.
- Server: Responds to the client's request for establishing, starting, or stopping a TWAMP session.

Purpose of TWAMP

Traditionally, network elements (NEs) themselves generate and maintain statistics about the IP network performance.

To display statistics about the performance of an entire network, a network management system (NMS) is required to manage multiple NEs and collect statistics about these NEs.

However, there may be no NMS deployed or the NMS may be incapable of collecting statistics.

TWAMP is therefore introduced. NEs themselves no longer need to generate or maintain statistics about the IP network performance. The performance management system manages only the TWAMP client and easily obtains statistics about the entire network.

Features of TWAMP

- Allows quick and flexible statistics of IP network performance when the network management system is incapable of doing so.
- Allows performance statistics in an IP network where clock synchronization is unavailable.

7.2 Network Scenarios

Application of TWAMP in an IP Network

In an IP network as illustrated in Figure 7-1, A, B and C act as servers, which are passive in TWAMP performance measurement. While E serves as a client, which is active in the measurement. E initiates statistics on any IP address in the network, collects data, and reports them to the performance management system.

Performance of a network segment can be measured by comparison of the performance data on the two end nodes of the segment. For example, to measure the performance of the network segment between A and B, the client first initiates a TWAMP measurement on A, and then on B. After that, the performance of the segment between A and B is measured based on the comparison between the collected performance data of A and B.

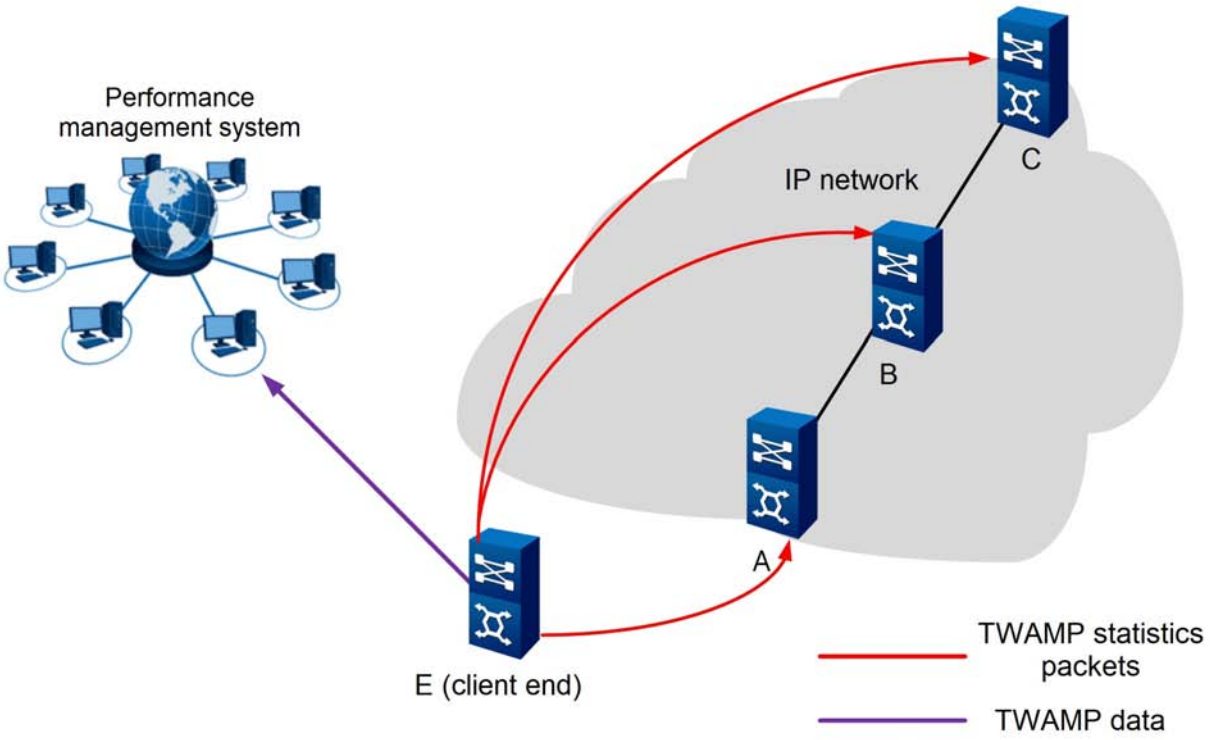


Figure 7-1 Application of TWAMP in an IP Network

Application of TWAMP in an L3VPN (Client in a Private Network)

In a Layer 3 Virtual Private Network (L3VPN), performance data of different IP network segments can be collected depending on the location of the client.

As shown in Figure 7-2, CE acts as the client. It initiates TWAMP statistics on PE1 and PE2 respectively, then compares the data collected from them, and obtains the performance data on the user network interfaces (UNI-UNI) between PE1 and PE2.

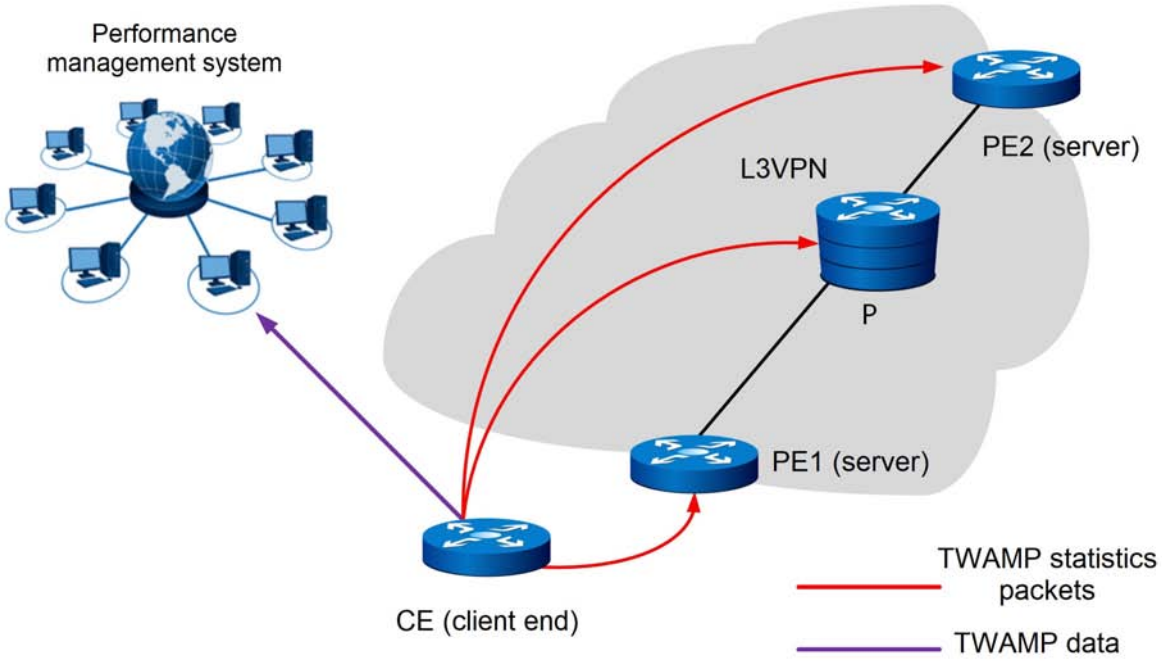


Figure 7-2 Application of TWAMP in an L3VPN (Client in a Private Network)

Application of TWAMP in an L3VPN (Client in a Public Network)

As shown in Figure 7-3, PE1 acts as the client. It initiates TWAMP statistics on P and PE2 respectively, then compares the data collected from them, and obtains the performance data on the UNI-UNI between P and PE2.

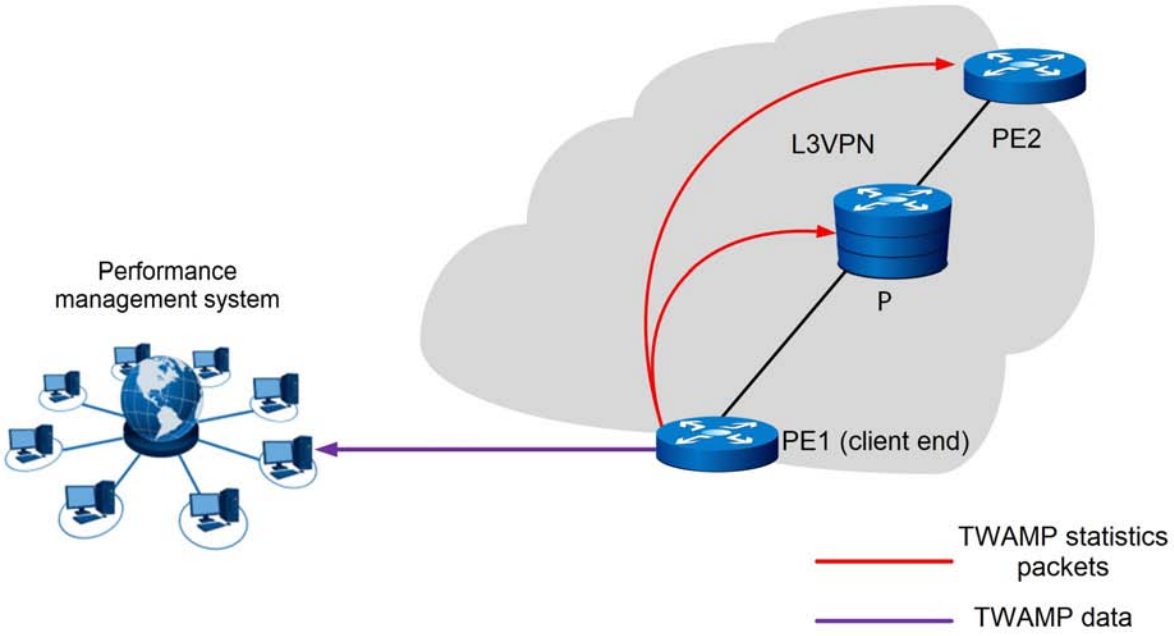


Figure 7-3 Application of TWAMP in an L3VPN (Client in a Public Network)

7.3 Configuration Flow

Figure 7-4 shows the flow of configuring TWAMP.

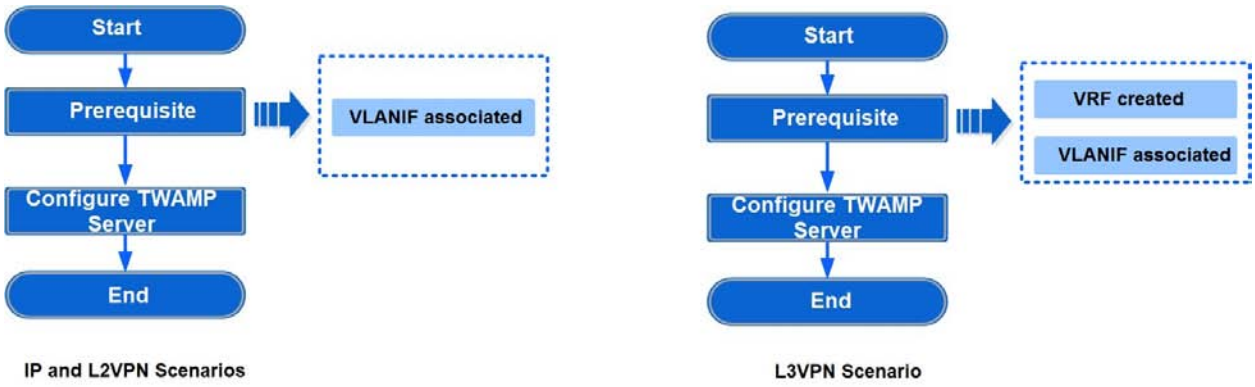


Figure 7-4 TWAMP Configuration Flow

7.4 Command Format

1. Access the TWAMP reflector view and create a session for the reflector.

```
Admin(config-twamp)#twamp-reflector 1
Admin(config-twamp-reflect-1)#
```

2. Delete a session from the reflector.

```
Admin(config-twamp)#no twamp-reflector 1
```

3. Access the secondary view for TWAMP reflector sessions, and configure a physical reflector port (generally UNI port) for an L2VPN scenario. This step is not required for other scenarios.

```
Admin(config-twamp-reflect-1)#reflector-interface 1/19/4
```

4. Delete a physical reflector port (generally a UNI port) for an L2VPN scenario. This step is not required for other scenarios.

```
Admin(config-twamp-reflect-1)#no reflector-interface 1/19/4
```

5. Access the secondary view for TWAMP reflector sessions, and configure the VLAN of the reflector port from which the TWAMP packets are reflected.

```
Admin(config-twamp-reflect-1)#twamp reflect vlan-id 800
```

6. Delete the VLAN of the reflector port from which the TWAMP packets are reflected.

```
Admin(config-twamp-reflect-1)#no twamp reflect vlan-id 800
```

7. Access the secondary view for TWAMP reflector sessions and commit the configuration. Each modification of configuration needs to be committed.

```
Admin(config-twamp-reflect-1)#commit
```

8. Check the configuration result.

```
Admin(config)#show twamp running-config
```

7.5 Configuration Examples

This section introduces how to configure TWAMP in different network scenarios.

7.5.1 Configuration for an IP Scenario

Planning Data

Item	Description	Example
Session Id (wamp-reflector)	ID of the test session	2
send-ip	IP address of the uplink port on the local device (server)	IPV4; 40.1.1.1
ref-ip	IP address of the uplink port on the opposite-end device (client)	IPV4; 50.1.1.1
send-port	Port number range: 1025 to 65535	4000
ref-port	Port number range: 1025 to 65535	5000
DSCP	Default value	255
Refwait (s)	Default value	900
Delay (s)	Default value	5

Example

1. Access the TWAMP view.

```
Admin(config)#twamp
Admin(config-twamp)#
```

2. Create a session on the reflector.

```
Admin(config-twamp)#twamp-reflector 2
Admin(config-twamp-reflect-2)#send-ip 40.1.1.1 ref-ip 50.1.1.1 send-port 4000 ref-port 5000
```

3. Configure the VLAN of the reflector port from which TWAMP packets are reflected.

```
Admin(config-twamp-reflect-2)#twamp reflect vlan-id 800
```

4. Commit the configuration.

```
Admin(config-twamp-reflect-2)#commit
```

5. Check the configuration result.

```
Admin(config)#show twamp running-config
twamp config ----------------------------------------
        twamp
        twamp-reflector 2 send-ip 40.1.1.1 ref-ip 50.1.1.1 send-port
        4000 ref-port 5000
        twamp reflect vlan-id 800
        commit
```

7.5.2 Configuration for an L2VPN Scenario

Planning Data

Item	Description	Example
Session Id (wamp-reflector)	Value range: 1 to 4294967295	1
send-ip	IP address of the uplink port on the local device (server)	IPV4; 30.1.1.1
ref-ip	IP address of the uplink port on the opposite-end device (client)	IPV4; 40.1.1.1
send-port	Port number range: 1025 to 65535	3000
ref-port	Port number range: 1025 to 65535	4000
reflector-interface	Value format: OLT subrack No./slot No./port No.	1/19/4
DSCP	Default value	255
Refwait (s)	Default value	900
Delay (s)	Default value	5

Example

1. Access the TWAMP view.

```
Admin(config)#twamp
Admin(config-twamp)#
```

2. Create a session on the reflector.

```
Admin(config-twamp)#twamp-reflector 1
Admin(config-twamp-reflect-1)#send-ip 30.1.1.1 ref-ip 40.1.1.1 send-port 3000 ref-port 4000
```

3. Configure the physical reflector port.

```
Admin(config-twamp-reflect-1)#reflector-interface 1/19/4
```

4. Configure the VLAN of the reflector port from which TWAMP packets are reflected.

```
Admin(config-twamp-reflect-1)#twamp reflect vlan-id 800
```

5. Commit the configuration.

```
Admin(config-twamp-reflect-1)#commit
```

6. Check the configuration result.

```
Admin(config)#show twamp running-config
twamp config ----------------------------------------
        twamp
```

```
twamp-reflector 1 send-ip 30.1.1.1 ref-ip 40.1.1.1 send-port
3000 ref-port 4000
reflector-interface 1/19/4
twamp reflect vlan-id 800
commit
```

7.5.3 Configuration for an L3VPN Scenario

Prerequisite

- The VRF (VPN bound with the test session of the reflector) has been created.
- The VLANIF has been associated, that is, the VLANIF has been bound with the IP address of the sender's uplink port.

Planning Data

Item	Description	Example
Session Id (wamp-reflector)	Value range: 1 to 4294967295	3
send-ip	IP address of the uplink port on the local device (server)	IPV4; 22.1.1.1
ref-ip	IP address of the uplink port on the opposite-end device (client)	IPV4; 90.1.1.1
send-port	Port number range: 1025 to 65535	4000
ref-port	Port number range: 1025 to 65535	30000
vrf	The created VRF	vpnb
DSCP	Default value	255
Refwait (s)	Default value	900
Delay (s)	Default value	5

Example

1. Access the TWAMP view.

```
Admin(config)#twamp
Admin(config-twamp)#
```

2. Create a session on the reflector.

```
Admin(config-twamp)#twamp-reflector 3
Admin(config-twamp-reflect-3)#send-ip 22.1.1.1 ref-ip 90.1.1.1 send-port 4000 ref-port
30000 vrf vpnb
```

3. Configure the VLAN of the reflector port from which TWAMP packets are reflected.

```
Admin(config-twamp-reflect-3)#twamp reflect vlan-id 300
```

4. Commit the configuration.

```
Admin(config-twamp-reflect-3)#commit
```

5. Check the configuration result.

```
Admin(config)#show twamp running-config
twamp config ----------------------------------------
         twamp
         twamp-reflector 3 send-ip 22.1.1.1 ref-ip 90.1.1.1 send-port
         4000 ref-port 30000 vrf vpnb
         twamp reflect vlan-id 300
         commit
```

8 Configuring Voice Services

- Example of Configuring Voice Service
- Optional Functions

8.1 Example of Configuring Voice Service

8.1.1 Configuring the H.248 Voice Service

Command Format

Configure parameters of the H.248 uplink interface.

```
ngn-uplink-interface name <name> protocol-type [mgcp|h.248|sip] {[mgc] <1-3> <addr> <0-65535>}*3 {[keepalive] [enable|disable|passive]}*1 {[m-dns] [ipv4|ipv6] <ipaddr>}*1 {[s-dns] [ipv4|ipv6] <ipaddr>}*1 {[dhcp] [enable|disable]}*1 {[sip-reg-addr] <addr>}*1 {[sip-reg-port] <0-65535>}*1 {[sip-proxy-addr] <addr>}*1 {[sip-proxy-port] <0-65535>}*1 {[sip-expires] <0-4294967294>}*1
```

Configure parameters of the NGN uplink user.

```
ngn-uplink-user service <name> {[vid] <vid>}*1 {[potsqinqstate] [enable|disable] svlanid <0-4085>}*1 {[service-cos] <value>}*1 {[customer-cos] <value>}*1 {[ip-mode] [static|pppoe|dhcp|pppoev6|dhcpv6]}*1 {[public-ip] [ipv4|ipv6] <ipaddress/prefix>}*1 {[public-gate] [ipv4|ipv6] <ipaddress>}*1 {[pppoeuser] <name> }*1 {[password] <pwd>}*1 {[dhcp-option60] [enable|disable]}*1 {[dhcp-value] <value>}*1 {[domainname] <name>}*1 {[protocol-port] <0-65535>}*1 {[user-index] <value>}*1
```

Configure the user telephone number.

```
ngn-uplink-user-port phone <value> {[username] <name>}*1 {[sip-user-name] <name>}*1 {[sip-user-password] <password>}*1 {[user-index] <value>}*1
```

Configure the NGN softswitch platform interconnection profile. (optional)

```
ngn-softswitch-profile <profilename> fixed <value> varb <value> vare <value> step <value> fixedlen [unfixed|fixed] begint <value> shortt <value> longt <value> matchem [exclusive|immediately] switch [disable|enable] txi <value> rxi <value> voicec [g711u|g711a|nochange] offhkwt [unregiste|registe] flashthd <value> 2833n [disable|enable] 2833d <value> 2198d <value> t38edm [default|v21|all] calleridm [fsk|dtmf] onhkdt <value> dailtonett <value> noanstt <value> busytonett <value> rohtt <value> retrantt <value> ecm [disable|enable] l [chinese|english] {[id] <id>}*1 {[timethd] <value> userthd <value>}*1 {[heart] [notify|change]}*1 {[tripartmode] <value>}*1 {[signaldscp] <value> rtpdscp <value> minport <value> maxport <value> portstep <value>}*1 {[portreg] [disable|enable]}*1
```

Bind the softswitch platform interconnection profile. (optional)

```
onu ngn-iad-softswitch-profile <onulist> profile <profile-name>
```

Configure voice service parameters of the ONU.

```
onu ngn-voice-service <onuno> pots <portno> phonenum <num> {[vid] <vid>}*1
{[code-mode] [g.711m|g.711a|g.723|g.729]}*1 {[fax-mode] [transparent|
t.38]}*1 {[slience] [enable|disable]}*1 {[echo-cancel] [enable|disable]}*1
{[input-gain] <num>}*1 {[voice-value] <value>}*1 {[dtmf] [transparent|
rfc2833|sip]}*1 {[heartbeat] [enable|disable]}*1 {[potsqinqstate] [enable|
disable] svlanid <0-4085>}*1 {[service-cos] <value>}*1 {[customer-cos]
<value>}*1 {[fax-control] [passthrough|softswitch|autovbd]}*1 {[bill-
type] [16kc|12kc|revpol|free]}*1
```

Data Planning

Procedure	Parameter	Description	Attribute	Example
Configuring parameters of the H.248 uplink interface	`ngn-uplink-interface name <name>`	The name of the uplink interface for the NGN voice service, consisting of the service name and the interface identifier.	Mandatory	ngn1@h.248
	`protocol-type [mgcp|h.248|sip]`	The MGC protocol type. ◆ mgcp: the MGCP protocol ◆ h248: the H248 protocol ◆ sip: the SIP protocol	Mandatory	h.248
	`{[mgc] <1-3> <addr> <0-65535>}*3`	<1-3>: the MGC sequence number. <addr>: the MGC address. <0-65535>: the MGC port number.	Optional	1 192.168.1.101 2944
	`{[keepalive] [enable|disable|passive]}*1`	The heartbeat switch. ◆ enable: Enable active heartbeat. ◆ disable: Disable the function. ◆ passive: Enable passive heartbeat.	Optional	enable
	`{[m-dns] [ipv4|ipv6] <ipaddr>}*1`	The master DNS server.	Optional	-
	`{[s-dns] [ipv4|ipv6] <ipaddr>}*1`	The slave DNS server.	Optional	-
	`{[dhcp] [enable|disable]}*1`	The DHCP function switch.	Optional	-

Procedure	Parameter	Description	Attribute	Example
	{[sip-reg-addr] <addr>}*1	The SIP registrar server address.	Optional	-
	{[sip-reg-port] <0-65535>}*1	The port number of the SIP registrar, that is, the protocol port number of the MG registered to the SIP registrar. The value ranges from 0 to 65535, and the default value is 5060.	Optional	-
	{[sip-proxy-addr] <addr>}*1	The address of the SIP proxy server.	Optional	-
	{[sip-proxy-port] <0-65535>}*1	The port number of the SIP proxy server. The value ranges from 0 to 65535, and the default value is 5060.	Optional	-
	{[sip-expires] <0-4294967294>}*1	The SIP timeout time (second). If the MG does not receive the corresponding information from the SIP server before this time expires, the registration fails. The value ranges from 0 to 4294967294.	Optional	-
Configuring parameters of the NGN uplink user	service <name>	The voice service name, same as the name of the uplink interface for the NGN voice service.	Mandatory	ngn1@h.248
	{[vid] <vid>}*1	The signaling VLAN ID.	Optional	300
	[potsqinqstate] [enable|disable]	The SVLAN enabling state.	Optional	-
	svlanid <0-4085>	The SVLAN ID.	Optional	-
	{[service-cos] <value>}*1	The outer CoS.	Optional	-
	{[customer-cos] <value>}*1	The inner CoS.	Optional	-
	{[ip-mode] [static|pppoe|dhcp|pppoev6|dhcpv6]}*1	The IP configuration mode.	Optional	-
	{[public-ip] [ipv4|ipv6] <ipaddress/prefix>}*1	The public network IP address / mask of the ONU. Configure this item according to the operator's network planning.	Optional	ipv4 10.90.60.2/16

Procedure	Parameter	Description	Attribute	Example
	{[public-gate] [ipv4|ipv6] <ipaddress>}*1	The public network gateway IP address of the ONU. Configure this item according to the operator's network planning.	Optional	ipv4 10.90.1.154
	{[pppoeuser] <name> }*1	The PPPoE user name.	Optional	-
	{[password] <pwd>}*1	The PPPoE user password.	Optional	-
	{[dhcp-option60] [enable|disable]}*1	Enables or disables the DHCP Option60 function.	Optional	-
	{[dhcp-value] <value>}*1	The DHCP Option60 suffix.	Optional	-
	{[domainname] <name>}*1	The end point domain name / SIP user name suffix. Configure this item according to the operator's network planning.	Optional	10.90.60.2
	{[protocol-port] <0-65535>}*1	The ONU protocol port. Configure this item according to the operator's network planning. The value ranges from 0 to 65535 and the default value is 2944.	Optional	2944
	{[user-index] <value>}*1	The index ID, ranging from 0 to 40000	Optional	1
Configuring the user phone number	phone <value>	The user index and logical number within 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.	Mandatory	88880003
	{[username] <name>}*1	The endpoint user name / SIP phone number. ◆ When the MGCP or H.248 protocol is used, the end point username should be configured. ◆ When the SIP protocol is used, the SIP telephone number should be configured.	Mandatory	a1
	{[sip-user-name] <name>}*1	The user name authenticated by SIP.	Optional	-

Procedure	Parameter	Description	Attribute	Example
	{[sip-user-password] <password>}*1	The user password authenticated by SIP.	Optional	-
	{[user-index] <value>}*1	The index ID, ranging from 0 to 40000.	Optional	1
Configuring the NGN softswitch platform interconnection profile (optional)	ngn-softswitch-profile <profilename>	The name of the NGN softswitch platform interconnection profile.	Mandatory	ngn1
	fixed <value>	The fixed part of the RTP resource name.	Mandatory	RTP/000
	varb <value>	The starting value of the variable part of the RTP resource name.	Mandatory	0
	vare <value>	The ending value of the variable part of the RTP resource name.	Mandatory	15
	step <value>	The step of the variable part of the RTP resource name.	Mandatory	1
	fixedlen [unfixed|fixed]	The fixed length of the RTP name. ◆ unfixed ◆ fixed	Mandatory	unfixed
	begint <value>	The DigitMap start timer (second). The value ranges from 1 to 255.	Mandatory	16
	shortt <value>	The DigitMap short timer (second). The value ranges from 1 to 255.	Mandatory	4
	longt <value>	The DigitMap long timer (second). The value ranges from 1 to 255.	Mandatory	16
	matchem [exclusive|immediately]	Reporting the matching result immediately when match with any rule is found. ◆ exclusive: reporting when exclusive matching is found ◆ immediately: reporting immediately	Mandatory	immediately
	switch [disable|enable]	The VBD state.	Mandatory	disable
	txi <value>	The VBD Tx packet interval (ms).	Mandatory	20
	rxi <value>	The VBD Rx packet interval (ms).	Mandatory	10

Procedure	Parameter	Description	Attribute	Example
	voicec [g711u| g711a|nochange]	The VBD encoding type. ◆ g711u: G.711U ◆ g711a: G.711A ◆ nochange: not changed	Mandatory	nochange
	offhkwt [unregiste| registe]	Howler tone timeout processing	Mandatory	unregiste
	flashthd <value>	The flash duration (ms).	Mandatory	90
	2833n [disable| enable]	The RFC2833 negotiation state. ◆ disable: no auto-negotiation ◆ enable: auto-negotiation	Mandatory	disable
	2833d <value>	The default RFC2833 PT.	Mandatory	97
	2198d <value>	The default RFC2198 PT.	Mandatory	96
	t38edm [default| v21|all]	The T.38 event detection mode. ◆ default: normal report ◆ v21: reporting V21 only ◆ all: all reporting V21	Mandatory	default
	calleridm [fsk| dtmf]	The caller ID mode.	Mandatory	fsk
	onhkdt <value>	The minimum onhook detection time (ms).	Mandatory	600
	dailtonett <value>	The dial tone time (s).	Mandatory	60
	noanstt <value>	The no-answer tone time (s).	Mandatory	60
	busytonett <value>	The busy tone time (s).	Mandatory	60
	rohtt <value>	The howler tone time (s).	Mandatory	60
	retrantt <value>	The retransmission timer (s).	Mandatory	25
	ecm [disable| enable]	The error correction switch. ◆ enable: Enable the function. ◆ disable: Disable the function.	Mandatory	disable
	l [chinese| english]	The CLI language. ◆ chinese ◆ english	Mandatory	english
	{[id] <id>}*1	The profile ID.	Optional	1
	[timethd] <value>	The NGN register timer threshold (s).	Optional	-
	userthd <value>	The threshold for quantity of NGN registered users.	Optional	-

Procedure	Parameter	Description	Attribute	Example
	{[heart] [notify|change]}*1	The heatbeat mode.	Optional	-
	{[tripartmode] <value>}*1	The three-party service establishing mode.	Optional	-
	[signaldscp] <value>	The signaling DSCP value.	Optional	-
	rtpdscp <value>	The media stream DSCP value.	Optional	-
	minport <value>	The minimum port number for RTP flow.	Optional	-
	maxport <value>	The maximum port number for RTP flow.	Optional	-
	portstep <value>	The step of the RTP flow port number.	Optional	-
	{[portreg] [disable|enable]}*1	The port registration.	Optional	-
Binding the softswitch platform interconnection profile (optional)	<onulist>	The ONU authorization number.	Mandatory	1
	profile <profile-name>	The name of the softswitch platform interconnection profile.	Mandatory	ngn1
Configuring voice service parameters of the ONU	<onuno>	The ONU authorization number.	Mandatory	1
	pots <portno>	The POTS port number.	Mandatory	1
	phonenum <num>	The telephone number.	Optional	88880003
	{[vid] <vid>}*1	The VLAN ID.	Optional	-
	{[code-mode] [g.711m|g.711a|g.723|g.729]}*1	The voice encoding mode, i.e., the compression encoding mode for the NGN service voice stream. Select the encoding mode as required. The default setting is G.711A.	Optional	g.711a
	{[fax-mode] [transparent|t.38]}*1	The fax mode. "transparent" refers to the transparent mode, i.e., T.30 fax. Select the fax mode as needed. The default setting is "transparent".	Mandatory	transparent

Procedure	Parameter	Description	Attribute	Example
	{[slience] [enable|disable]}*1	The silence switch. When this function is enabled and no voice is detected during the conversion, mute compression packets are transmitted. ◆ enable: Enable the function. ◆ disable: Disable the function.	Mandatory	enable
	{[echo-cancel] [enable|disable]}*1	The echo suppression. The echo is suppressed when this function is enabled. ◆ enable: Enable the function. ◆ disable: Disable the function.	Optional	-
	{[input-gain] <num>}*1	The input gain. The value range is -32 to 32.	Optional	-
	{[voice-value] <value>}*1	The output gain. The value range is -32 to 32.	Optional	-
	{[dtmf] [transparent| rfc2833|sip]}*1	The DTMF mode.	Optional	-
	{[heartbeat] [enable|disable]}*1	The heartbeat function. ◆ enable: Enable the function. ◆ disable: Disable the function.	Optional	-
	[potsqinqstate] [enable|disable]	The SVLAN enabling state.	Optional	-
	svlanid <0-4085>	The SVLAN ID.	Optional	-
	{[service-cos] <value>}*1	The outer CoS.	Optional	-
	{[customer-cos] <value>}*1	The inner CoS.	Optional	-
	{[fax-control] [passthrough| softswitch| autovbd]}*1	The fax control mode. ◆ passthrough: voice path ◆ softswitch: softswitch full-control ◆ autovbd: auto negotiation	Optional	-
	{[bill-type] [16kc|12kc| revpol|free]}*1	The bill type. ◆ 16kc: 16KC ◆ 16kc: 12KC ◆ revpol: reversal polarity ◆ free: no charging	Optional	-

Example

1. Configure parameters of the H.248 uplink interface.

```
Admin(config)#ngn-uplink-interface name ngn1@h.248 protocol-type h.248 mgc 1
192.168.1.101 2944 keepalive enable
```

2. Configure parameters of the NGN uplink user.

```
Admin(config)#ngn-uplink-user service ngn1@h.248 vid 300 public-ip ipv4 10.90.60.2/16
public-gate ipv4 10.90.1.154 domainname 10.90.60.2 protocol-port 2944 user-index 1
Admin(config)#
```

3. Configure the user telephone number.

```
Admin(config)#ngn-uplink-user-port phone 88880003 username a1 user-index 1
Admin(config)#
```

4. Configure the NGN softswitch platform interconnection profile.

```
Admin(config)#ngn-softswitch-profile ngn1 fixed RTP/000 varb 15 vare 15 step 1 fixedlen
unfixed begint 16 shortt 4 longt 16 matchem immediately switch disable txi 20 rxi 10 voicec
nochange offhkwt unregiste flashthd 90 2833n disable 2833d 97 2198d 96 t38edm default
calleridm fsk onhkdt 600 dailtonett 60 noanstt 60 busytonett 60 rohtt 60 retrantt 25 ecm
disable l chinese id 1
Admin(config)#
```

5. Bind the softswitch platform interconnection profile.

```
Admin(config-if-pon-1/1/1)#onu ngn-iad-softswitch-profile 1 profile ngn1
Admin(config-if-pon-1/1/1)#
```

6. Configure voice service parameters of the ONU.

```
Admin(config-if-pon-1/1/1)#onu ngn-voice-service 1 pots 1 phonenum 88880003
code-mode g.711a fax-mode transparent slience enable
Admin(config-if-pon-1/1/1)#
```

7. Save the configuration data.

```
Admin(config)#save
Trying save configuration to flash, please wait ...... save config success
Admin(config)#
```

8.1.2 Configuring the SIP Voice Service

Command Format

Configure parameters of the SIP uplink interface.

```
ngn-uplink-interface name <name> protocol-type [mgcp|h.248|sip] {[mgc] <1-
3> <addr> <0-65535>}*3 {[keepalive] [enable|disable|passive]}*1 {[m-dns]
```

```
[ipv4|ipv6] <ipaddr>}*1 {[s-dns] [ipv4|ipv6] <ipaddr>}*1 {[dhcp] [enable|
disable]}*1 {[sip-reg-addr] <addr>}*1 {[sip-reg-port] <0-65535>}*1 {[sip-
proxy-addr] <addr>}*1 {[sip-proxy-port] <0-65535>}*1 {[sip-expires] <0-
4294967294>}*1
```

Configure parameters of the NGN uplink user.

```
ngn-uplink-user service <name> {[vid] <vid>}*1 {[potsqinqstate] [enable|
disable] svlanid <0-4085>}*1 {[service-cos] <value>}*1 {[customer-cos]
<value>}*1 {[ip-mode] [static|pppoe|dhcp|pppoev6|dhcpv6]}*1 {[public-ip]
[ipv4|ipv6] <ipaddress/prefix>}*1 {[public-gate] [ipv4|ipv6] <ipaddress>}
*1 {[pppoeuser] <name> }*1 {[password] <pwd>}*1 {[dhcp-option60] [enable|
disable]}*1 {[dhcp-value] <value>}*1 {[domainname] <name>}*1 {[protocol-
port] <0-65535>}*1 {[user-index] <value>}*1
```

Configure the user telephone number.

```
ngn-uplink-user-port phone <value> {[username] <name>}*1 {[sip-user-name]
<name>}*1 {[sip-user-password] <password>}*1 {[user-index] <value>}*1
```

Configure voice service parameters of the ONU.

```
onu ngn-voice-service <onuno> pots <portno> phonenum <num> {[vid] <vid>}*1
{[code-mode] [g.711m|g.711a|g.723|g.729]}*1 {[fax-mode] [transparent|
t.38]}*1 {[slience] [enable|disable]}*1 {[echo-cancel] [enable|disable]}*1
{[input-gain] <num>}*1 {[voice-value] <value>}*1 {[dtmf] [transparent|
rfc2833|sip]}*1 {[heartbeat] [enable|disable]}*1 {[potsqinqstate] [enable|
disable] svlanid <0-4085>}*1 {[service-cos] <value>}*1 {[customer-cos]
<value>}*1 {[fax-control] [passthrough|softswitch|autovbd]}*1 {[bill-
type] [16kc|12kc|revpol|free]}*1
```

Data Planning

Procedure	Parameter	Description	Attribute	Example
Configuring parameters of the SIP uplink interface	`ngn-uplink-interface name <name>`	The name of the uplink interface for the NGN voice service, consisting of the service name and the interface identifier.	Mandatory	ngn1@sip
	`protocol-type [mgcp|h.248|sip]`	The MGC protocol type. ◆ mgcp: the MGCP protocol ◆ h248: the H248 protocol ◆ sip: the SIP protocol	Mandatory	sip

Procedure	Parameter	Description	Attribute	Example
	{[mgc] <1-3> <addr> <0-65535>} *3	<1-3>: the MGC sequence number. <addr>: the MGC address. <0-65535>: the MGC port number.	Optional	-
	{[keepalive] [enable|disable| passive]}*1	The heartbeat switch. ◆ enable: Enable active heartbeat. ◆ disable: Disable the function. ◆ passive: Enable passive heartbeat.	Optional	-
	{[m-dns] [ipv4| ipv6] <ipaddr>}*1	The master DNS server.	Optional	-
	{[s-dns] [ipv4| ipv6] <ipaddr>}*1	The slave DNS server.	Optional	-
	{[dhcp] [enable| disable]}*1	The DHCP function switch.	Optional	-
	{[sip-reg-addr] <addr>}*1	The SIP registrar server address.	Optional	10.80.20.3
	{[sip-reg-port] <0-65535>}*1	The port number of the SIP registrar, that is, the protocol port number of the MG registered to the SIP registrar. The value ranges from 0 to 65535, and the default value is 5060.	Optional	5060
	{[sip-proxy-addr] <addr>}*1	The address of the SIP proxy server.	Optional	10.80.20.3
	{[sip-proxy-port] <0-65535>}*1	The port number of the SIP proxy server. The value ranges from 0 to 65535, and the default value is 5060.	Optional	5060
	{[sip-expires] <0-4294967294>}*1	The SIP timeout time (second). If the MG does not receive the corresponding information from the SIP server before this time expires, the registration fails. The value ranges from 0 to 4294967294.	Optional	3600

Procedure	Parameter	Description	Attribute	Example
Configuring parameters of the NGN uplink user	service <name>	The voice service name, same as the name of the uplink interface for the NGN voice service.	Mandatory	ngn1@sip
	{[vid] <vid>}*1	The signaling VLAN ID.	Optional	300
	[potsqinqstate] [enable|disable]	The SVLAN enabling state.	Optional	-
	svlanid <0-4085>	The SVLAN ID.	Optional	-
	{[service-cos] <value>}*1	The outer CoS.	Optional	-
	{[customer-cos] <value>}*1	The inner CoS.	Optional	-
	{[ip-mode] [static|pppoe|dhcp|pppoev6|dhcpv6]}*1	The IP configuration mode.	Optional	static
	{[public-ip] [ipv4|ipv6] <ipaddress/prefix>}*1	The public network IP address / mask of the ONU. Configure this item according to the operator's network planning.	Optional	ipv4 10.80.20.3/16
	{[public-gate] [ipv4|ipv6] <ipaddress>}*1	The public network gateway IP address of the ONU. Configure this item according to the operator's network planning.	Optional	ipv4 10.80.1.254
	{[pppoeuser] <name> }*1	The PPPoE user name.	Optional	-
	{[password] <pwd>}*1	The PPPoE user password.	Optional	-
	{[dhcp-option60] [enable|disable]}*1	Enabling DHCP Option60.	Optional	-
	{[dhcp-value] <value>}*1	The DHCP Option60 suffix.	Optional	-
	{[domainname] <name>}*1	The end point domain name / SIP user name suffix. Configure this item according to the operator's network planning.	Optional	10.80.20.3

Procedure	Parameter	Description	Attribute	Example
	{[protocol-port] <0-65535>}*1	The ONU protocol port. Configure this item according to the operator's network planning. The value ranges from 0 to 65535 and the default value is 5060.	Optional	5060
	{[user-index] <value>}*1	The index ID, ranging from 0 to 40000	Optional	1
Configuring the user phone number	phone <value>	The user index and logical number within 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.	Mandatory	88880003
	{[username] <name>}*1	The endpoint user name / SIP phone number. ◆ When the MGCP or H.248 protocol is used, the endpoint username should be configured. ◆ When the SIP protocol is used, the SIP telephone number should be configured.	Mandatory	88882211
	{[sip-user-name] <name>}*1	The user name authenticated by SIP.	Optional	test3
	{[sip-user-password] <password>}*1	The user password authenticated by SIP.	Optional	test3
	{[user-index] <value>}*1	The index ID, ranging from 0 to 40000.	Optional	1
Configuring voice service parameters of the ONU	<onuno>	The ONU authorization number.	Mandatory	1
	pots <portno>	The POTS port number.	Mandatory	1
	phonenum <num>	The telephone number.	Optional	88880003
	{[vid] <vid>}*1	The VLAN ID.	Optional	-

Procedure	Parameter	Description	Attribute	Example
	{[code-mode] [g.711m|g.711a|g.723|g.729]}*1	The voice encoding mode, i.e., the compression encoding mode for the NGN service voice stream. Select the encoding mode as required. The default setting is G.711A.	Optional	g.711a
	{[fax-mode] [transparent|t.38]}*1	The fax mode. "transparent" refers to the transparent mode, i.e., T.30 fax. Select the fax mode as needed. The default setting is "transparent".	Mandatory	transparent
	{[slience] [enable|disable]}*1	The silence switch. When this function is enabled and no voice is detected during the conversion, mute compression packets are transmitted. ◆ enable: Enable the function. ◆ disable: Disable the function.	Mandatory	enable
	{[echo-cancel] [enable|disable]}*1	The echo suppression. The echo is suppressed when this function is enabled. ◆ enable: Enable the function. ◆ disable: Disable the function.	Optional	-
	{[input-gain] <num>}*1	The input gain. The value range is -32 to 32.	Optional	-
	{[voice-value] <value>}*1	The output gain. The value range is -32 to 32.	Optional	-
	{[dtmf] [transparent|rfc2833|sip]}*1	The DTMF mode.	Optional	-
	{[heartbeat] [enable|disable]}*1	The heartbeat function. ◆ enable: Enable the function. ◆ disable: Disable the function.	Optional	-
	[potsqinqstate] [enable|disable]	The SVLAN enabling state.	Optional	-
	svlanid <0-4085>	The SVLAN ID.	Optional	-
	{[service-cos] <value>}*1	The outer CoS.	Optional	-

Procedure	Parameter	Description	Attribute	Example
	{[customer-cos] <value>}*1	The inner CoS.	Optional	-
	{[fax-control] [passthrough| softswitch| autovbd]}*1	The fax control mode. ◆ passthrough: voice path ◆ softswitch: softswitch full-control ◆ autovbd: auto negotiation	Optional	-
	{[bill-type] [16kc|12kc| revpol|free]}*1	The bill type. ◆ 16kc: 16KC ◆ 16kc: 12KC ◆ revpol: reversal polarity ◆ free: no charging	Optional	-

Example

1. Configure parameters of the SIP uplink interface.

```
Admin(config)#ngn-uplink-interface name ngn1@sip protocol-type sip sip-reg-addr 10.80.20.3 sip-reg-port 5060 sip-proxy-addr 10.80.20.3 sip-proxy-port 5060 sip-expires 3600
```

2. Configure parameters of the NGN uplink user.

```
Admin(config)#ngn-uplink-user service ngn1@sip vid 300 ip-mode static public-ip ipv4 10.80.20.3/16 public-gate ipv4 10.80.1.254 domainname 10.80.20.3 protocol-port 5060 user-index 1
```

3. Configure the user telephone number.

```
Admin(config)#ngn-uplink-user-port phone 88880003 username 88882211 sip-user-name test3 sip-user-password test3 user-index 1
```

4. Configure voice service parameters of the ONU.

```
Admin(config-if-pon-1/1/1)#onu ngn-voice-service 1 pots 1 phonenum 88880003 code-mode g.711a fax-mode transparent slience enable
Admin(config-if-pon-1/1/1)#
```

5. Save the configuration data.

```
Admin(config)#save
Trying save configuration to flash, please wait ......
save config success
Admin(config)#
```

8.2 Optional Functions

8.2.1 Configuring NGN Heartbeat Parameters

Command Format

```
ngn-keepalive service <name> aliveinterval <1-65535> alivetimes <1-65535>
```

Planning Data

Parameter	Description	Attribute	Example
service <name>	The NGN service name.	Mandatory	ngn1
aliveinterval <1-65535>	The heartbeat interval (s), i.e., the interval for sending keep-alive messages.	Mandatory	60
alivetimes <1-65535>	The heartbeat timeout times. If the MGC fails to receive the keep-alive messages from the ONU in time for the set times, it is considered that the MGC loses its communication with the ONU.	Mandatory	60

Example

```
Admin(config)#ngn-keepalive service ngn1 aliveinterval 60 alivetimes 60
Admin(config)#
```

8.2.2 Configuring IAD MD5 Authentication

Command Format

```
ngn-iad-md5 domain <name> md5-state [enable|disable] {[mgid] <value>}*1
{[key] <value>}*1 {[dhg-value] <value>}*1 {[dhp-value] <value>}*1
```

Planning Data

Parameter	Description	Attribute	Example
domain <name>	The end point domain name. It should be consistent with the endpoint domain name configured in the "NGN uplink user parameter".	Mandatory	10.90.60.2
md5-state [enable|disable]	The MD5 state. Configure this item according to the network planning of the operator.	Mandatory	enable

Parameter	Description	Attribute	Example
{[mgid] <value>}*1	The MG ID. Configure this item according to the network planning of the operator.	Optional	60
{[key] <value>}*1	The key. Configure this item according to the network planning of the operator.	Optional	60
{[dhg-value] <value>}*1	The base g. Configure this item according to the network planning of the operator.	Optional	60
{[dhp-value] <value>}*1	The prime p. Configure this item according to the network planning of the operator.	Optional	60

Example

```
Admin(config)#ngn-iad-md5 domain 10.90.60.2 md5-state enable mgid 60 key 60 dhg-value 60 dhp-value 60
Admin(config)#
```

8.2.3 Configuring the Digitmap

Command Format

Configure the digitmap.

```
ngn-bitmap bitmap1 <bitmap> {id <index> <name>}*1
ngn-bitmap bitmap2 <bitmap> {id <index>}*1
ngn-bitmap bitmap3 <bitmap> {id <index>}*1
ngn-bitmap bitmap4 <bitmap> {id <index>}*1
ngn-bitmap bitmap5 <bitmap> {id <index>}*1
ngn-bitmap bitmap6 <bitmap> {id <index>}*1
ngn-bitmap bitmap7 <bitmap> {id <index>}*1
ngn-bitmap bitmap8 <bitmap> {id <index>}*1
```

Bind the digitmap profile to an ONU.

```
onu bitmap-profile <onulist> profile-id <index>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the digitmap	<bitmap>	The digitmap, no longer than 128 bytes	Mandatory	123456777-77

Procedure	Parameter	Description	Attribute	Example
	{id <index> <name>}*1	The ID and name of the digitmap profile	Optional	3, wang
Binding the digitmap profile to an ONU	<onulist>	The ONU authorization No.	Mandatory	1
	profile-id <index>	The digitmap profile ID	Mandatory	3

Example

1. Configure the digitmap.

```
Admin(config)#ngn-bitmap bitmap1 12345677777 id 3 wang
Admin(config)#
```

2. Bind the digitmap profile to ONU 1 under PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/1)#onu bitmap-profile 1 profile-id 3
Admin(config-if-pon-1/1/1)#
```

9 Configuring Data Services

- Example for Data Service Configuration in the Transparent Transmission Mode
- Example for Data Service Configuration in the VLAN Translation Mode
- Example for Data Service Configuration in the TAG Mode

9.1 Example for Data Service Configuration in the Transparent Transmission Mode

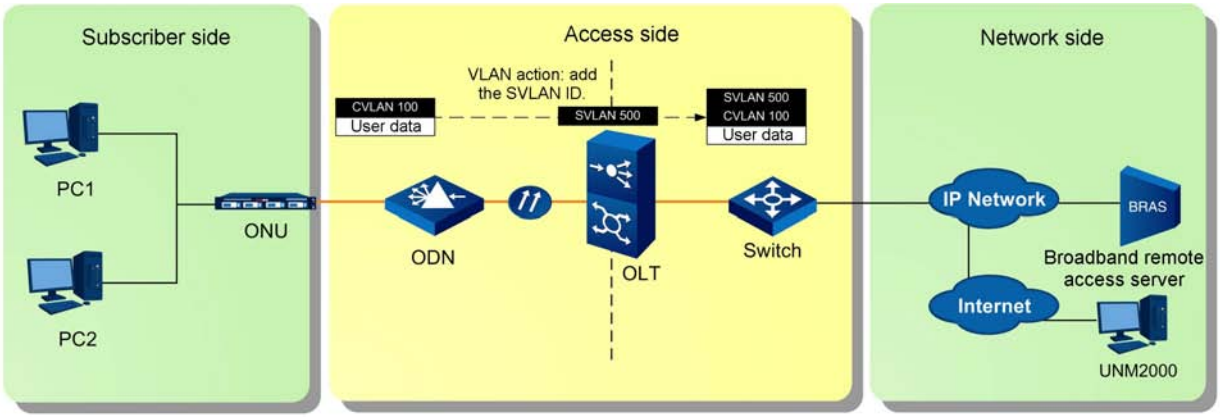
9.1.1 Network Scenario

Service Planning

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

Network Diagram

The network diagram for the data service in the transparent transmission mode is shown in the figure below.



9.1.2 Configuring Parameters of Data Services at the ONU Ports

Command Format

Configure the quantity of services at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service count <service-count>
```

Configure the type of service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> type [multicast|
unicast]
```

Note:

The service type is unicast by default. Configure it to multicast service if it is required.

Configure the VLAN mode for the service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> [tag|transparent]
priority <priority> tpid <tpid> vid <vlanlist>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring quantity of services at the ONU port	`<onulist>`	The ONU authorization No.	Mandatory	1
	`eth <onu-port>`	The ONU port No.	Mandatory	1
	`service count <service-count>`	The quantity of services	Mandatory	1
Configuring VLAN mode for the service at the ONU port	`service <serviceid>`	The service ID, ranging from 1 to 10	Mandatory	1
	`[tag| transparent]`	The service VLAN mode ◆ tag: the TAG identifier ◆ transparent: transparent transmission	Mandatory	transparent
	`priority <priority>`	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	Mandatory	7
	`tpid <tpid>`	The TPID, i.e, the tag protocol identifier. The value ranges from 0 to 65534, and the default value is 33024.	Mandatory	33024
	`vid <vlanlist>`	The CVLAN ID, ranging from 1 to 4085	Mandatory	100

Example

1. Configure the ONU with the authorization number 1 under PON Port 1 in Slot 1 of Subrack 1, adding a service to Port 1 of the ONU.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service count 1
Admin(config-if-pon-1/1/1)#
```

2. Configure the VLAN mode for Port 1 of ONU 1, setting the service ID to 1, service VLAN mode to transparent transmission, priority level to 7, tag protocol identifier to 33024, and VLAN ID to 100.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 transparent priority 7 tpid 33024 vid 100
Admin(config-if-pon-1/1/1)#
```

9.1.3 Configuring the ONU QinQ Profile

Command Format

```
onuqinq-classification-profile [add|modify] <profile-name> {<field-type> <field-val> <operator>}*8
```

Planning Data

Parameter	Description	Attribute	Example
[add|modify]	◆ add ◆ modify	Mandatory	add
<profile-name>	The profile name	Mandatory	qinq

Parameter	Description	Attribute	Example
<field-type>	The rule domain type. The value ranges from 0 to 18. ◆ 0 (Src Mac): source MAC address ◆ 1 (Dst Mac): destination MAC address ◆ 2 (Src IPv4): source IP address ◆ 3 (Dst IPv4): destination IP address ◆ 4 (VID): VLAN ID ◆ 5 (Ethernet Type): Ethernet type ◆ 6 (Protocol Type): IP protocol type ◆ 7 (COS): Ethernet priority ◆ 8 (TOS): IP TOS/DSCP (IP v4) ◆ 9 (L4 Src Port): L4 source port ◆ 10 (L4 Dst Port): L4 destination port ◆ 11 (Dst IPv6 Prefix): destination IPv6 address ◆ 12 (Src IPv6 Prefix): source IPv6 address ◆ 13 (IP Version): IP version ◆ 14 (IPv6 Traffic Class): IPv6 traffic class ◆ 15 (IPv6 Flow Label): IPv6 flow label ◆ 16 (IPv6 Next Header): IPv6 next header ◆ 17 (Src IPv6): source IPv6 address ◆ 18 (Dst IPv6): destination IPv6 address	Optional	0
<field-val>	The rule domain value, which depends on the type of the rule domain. The rule domain type is	Optional	000000000000

Parameter	Description	Attribute	Example
	displayed before the brackets, while the rule domain value is inside the brackets. ◆ 0: the source MAC address (6 bytes) ◆ 1: the destination MAC address (6 bytes) ◆ 2: based on the source IP address classification (4 bytes) ◆ 3: based on the destination IP address classification (4 bytes) ◆ 4: based on the VLAN ID classification (2 bytes; 0 to 4085; 0 to 4095 is available for temporary requirement) ◆ 5: based on the Ethernet type (2 bytes, 0 to 0xffff) ◆ 6: based on the IP protocol type (1 byte, 0 to 0xff) ◆ 7: based on the Ethernet priority classification (1 byte, 1 to 7) ◆ 8: based on the IP TOS/DSCP (IPv4) classification (1 byte, 0 to 0xff) ◆ 9: based on the L4 source PORT classification (2 bytes, 0 to 0xffff) ◆ 10: based on the L4 destination PORT classification (2 bytes, 0 to 0xffff) ◆ 11: based on the destination IPv6 address prefix classification ◆ 12: based on the source IPv6 address prefix classification ◆ 13: based on the IP version (v4 or v6) classification (2 bytes, v4 or v6) ◆ 14: based on the IPv6 traffic class (1 byte, 0 to 255) ◆ 15: based on the IPv6 flow label (4 bytes, 0 to 0xFFFFF) ◆ 16: based on the IPv6 next header (1 byte, 0 to 255) ◆ 17: based on the source IPv6 address (16 bytes) ◆ 18: based on the destination IPv6 address (16 bytes)		

Parameter	Description	Attribute	Example
<operator>	The operator, which is an integer ranging from 0 to 6 ◆ 0 indicates "equal to" (=). ◆ 1 indicates "not equal to" (! =). ◆ 2 indicates "equal to or smaller than" (< =). ◆ 3 indicates "equal to or larger than" (> =). ◆ 4 indicates "exist then match". ◆ 5 indicates "not exist then match". ◆ 6 indicates "always match".	Optional	4

Example

Configure a QinQ profile named "qinq". The profile rule is that it is valid when the source MAC address 000000000000 exists (exist then match).

```
Admin(config)#onuqinq-classification-profile add qinq 0 000000000000 4
Admin(config)#
```

9.1.4 Binding the QinQ Profile to an ONU

Command Format

```
onu port vlan <onulist> eth <onu-port> service <serviceid> qinq [enable|
disable] {priority <priority> tpid <tpid> vid <s-vlanlist> <qinq-
classification-profile> <service-profile>}*1
```

Planning Data

Parameter	Description	Attribute	Example
<onulist>	ONU authorization No.	Mandatory	1
<onu-port>	ONU port	Mandatory	1
service <serviceid>	Service ID	Mandatory	1
qinq [enable|disable]	QinQ state ◆ enable: enabled ◆ disable: disabled	Mandatory	enable
priority <priority>	The SVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	Optional	7
tpid <tpid>	The TPID, i.e, the tag protocol identifier. The value ranges from 1 to 65535, and the default value is 33024.	Optional	33024

Parameter	Description	Attribute	Example
vid <s-vlanlist>	The SVLAN ID, ranging from 1 to 4085	Optional	500
<qinq-classification-profile>	QinQ profile name	Optional	qinq
<service-profile>	Service VLAN name	Optional	data1

Example

Enable the QinQ function for Service 1 at Port 1 of ONU 1, setting the priority of the service to "7", the TPID to "33024", the SVLAN to "500", the QinQ profile name to "qinq" and the service VLAN name to "data1". The ONU is under PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 qinq enable priority 7 tpid 33024 vid 500 qinq data1
Admin(config-if-pon-1/1/1)#
```

9.2 Example for Data Service Configuration in the VLAN Translation Mode

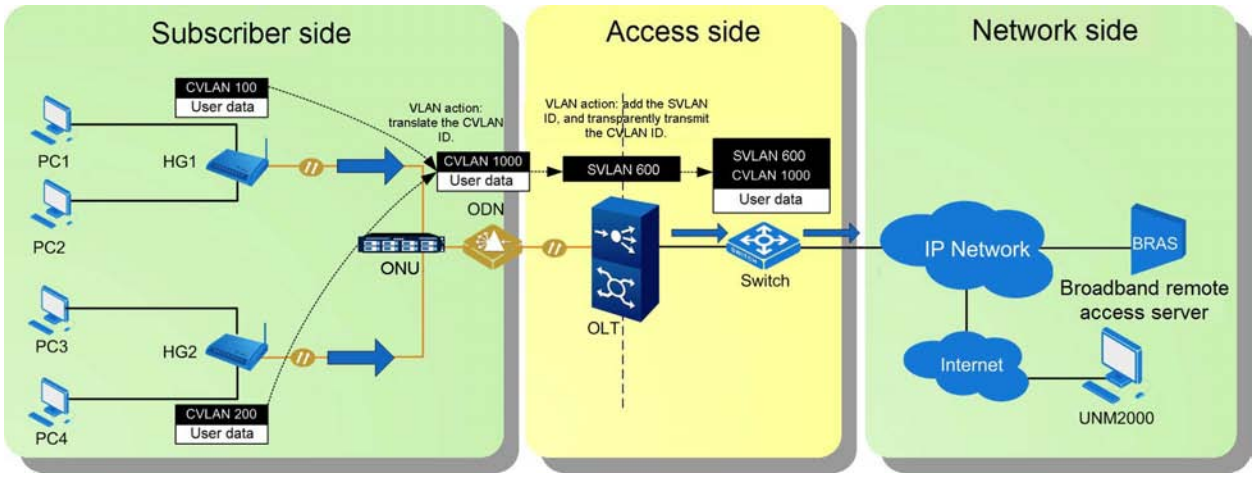
9.2.1 Network Scenario

Service Planning

The subscribers' 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 OLT. The OLT 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 N:1 translation mode is shown in the figure below.



- In the uplink direction, the data services uploaded by the two subscribers' PCs are added with different CVLAN IDs by the home gateways and uplinked to the ONU. The ONU translates the CVLAN IDs and transmits them to the OLT via the splitters. The OLT 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 OLT. The OLT 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 subscribers' PCs.

9.2.2 Configuring the OLT QinQ Domain

Command Format

Create a QinQ domain.

```
oltqinq-domain add <name>
```

Configure the quantity of services in the QinQ domain.

```
oltqinq-domain modify <name> service-count <service-count>
```

Configure uplink rules for the OLT QinQ domain.

```
oltqinq-domain <name> service <1-8> classification upstream {field-id <1-
27> value <value> condition <condition>}*4 {serv-id <1-8>}*1
```

Configure downlink rules for the OLT QinQ domain.

```
oltqinq-domain <name> service <1-8> classification downstream {field-id <1-27> value <value> condition <condition>}*4
```

Configure the service VLAN for the QinQ domain.

```
oltqinq-domain <name> service <1-8> {vlan <1-4> user-vlanid [<0-4085>|null] user-cos [<0-7>|null] [add|translation|transparent] tpid <tpid> cos [<cos>|null] vlanid [<vlanid>|null]}*4
```

Planning Data

Procedure	Parameter	Description	Attribute	Example	
Creating a QinQ domain	<name>	The name of the QinQ domain.	Mandatory	qinqdomain	
Configuring the quantity of services in the QinQ domain	service-count <service-count>	The service quantity. The value ranges from 1 to 8. You should configure one service at least, and eight services at most.	Mandatory	2	
Configuring uplink rules for the OLT QinQ domain	service <1-8>	The service index. The quantity of services should be same as that of uplink rule clauses. The value ranges from 1 to 8.	Mandatory	1	2

Procedure	Parameter	Description	Attribute	Example	
	classification upstream field-id <1-27>	The uplink rule type. Altogether 27 types are provided and the default one is 1. ◆ 1: DA (destination MAC address) ◆ 2: SA (source MAC address) ◆ 3: ethtype (Ethernet type) ◆ 4: vlan4 (Layer 4 VLAN) ◆ 5: vlan3 (Layer 3 VLAN) ◆ 6: vlan2 (Layer 2 VLAN) ◆ 7: vlan1 (Layer 1 VLAN) ◆ 8: TOS (service type) ◆ 10: TTL (Time-to-Live) ◆ 11: protocol type ◆ 12: sip (source IP address) ◆ 14: dip (destination IP address) ◆ 16: L4srcport (Layer 4 source port number) ◆ 17: L4dstport (Layer 4 destination port number) ◆ 18: cos4 (Priority level 4) ◆ 19: cos3 (Priority level 3) ◆ 20: cos2 (Priority level 2) ◆ 21: cos2 (Priority level 1) ◆ 22: based on the destination IPv6 address prefix classification (DA IPv6 Prefix) ◆ 23: based on the source IPv6 address prefix classification (SA IPv6 Prefix) ◆ 24: based on the IP version (v4 or v6) classification (IP version) ◆ 25: based on the IP priority field (IPv6) classification (IPv6 Traffic Class) ◆ 26: based on the IP flow label field (IPv6 Flow Label) ◆ 27: based on next packet header (IPv6 Next Header)	Mandatory	1	1
	value <value>	The domain value corresponding to the uplink rule. Enter the value according to the domain type.	Mandatory	00000-00000-00	00000-00000-00

Procedure	Parameter	Description	Attribute	Example	
	`condition <condition>`	The uplink operator. The value ranges from 0 to 7, and the default value is 5. ◆ 0: Never (never match) ◆ 1: = (equal to) ◆ 2: != (not equal to) ◆ 3: <= (smaller than or equal to) ◆ 4: >= (larger than or equal to) ◆ 5: Exist (exist means match) ◆ 6: No exist (not exist means match) ◆ 7: Always (always match)	Mandatory	5	5
	`{serv-id <1-8>}*1`	The service ID. If no ID is entered, the service index will be used as the service ID.	Optional	1	2
Configuring downlink rules for the OLT QinQ domain	`service <1-8>`	The service index. The quantity of services should be same as that of downlink rule clauses. The value ranges from 1 to 8.	Mandatory	1	2

Procedure	Parameter	Description	Attribute	Example	
	classification downstream field-id <1-27>	The downlink rule type. Altogether 27 types are provided and the default one is 1. ◆ 1: DA (destination MAC address) ◆ 2: SA (source MAC address) ◆ 3: ethtype (Ethernet type) ◆ 4: vlan4 (Layer 4 VLAN) ◆ 5: vlan3 (Layer 3 VLAN) ◆ 6: vlan2 (Layer 2 VLAN) ◆ 7: vlan1 (Layer 1 VLAN) ◆ 8: TOS (service type) ◆ 10: TTL (Time-to-Live) ◆ 11: protocol type ◆ 12: sip (source IP address) ◆ 14: dip (destination IP address) ◆ 16: L4srcport (Layer 4 source port number) ◆ 17: L4dstport (Layer 4 destination port number) ◆ 18: cos4 (Priority level 4) ◆ 19: cos3 (Priority level 3) ◆ 20: cos2 (Priority level 2) ◆ 21: cos2 (Priority level 1) ◆ 22: based on the destination IPv6 address prefix classification (DA IPv6 Prefix) ◆ 23: based on the source IPv6 address prefix classification (SA IPv6 Prefix) ◆ 24: based on the IP version (v4 or v6) classification (IP version) ◆ 25: based on the IP priority field (IPv6) classification (IPv6 Traffic Class) ◆ 26: based on the IP flow label field (IPv6 Flow Label) ◆ 27: based on next packet header (IPv6 Next Header)	Mandatory	1	1
	value <value>	The value of the selected downlink domain. Enter the value according to the domain type.	Mandatory	00000-00000-00	00000-00000-00

Procedure	Parameter	Description	Attribute	Example	
	condition <condition>	The downlink operator. The value ranges from 0 to 7, and the default value is 5. ◆ 0: Never (never match) ◆ 1: = (equal to) ◆ 2: != (not equal to) ◆ 3: <= (smaller than or equal to) ◆ 4: >= (larger than or equal to) ◆ 5: exist (exist means match) ◆ 6: no exist (not exist means match) ◆ 7: always (always match)	Mandatory	5	5
Configuring the service VLAN for the QinQ domain	vlan <1-4>	The VLAN layer No., i.e., the number of the current VLAN layer. Services can be configured on up to four VLAN layers. The value ranges from 1 to 4.	Mandatory	1	2
	user-vlanid [<0-4085>| null]	The original VLAN ID	Mandatory	100 200	null
	user-cos [<0-7>|null]	The CoS value. null: no configuration. The value ranges from 0 to 7, and the default value is 0.	Mandatory	0	null
	[add| translation| transparent]	Action of the VLAN at the selected layer ◆ add: adding ◆ translation: translation ◆ transparent: transparent transmission	Mandatory	transla-tion	add
	tpid <tpid>	The TPID, i.e, the tag protocol identifier. The value ranges from 1 to 0xfffe.	Mandatory	33024	33024
	cos [<cos>| null]	The CoS value. null: no configuration. The value ranges from 0 to 7, and the default value is 0.	Mandatory	null	null
	vlanid [<vlanid>| null]	The new VLAN ID. null: no configuration. The value ranges from 1 to 4085.	Mandatory	1000	600

Example

1. Create a QinQ domain named "qinqdomain".

```
Admin(config)#oltqinq-domain add qinqdomain
Admin(config)#
```

2. Set the service quantity to 2 for the QinQ domain named "qinqdomain".

```
Admin(config)#oltqinq-domain modify qinqdomain service-count 2
```

3. Configure the uplink rule for the OLT QinQ domain "qinqdomain". Configure the first service, setting the uplink rule type to 1, the selected uplink domain value to the MAC address 000000000000, the uplink operator to 5, and the service ID to 1.

```
Admin(config)#oltqinq-domain qinqdomain service 1 classification upstream field-id 1 value 000000000000 condition 5 serv-id 1
```

4. Configure the downlink rule for the OLT QinQ domain "qinqdomain". Configure the first service, setting the downink rule type to 1, the selected downlink domain value to the MAC address 000000000000, and the downlink operator to 5.

```
Admin(config)#oltqinq-domain qinqdomain service 1 classification downstream field-id 1 value 000000000000 condition 5
```

5. Configure the service VLAN for the QinQ domain. Configure the first service as follows. Set the original VLAN ID of the first layer VLAN to "100", CoS value to "0", VLAN mode to "translation", TPID to "33024", and CoS value to "null". Set the new VLAN ID to "1000", the second layer VLAN action to "add", the VLAN ID value to "600", the TPID to "33024", and the CoS value to "null".

```
Admin(config)#oltqinq-domain qinqdomain service 1 vlan 1 user-vlanid 100 user-cos 0 translation tpid 33024 cos null vlanid 1000 vlan 2 user-vlanid null user-cos null add tpid 33024 cos null vlanid 600
Admin(config)#
```

6. Configure the uplink rule for the OLT QinQ domain "qinqdomain". Configure the second service, setting the uplink rule type to 1, the selected uplink domain value to the MAC address 000000000000, the uplink operator to 5, and the service ID to 2.

```
Admin(config)#oltqinq-domain qinqdomain service 2 classification upstream field-id 1 value 000000000000 condition 5 serv-id 2
```

7. Configure the downlink rule for the OLT QinQ domain "qinqdomain". Configure the second service, setting the downink rule type to 1, the selected downlink domain value to the MAC address 000000000000, and the downlink operator to 5.

```
Admin(config)#oltqinq-domain qinqdomain service 2 classification downstream field-id 1 value 000000000000 condition 5
```

8. Configure the service VLAN for the QinQ domain. Configure the second service as follows. Set the original VLAN ID of the first layer VLAN to "200", CoS value to "0", VLAN mode to "translation", TPID to "33024", and CoS value to "null". Set the new VLAN ID to "1000", the second layer VLAN action to "add", the VLAN ID value to "600", the TPID to "33024", and the CoS value to "null".

```
Admin(config)#oltqinq-domain qinqdomain service 2 vlan 1 user-vlanid 200 user-cos 0 translation tpid 33024 cos null vlanid 1000 vlan 2 user-vlanid null user-cos null add tpid 33024 cos null vlanid 600
Admin(config)#
```

9.2.3 Binding the QinQ Domain to a PON Port

Command Format

```
oltqinq-domain <name>
```

Planning Data

Parameter	Description	Attribute	Example
<name>	Name of the QinQ domain	Mandatory	qinqdomain

Example

Bind the domain "qinqdomain" to PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/1)#oltqinq-domain qinqdomain
Admin(config-if-pon-1/1/1)#
```

9.2.4 Configuring Parameters of Data Services at the ONU Ports

Command Format

Configure the quantity of services at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service count <service-count>
```

Configure the type of service at the ONU port.

`onu port vlan <onulist> eth <onu-port> service <serviceid> type [multicast|unicast]`

Note:

The service type is unicast by default. Configure it to multicast service if it is required.

Configure the VLAN mode for the service at the ONU port.

`onu port vlan <onulist> eth <onu-port> service <serviceid> [tag|transparent] priority <priority> tpid <tpid> vid <vlanlist>`

Planning Data

Procedure	Parameter	Description	Attribute	Example	
Configuring quantity of services at the ONU port	`<onulist>`	The ONU authorization No.	Mandatory	1	1
	`eth <onu-port>`	The ONU port No.	Mandatory	1	2
	`service count <service-count>`	The quantity of services	Mandatory	1	1
Configuring VLAN mode for the service at the ONU port	`service <serviceid>`	The service ID, ranging from 1 to 10	Mandatory	1	1
	`[tag| transparent]`	The service VLAN mode ◆ tag: the TAG identifier ◆ transparent: transparent transmission	Mandatory	transparent	transparent
	`priority <priority>`	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	Mandatory	7	7
	`tpid <tpid>`	The TPID, i.e, the tag protocol identifier. The value ranges from 0 to 65534, and the default value is 33024.	Mandatory	33024	33024
	`vid <vlanlist>`	The CVLAN ID, ranging from 1 to 4085	Mandatory	100	200

Example

1. Configure the ONU with the authorization number 1 under PON Port 1 in Slot 1 of Subrack 1, adding a service to Port 1 of the ONU.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service count 1
Admin(config-if-pon-1/1/1)#
```

2. Configure the ONU with the authorization number 1 under PON Port 1 in Slot 1 of Subrack 1, adding a service to Port 2 of the ONU.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 2 service count 1
Admin(config-if-pon-1/1/1)#
```

3. Configure the VLAN mode for Port 1 of ONU 1, setting the service ID to 1, service VLAN mode to transparent transmission, priority level to 7, tag protocol identifier to 33024, and VLAN ID to 100.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 transparent priority 7 tpid
33024 vid 100
Admin(config-if-pon-1/1/1)#
```

4. Configure the VLAN mode for Port 1 of ONU 2, setting the service ID to 1, service VLAN mode to transparent transmission, priority level to 7, tag protocol identifier to 33024, and VLAN ID to 200.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 2 service 1 transparent priority 7 tpid
33024 vid 200
Admin(config-if-pon-1/1/1)#
```

9.3 Example for Data Service Configuration in the TAG Mode

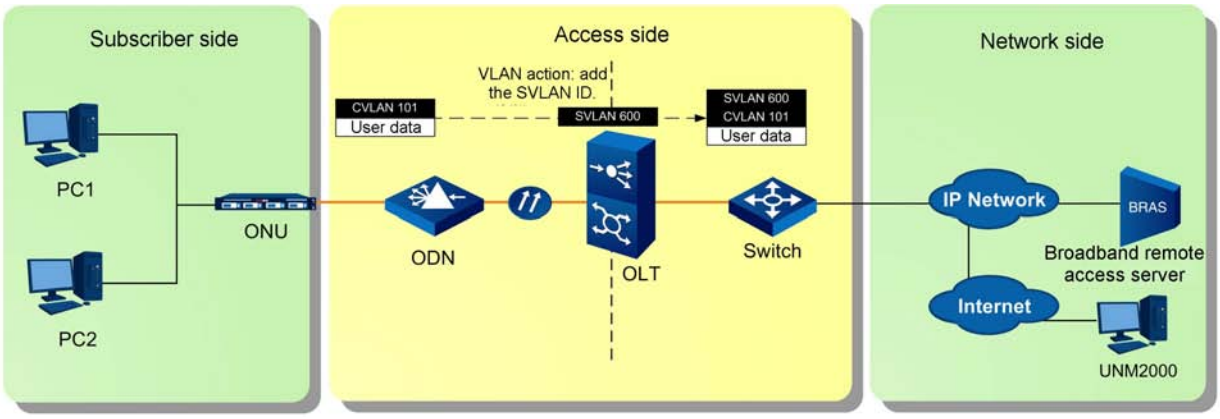
9.3.1 Network Scenario

Service Planning

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

Network Diagram

The network diagram for the data service in the TAG mode is shown in the figure below.



9.3.2 Configuring the OLT QinQ Domain

Command Format

Create a QinQ domain.

```
oltqinq-domain add <name>
```

Configure the quantity of services in the QinQ domain.

```
oltqinq-domain modify <name> service-count <service-count>
```

Configure uplink rules for the OLT QinQ domain.

```
oltqinq-domain <name> service <1-8> classification upstream {field-id <1-27> value <value> condition <condition>}*4 {serv-id <1-8>}*1
```

Configure downlink rules for the OLT QinQ domain.

```
oltqinq-domain <name> service <1-8> classification downstream {field-id <1-27> value <value> condition <condition>}*4
```

Configure the service VLAN for the QinQ domain.

```
oltqinq-domain <name> service <1-8> {vlan <1-4> user-vlanid [<0-4085>|null] user-cos [<0-7>|null] [add|translation|transparent] tpid <tpid> cos [<cos>|null] vlanid [<vlanid>|null]}*4
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Creating a QinQ domain	`<name>`	The name of the QinQ domain.	Mandatory	qinqdomain
Configuring the quantity of services in the QinQ domain	`service-count <service-count>`	The service quantity. The value ranges from 1 to 8. You should configure one service at least, and eight services at most.	Mandatory	1
Configuring uplink rules for the OLT QinQ domain	`service <1-8>`	The service index. The quantity of services should be same as that of uplink rule clauses. The value ranges from 1 to 8.	Mandatory	1

Procedure	Parameter	Description	Attribute	Example
	classification upstream field-id <1-27>	The uplink rule type. Altogether 27 types are provided and the default one is 1. ◆ 1: DA (destination MAC address) ◆ 2: SA (source MAC address) ◆ 3: ethtype (Ethernet type) ◆ 4: vlan4 (Layer 4 VLAN) ◆ 5: vlan3 (Layer 3 VLAN) ◆ 6: vlan2 (Layer 2 VLAN) ◆ 7: vlan1 (Layer 1 VLAN) ◆ 8: TOS (service type) ◆ 10: TTL (Time-to-Live) ◆ 11: protocol type ◆ 12: sip (source IP address) ◆ 14: dip (destination IP address) ◆ 16: L4srcport (Layer 4 source port number) ◆ 17: L4dstport (Layer 4 destination port number) ◆ 18: cos4 (Priority level 4) ◆ 19: cos3 (Priority level 3) ◆ 20: cos2 (Priority level 2) ◆ 21: cos2 (Priority level 1) ◆ 22: based on the destination IPv6 address prefix classification (DA IPv6 Prefix) ◆ 23: based on the source IPv6 address prefix classification (SA IPv6 Prefix) ◆ 24: based on the IP version (v4 or v6) classification (IP version) ◆ 25: based on the IP priority field (IPv6) classification (IPv6 Traffic Class) ◆ 26: based on the IP flow label field (IPv6 Flow Label) ◆ 27: based on next packet header (IPv6 Next Header)	Mandatory	1
	value <value>	The domain value corresponding to the uplink rule. Enter the value according to the domain type.	Mandatory	000000000000

Procedure	Parameter	Description	Attribute	Example
	`condition <condition>`	The uplink operator. The value ranges from 0 to 7, and the default value is 5. ◆ 0: Never (never match) ◆ 1: = (equal to) ◆ 2: != (not equal to) ◆ 3: <= (smaller than or equal to) ◆ 4: >= (larger than or equal to) ◆ 5: Exist (exist means match). ◆ 6: No exist (not exist means match). ◆ 7: Always (always match).	Mandatory	5
	`{serv-id <1-8>}*1`	The service ID. If no ID is entered, the service index will be used as the service ID.	Optional	1
Configuring downlink rules for the OLT QinQ domain	`service <1-8>`	The service index. The quantity of services should be same as that of downlink rule clauses. The value ranges from 1 to 8.	Mandatory	1

Procedure	Parameter	Description	Attribute	Example
	classification downstream field-id <1-27>	The downlink rule type. Altogether 27 types are provided and the default one is 1. ◆ 1: DA (destination MAC address) ◆ 2: SA (source MAC address) ◆ 3: ethtype (Ethernet type) ◆ 4: vlan4 (Layer 4 VLAN) ◆ 5: vlan3 (Layer 3 VLAN) ◆ 6: vlan2 (Layer 2 VLAN) ◆ 7: vlan1 (Layer 1 VLAN) ◆ 8: TOS (service type) ◆ 10: TTL (Time-to-Live) ◆ 11: protocol type ◆ 12: sip (source IP address) ◆ 14: dip (destination IP address) ◆ 16: L4srcport (Layer 4 source port number) ◆ 17: L4dstport (Layer 4 destination port number) ◆ 18: cos4 (Priority level 4) ◆ 19: cos3 (Priority level 3) ◆ 20: cos2 (Priority level 2) ◆ 21: cos2 (Priority level 1) ◆ 22: based on the destination IPv6 address prefix classification (DA IPv6 Prefix) ◆ 23: based on the source IPv6 address prefix classification (SA IPv6 Prefix) ◆ 24: based on the IP version (v4 or v6) classification (IP version) ◆ 25: based on the IP priority field (IPv6) classification (IPv6 Traffic Class) ◆ 26: based on the IP flow label field (IPv6 Flow Label) ◆ 27: based on next packet header (IPv6 Next Header)	Mandatory	1
	value <value>	The value of the selected downlink domain. Enter the value according to the domain type.	Mandatory	000000000000

Procedure	Parameter	Description	Attribute	Example	
	condition <condition>	The downlink operator. The value ranges from 0 to 7, and the default value is 5. ◆ 0: Never (never match) ◆ 1: = (equal to) ◆ 2: != (not equal to) ◆ 3: <= (smaller than or equal to) ◆ 4: >= (larger than or equal to) ◆ 5: exist (exist means match) ◆ 6: no exist (not exist means match) ◆ 7: always (always match)	Mandatory	5	
Configuring the service VLAN for the QinQ domain	vlan <1-4>	The VLAN layer No., i.e., the number of the current VLAN layer. Services can be configured on up to four VLAN layers. The value ranges from 1 to 4.	Mandatory	1	2
	user-vlanid [<0-4085>| null]	The original VLAN ID	Mandatory	101	null
	user-cos [<0-7>|null]	The CoS value. null: no configuration. The value ranges from 0 to 7, and the default value is 0.	Mandatory	0	null
	[add| translation| transparent]	Action of the VLAN at the selected layer ◆ add: adding ◆ translation: translation ◆ transparent: transparent transmission	Mandatory	trans-parent	add
	tpid <tpid>	The TPID, i.e, the tag protocol identifier. The value ranges from 1 to 0xfffe.	Mandatory	33024	33024
	cos [<cos>| null]	The CoS value. null: no configuration. The value ranges from 0 to 7, and the default value is 0.	Mandatory	null	null
	vlanid [<vlanid>| null]	The new VLAN ID. null: no configuration. The value ranges from 1 to 4085.	Mandatory	null	600

Example

1. Create a QinQ domain named "qinqdomain".

```
Admin(config)#oltqinq-domain add qinqdomain
```

2. Set the service quantity to 1 for the QinQ domain named "qinqdomain".

```
Admin(config)#oltqinq-domain modify qinqdomain service-count 1
```

3. Configure the uplink rule for the OLT QinQ domain "qinqdomain". Configure the first service, setting the uplink rule type to 1, the selected uplink domain value to the MAC address 000000000000, the uplink operator to 5, and the service ID to 1.

```
Admin(config)#oltqinq-domain qinqdomain service 1 classification upstream field-id 1 value 000000000000 condition 5 serv-id 1
```

4. Configure the downlink rule for the OLT QinQ domain "qinqdomain". Configure the first service, setting the downink rule type to 1, the selected downlink domain value to the MAC address 000000000000, and the downlink operator to 5.

```
Admin(config)#oltqinq-domain qinqdomain service 1 classification downstream field-id 1 value 000000000000 condition 5
```

5. Configure the service VLAN for the QinQ domain. Configure the first service as follows. Set the original VLAN ID of the first layer VLAN to 101, the CoS value to 0, the VLAN mode to "transparent", the TPID to 33024, and the CoS to "null". Set the new VLAN ID to "null", the second layer VLAN action to "add", the VLAN ID to "600", the TPID to "33024", and the CoS value to "null".

```
Admin(config)#oltqinq-domain qinqdomain service 1 vlan 1 user-vlanid 101 user-cos 0 transparent tpid 33024 cos null vlanid null vlan 2 user-vlanid null user-cos null add tpid 33024 cos null vlanid 600
Admin(config)#
```

9.3.3 Binding the QinQ Domain to an ONU

Command Format

```
onu oltqinq-domain <onuid> <name>
```

Planning Data

Parameter	Description	Attribute	Example
<onuid>	ONU authorization No.	Mandatory	1
<name>	Name of the QinQ domain	Mandatory	qinqdomain

Example

Bind the domain "qinqdomain" to ONU 1 under PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/1)#onu oltqinq-domain 1 qinqdomain
Admin(config-if-pon-1/1/1)#
```

9.3.4 Configuring Parameters of Data Services at the ONU Ports

Command Format

Configure the quantity of services at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service count <service-count>
```

Configure the type of service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> type [multicast|
unicast]
```

Note:

The service type is unicast by default. Configure it to multicast service if it is required.

Configure the VLAN mode for the service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> [tag|transparent]
priority <priority> tpid <tpid> vid <vlanlist>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring quantity of services at the ONU port	<onulist>	The ONU authorization No.	Mandatory	1
	eth <onu-port>	The ONU port No.	Mandatory	1
	service count <service-count>	The quantity of services	Mandatory	1

Procedure	Parameter	Description	Attribute	Example
Configuring VLAN mode for the service at the ONU port	service <serviceid>	The service ID, ranging from 1 to 10	Mandatory	1
	[tag| transparent]	The service VLAN mode ◆ tag: the TAG identifier ◆ transparent: transparent transmission	Mandatory	tag
	priority <priority>	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	Mandatory	7
	tpid <tpid>	The TPID, i.e, the tag protocol identifier. The value ranges from 0 to 65534, and the default value is 33024.	Mandatory	33024
	vid <vlanlist>	The CVLAN ID, ranging from 1 to 4085	Mandatory	101

Example

1. Configure the ONU with the authorization number 1 under PON Port 1 in Slot 1 of Subrack 1, adding a service to Port 1 of the ONU.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service count 1
Admin(config-if-pon-1/1/1)#
```

2. Configure the VLAN mode for Port 1 of ONU 1, setting the service ID to 1, the service VLAN mode to "tag", the priority level to 7, the tag protocol identifier to 33024, and the VLAN ID to 101.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 tag priority 7 tpid 33024
vid 101
Admin(config-if-pon-1/1/1)#
```

10 Configuring the Multicast Service

- Background Information
- Configuration Rules
- Multicast Service Configuration Examples
- Example of Configuring the SSM Multicast Service
- Optional Functions

10.1 Background Information

Multicast is a communication mode in which one copy of data packet is sent to multiple subscribers. Each multicast address stands for a multicast group, and all hosts in the multicast group can receive the same data from the multicast source.

Advantages of multicast service application:

- Saving bandwidth: There is only one copy of the same multicast data stream on each link. This can save the network bandwidth.
- Lessening the load: In the multicast mode, increase of subscribers does not visibly increase the burden on the network. This helps avoid heavy load on the video server and the CPU.
- Long-haul transmission: The multicast packets can be transmitted across network segments to allow long-haul transmission of massive data.
- Security: The multicast packets are transmitted only to the expected receivers, so as to guarantee the security of information.

10.2 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 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.
- The multicast SSM IP address is the multicast address, while the source IP address of SSM-Mapping is the unicast address.

10.3 Multicast Service Configuration Examples

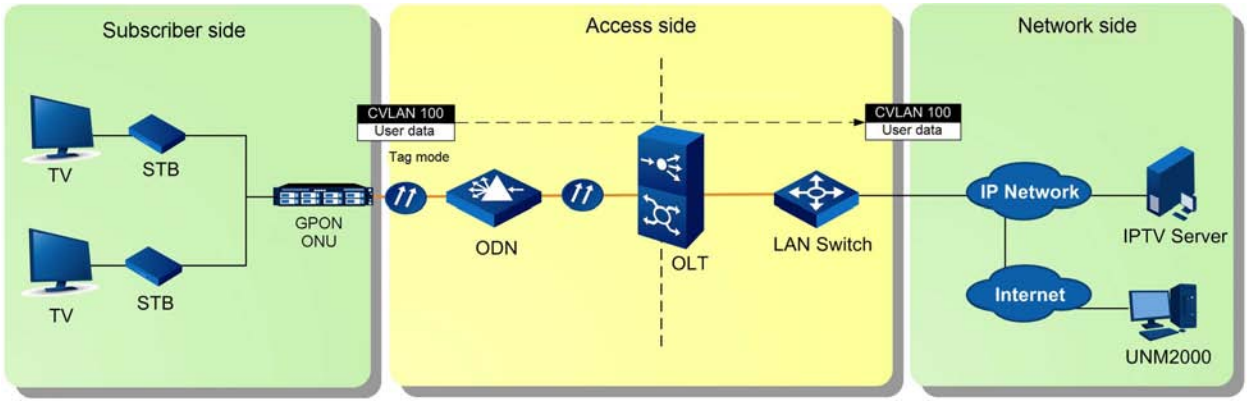
10.3.1 Network Scenario

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 OLT should work in the proxy-snooping mode.

Network Diagram

The figure below shows the network diagram for the multicast services implemented by the OLT in the proxy-snooping mode.



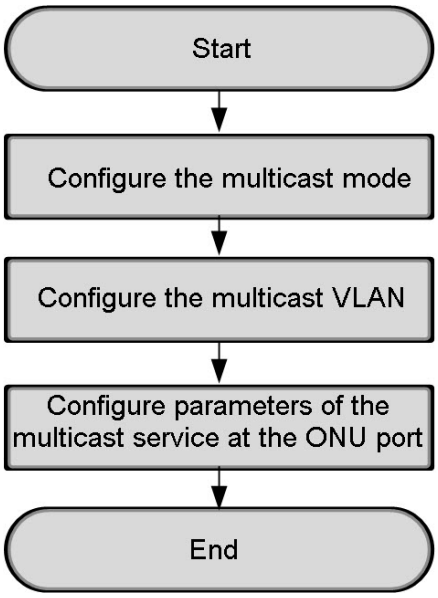
- In the downlink direction, the ONU strips the tag from the multicast stream (VLAN ID=100) on the OLT side, and transmits the stream to the set top box. The set top box then forwards the stream to video subscribers.
- In the uplink direction, the ONU attaches the tag (VLAN ID=100) to the multicast protocol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

10.3.2 Configuration Flow

Prerequisites

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

Configuration Flow



10.3.3 Configuring the Multicast Mode

Command Format

```
igmp mode [control|proxy-proxy|snooping|proxy-snooping|disable]
```

Data Planning

Parameter	Description	Attribute	Example
`igmp mode [control|proxy-proxy|snooping|proxy-snooping|disable]`	The multicast mode. ◆ control: controlled mode ◆ proxy-proxy: proxy-proxy mode ◆ snooping: snooping mode ◆ proxy-snooping: proxy-snooping mode ◆ disable: disabled mode	Mandatory	proxy-snooping

Example

Set the multicast mode to proxy-snooping mode.

```
Admin(config-igmp)#igmp mode proxy-snooping
Admin(config-igmp)#
```

10.3.4 Configuring the Multicast VLAN

Command Format

```
igmp vlan {[default]}*1 {<value>}*1
```

Planning Data

Parameter	Description	Attribute	Example
igmp vlan {[default]}*1	The default multicast VLAN	Optional	-
{<value>}*1	The multicast VLAN, ranging from 1 to 4085	Optional	100

Example

Set the multicast VLAN to 100.

```
Admin(config-igmp)#igmp vlan 100
Admin(config-igmp)#
```

10.3.5 Configuring Parameters of Multicast Service at the ONU Port

Command Format

Configure the quantity of services at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service count <service-count>
```

Configure the type of service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> type [multicast|
unicast]
```

Note:

The service type is unicast by default. Configure it to multicast service if it is required.

Configure the VLAN mode for the service at the ONU port.

`onu port vlan <onulist> eth <onu-port> service <serviceid> [tag|transparent] priority <priority> tpid <tpid> vid <vlanlist>`

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring quantity of services at the ONU port	`<onulist>`	The ONU authorization No.	Mandatory	1
	`eth <onu-port>`	The ONU port No.	Mandatory	1
	`service count <service-count>`	The auantity of services	Mandatory	1
Configuring services at the ONU port	`service <serviceid>`	The service ID, ranging from 1 to 10	Mandatory	1
	`type [multicast| unicast]`	The type of service at the ONU port ◆ multicast: multicast service ◆ unicast: unicast service	Mandatory	multicast
Configuring VLAN mode for the service at the ONU port	`service <serviceid>`	The service ID, ranging from 1 to 10	Mandatory	1
	`[tag| transparent]`	The service VLAN mode ◆ tag: the TAG identifier ◆ transparent: transparent transmission	Mandatory	tag
	`priority <priority>`	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	Mandatory	0
	`tpid <tpid>`	The TPID, i.e, the tag protocol identifier. The value ranges from 0 to 65534, and the default value is 33024.	Mandatory	33024
	`vid <vlanlist>`	The CVLAN ID, ranging from 1 to 4085	Mandatory	100

Example

1. Configure the ONU with the authorization number 1 under PON Port 1 in Slot 1 of Subrack 1, adding a service to Port 1 of the ONU.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service count 1
Admin(config-if-pon-1/1/1)#
```

2. Set the type of Service 1 at Port 1 of ONU 1 to "multicast". The ONU is connected to PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 type multicast
```

3. Configure the VLAN mode for Port 1 of ONU 1, setting the service ID to 1, the service VLAN mode to "tag", the priority level to 0, the tag protocol identifier to 33024, and the VLAN ID to 100.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 tag priority 0 tpid 33024
vid 100
Admin(config-if-pon-1/1/1)#
```

10.4 Example of Configuring the SSM Multicast Service

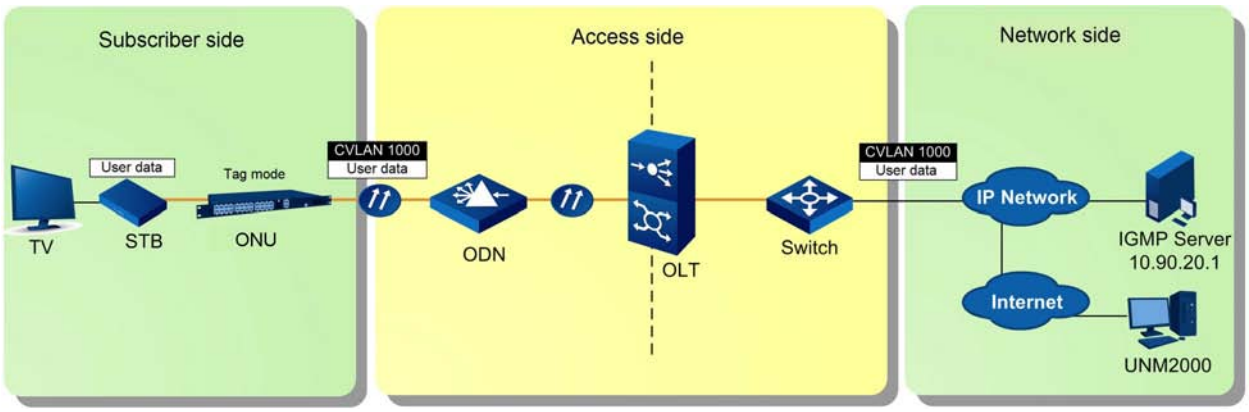
10.4.1 Network Scenario

Service Planning

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

Network Diagram

The network diagram for the SSM multicast service is shown in the figure below.



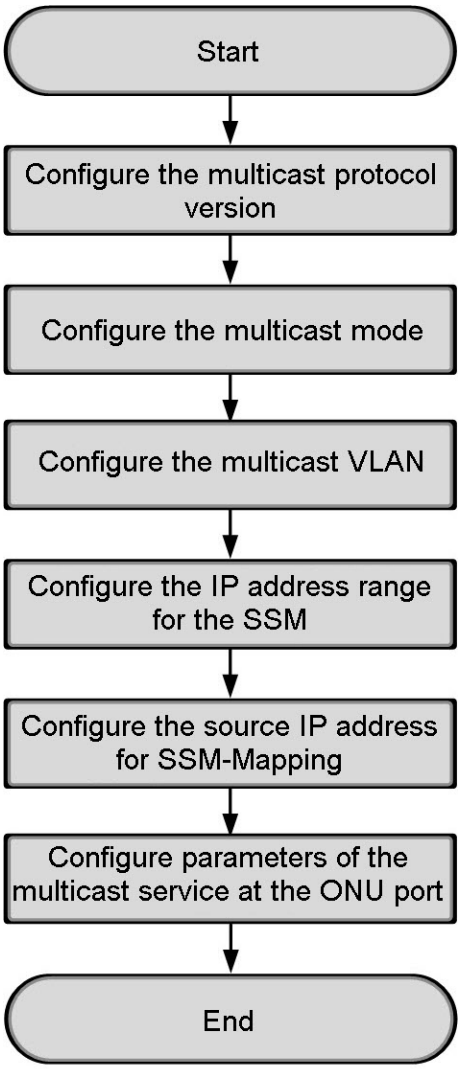
- In the downlink direction, the multicast SPT (Shortest Path Tree) is set up between the multicast source and the OLT equipment. The multicast source 10.90.20.1 provides the SSM service for the subscriber connected to the OLT. The ONU strips the VLAN tag from the multicast packets and then forwards the packets to the set top box on the subscriber side.
- In the uplink direction, the ONU adds the tag to the multicast protocol packets requesting joining / leaving a multicast group received from the set top box, and sends the packets to the OLT equipment. The OLT then forwards the protocol packets to the IPTV server.

10.4.2 Configuration Flow

Prerequisites

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

Configuration Flow



10.4.3 Configuring the Multicast Protocol Version

Command Format

```
igmp version [v1|v2|v3]
```

Planning Data

Parameter	Description	Attribute	Example
`igmp version [v1|v2|v3]`	The multicast protocol version ◆ v1: IGMP Version 1 ◆ v2: IGMP Version 2 ◆ v3: IGMP Version 3	Mandatory	v3

Example

Set the multicast protocol version to IGMP Version 3.

```
Admin(config-igmp)#igmp version v3
Admin(config-igmp)#
```

10.4.4 Configuring the Multicast Mode

Command Format

```
igmp mode [control|proxy-proxy|snooping|proxy-snooping|disable]
```

Data Planning

Parameter	Description	Attribute	Example
`igmp mode [control|proxy-proxy|snooping|proxy-snooping|disable]`	The multicast mode. ◆ control: controlled mode ◆ proxy-proxy: proxy-proxy mode ◆ snooping: snooping mode ◆ proxy-snooping: proxy-snooping mode ◆ disable: disabled mode	Mandatory	proxy-proxy

Example

Set the multicast mode to the proxy mode.

```
Admin(config-igmp)#igmp mode proxy-proxy
Admin(config-igmp)#
```

10.4.5 Configuring the Multicast VLAN

Command Format

```
igmp vlan {[default]}*1 {<value>}*1
```

Planning Data

Parameter	Description	Attribute	Example
`igmp vlan {[default]}*1`	The default multicast VLAN	Optional	-
`{<value>}*1`	The multicast VLAN, ranging from 1 to 4085	Optional	1000

Example

Set the multicast VLAN to 1000.

```
Admin(config-igmp)#igmp vlan 1000
Admin(config-igmp)#
```

10.4.6 Configuring the Multicast SSM IP Address Range

Command Format

```
igmp-ssm ip-range <ipaddr/m>
```

Planning Data

Parameter	Description	Attribute	Example
`igmp-ssm ip-range <ipaddr/m>`	The SSM IP address range, i.e., the multicast addresses.	Mandatory	239.0.0.0/16

Example

Set the multicast SSM IP address range to 239.0.0.0/16.

```
Admin(config-igmp)#igmp-ssm ip-range 239.0.0.0/16
Admin(config-igmp)#
```

10.4.7 Configuring the Source IP Address of Multicast SSM-Mapping

Command Format

```
igmp ssm-map <ipaddr>
```

Planning Data

Parameter	Description	Attribute	Example
`ssm-map <ipaddr>`	The SSM-Mapping source IP address, i.e., the unicast address	Mandatory	10.90.20.1

Example

Set the source IP address of multicast SSM-Mapping to 10.90.20.1.

```
Admin(config-igmp)#igmp ssm-map 10.90.20.1
Admin(config-igmp)#
```

10.4.8 Configuring Parameters of Multicast Service at the ONU Port

Command Format

Configure the quantity of services at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service count <service-count>
```

Configure the type of service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> type [multicast|
unicast]
```

Note:

The service type is unicast by default. Configure it to multicast service if it is required.

Configure the VLAN mode for the service at the ONU port.

```
onu port vlan <onulist> eth <onu-port> service <serviceid> [tag|transparent]
priority <priority> tpid <tpid> vid <vlanlist>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring quantity of services at the ONU port	<onulist>	The ONU authorization No.	Mandatory	1
	eth <onu-port>	The ONU port No.	Mandatory	1
	service count <service-count>	The quantity of services	Mandatory	1
Configuring services at the ONU port	service <serviceid>	The service ID, ranging from 1 to 10	Mandatory	1

Procedure	Parameter	Description	Attribute	Example
	type [multicast| unicast]	Type of service at the ONU port ◆ multicast: multicast service ◆ unicast: unicast service	Mandatory	multicast
Configuring VLAN mode for the service at the ONU port	service <serviceid>	The service ID, ranging from 1 to 10	Mandatory	1
	[tag| transparent]	The service VLAN mode ◆ tag: the TAG identifier ◆ transparent: transparent transmission	Mandatory	tag
	priority <priority>	The CVLAN priority, ranging from 0 to 7. The value 7 stands for the highest priority level, and 0 the lowest one.	Mandatory	5
	tpid <tpid>	The TPID, i.e, the tag protocol identifier. The value ranges from 0 to 65534, and the default value is 33024.	Mandatory	33024
	vid <vlanlist>	The CVLAN ID, ranging from 1 to 4085	Mandatory	1000

Example

1. Configure the ONU with the authorization number 1 under PON Port 1 in Slot 1 of Subrack 1, adding a service to Port 1 of the ONU.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service count 1
Admin(config-if-pon-1/1/1)#
```

2. Set the type of Service 1 at Port 1 of ONU 1 to "multicast". The ONU is connected to PON Port 1 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 type multicast
```

3. Configure the VLAN mode for Port 1 of ONU 1, setting the service ID to 1, the service VLAN mode to "tag", the priority level to 5, the tag protocol identifier to 33024, and the VLAN ID to 1000.

```
Admin(config-if-pon-1/1/1)#onu port vlan 1 eth 1 service 1 tag priority 5 tpid 33024
vid 1000
Admin(config-if-pon-1/1/1)#
```

10.5 Optional Functions

10.5.1 Configuring the Multicast Cascade Port

Command Format

```
igmp cascade slot <slotno> port <portno>
```

Planning Data

Parameter	Description	Attribute	Example
slot <slotno>	The slot number	Mandatory	19
port <portno>	The number of the uplink port	Mandatory	1

Example

Set the multicast cascade port to Port 1 in Slot 19.

```
Admin(config-igmp)#igmp cascade slot 19 port 1
Admin(config-igmp)#
```

10.5.2 Configuring OLT Multicast Protocol Parameters

Command Format

```
igmp parameters [robustness|old|last-query-interval|last-query-count|
query-interval|query-response-interval] <value>
```

Planning Data

Parameter	Description	Attribute	Example
igmp parameters [robustness|old|last-query-interval|last-query-count|query-interval|query-response-interval]	Configuring multicast protocol parameters ◆ robustness: the robustness parameter ◆ old: the aging time for the group member ◆ last-query-interval: the last query interval ◆ last-query-count: the count of last queries ◆ query-interval: the common query interval ◆ query-response-interval: the common query response time	Mandatory	robustness
<value>	The protocol parameter value ◆ robustness: 2 to 16 ◆ old: 0 / 1 ◆ last-query-interval: 1 to 255 (unit: s) ◆ last-query-count: 1 to 16 ◆ query-interval: 11 to 255 (unit: s) ◆ query-response-interval: 1 to 255 (unit: s)	Mandatory	2

Example

Set the OLT multicast protocol robustness parameter to 2.

```
Admin(config-igmp)#igmp parameters robustness 2
Admin(config-igmp)#
```

10.5.3 Configuring ONU Multicast Parameters

Command Format

```
igmp port <frameid/slotid/portid> <onu> <port> {[control] [enable|disable]}*1 {[bandwidth] <0-100000>}*1 {[leave] [fast|non-fast]}*1 {[max-group] <groupno>}*1 {[signal-vlan] <vlanno>}*1
```

Data Planning

Parameter	Description	Attribute	Example
<frameid/slotid/-portid>	The subrack number / slot number / port number.	Mandatory	1/1/1
<onu>	The ONU authorization number.	Optional	1
<port>	The ONU port number.	Mandatory	1

Parameter	Description	Attribute	Example
{[control] [enable|disable]}*1	The controlled mode. Enable or disable the mode.	Optional	-
{[bandwidth] <0-100000>}*1	The maximum bandwidth. The value ranges from 0 to 100000.	Optional	-
{[leave] [fast|non-fast]}*1	The leaving mode. ◆ fast: leaving fast ◆ non-fast: leaving normally	Optional	non-fast
{[max-group] <groupno>}*1	The maximum number of the groups. The value ranges from 0 to 254.	Optional	31
{[signal-vlan] <vlanno>}*1	The signaling VLAN, ranging from 0 to 4085.	Optional	-

Example

Set the leaving mode to "non-fast" for Port 1 of ONU 1 under PON Port 1 in Slot 1 of Subrack 1, and set the maximum number of online groups to 31.

```
Admin(config-igmp)#igmp port 1/1/1 1 1 leave non-fast max-group 31
Admin(config-igmp)#
```

10.5.4 Configuring the Prejoin Group

Command Format

```
igmp prejoin <groupaddress>
```

Planning Data

Parameter	Description	Attribute	Example
prejoin <groupaddress>	The address of the prejoin group	Mandatory	224.1.1.1

Example

Set the address of the prejoin group to 224.1.1.1.

```
Admin(config-igmp)#igmp prejoin 224.1.1.1
Admin(config-igmp)#
```

11 Configuring 1588v2

- 1588v2 Application Scenarios
- Configuring 1588v2 (Based on G.8275.1)
- Configuring 1588v2 (Based on IEEE)
- 1588v2 (Based on IEEE) Maintenance and Diagnosis

11.1 1588v2 Application Scenarios

Table 11-1 describes 1588v2 application scenarios.

Table 11-1 Common 1588v2 Application Scenarios

Network Scenario	Condition
Network-wide 1588v2 and SyncE deployment	◆ The bearer network devices support 1588v2 for time synchronization. Time signals are injected to a bearer network device. ◆ Devices on the entire network support synchronous Ethernet (SyncE) for clock synchronization.
Network-wide 1588v2 deployment	◆ The bearer network devices support 1588v2 for time synchronization. Time signals are injected to a bearer network device. ◆ All the devices in the network support 1588v2, instead of SyncE, for clock synchronization.
Clock or time signal injection to an OLT	The bearer network devices do not support 1588v2 synchronization. The time or clock signals are injected to an OLT.

11.1.1 Network-wide 1588v2 and SyncE Deployment

Time synchronization must be implemented on wireless Long Term Evolution (LTE) base stations. Time signals are injected to a bearer network device.

When devices on the entire network support synchronous Ethernet (SyncE), SyncE is recommended for clock synchronization and 1588v2 for time synchronization, as shown in Figure 11-1.

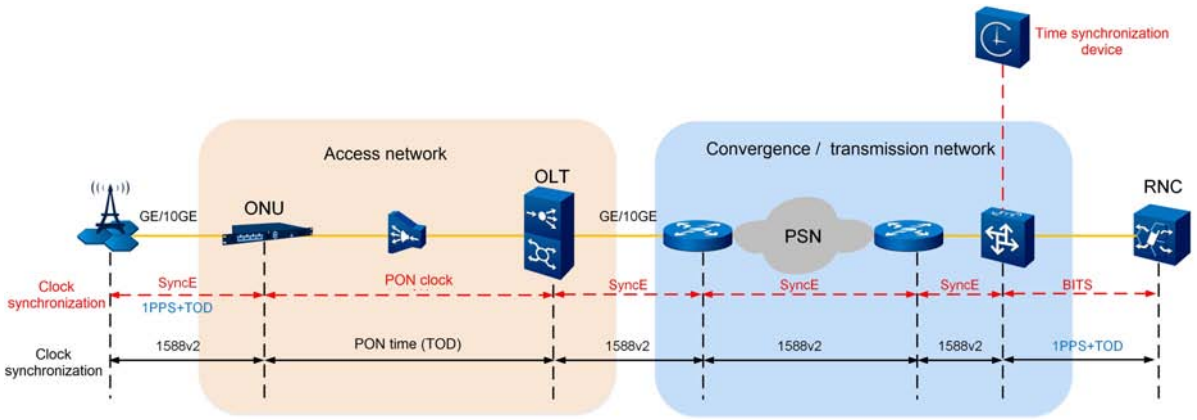


Figure 11-1 Network-wide 1588v2 and SyncE Deployment

SyncE uses Ethernet bitstreams to recover clock signals for Ethernet clock synchronization. The implementation mode is similar to that on an SDH or PDH network.

SyncE uses high-precision clock signals as the transit reference in the transmit direction. It restores and extracts the clock signals at the receive end. The physical layer transmits and receives the clock signals and is compatible with traditional Ethernets.

- Clock synchronization based on SyncE
  - Bear network devices use SyncE to synchronize clock signals between them.
  - An OLT receives SyncE clock signals through a GE or 10GE link connected to a bearer network device. The OLT uses PON lines to transmit the clock signals to an ONU. Then the ONU uses a user-side GE link to transmit the signals to base stations.
  - The base stations use the SyncE clock signals received for clock synchronization.
- Clock synchronization based on 1588v2
  - A bearer network device receives time signals through a 1PPS+TOD port and serves as an Ordinary Clock (OC) device.
  - The bearer network devices use 1588v2 to synchronize time between them.

- The combination of an OLT and an ONU is used as a boundary clock (BC) device. The OLT receives 1588v2 time signals through a GE or 10GE link connected to a bearer network device, and the ONU uses a user-side GE link to transmit the signals to base stations.
- The OLT uses a PON line to transmit time signals to the ONU in ONU management and control interface (OMCI) mode.
- Base stations are used as OC devices:
  - The base stations not supporting 1588v2 synchronization use a 1PPS +TOD port to receive time signals.
  - The base stations supporting 1588v2 synchronization use 1588v2 to synchronize time signals.

11.1.2 Network-wide 1588v2 Deployment

Time synchronization must be implemented on wireless LTE base stations by a bearer network.

As shown in Figure 11-2, when bearer network devices support 1588v2 synchronization, time signals are injected to a bearer network device and be synchronized.

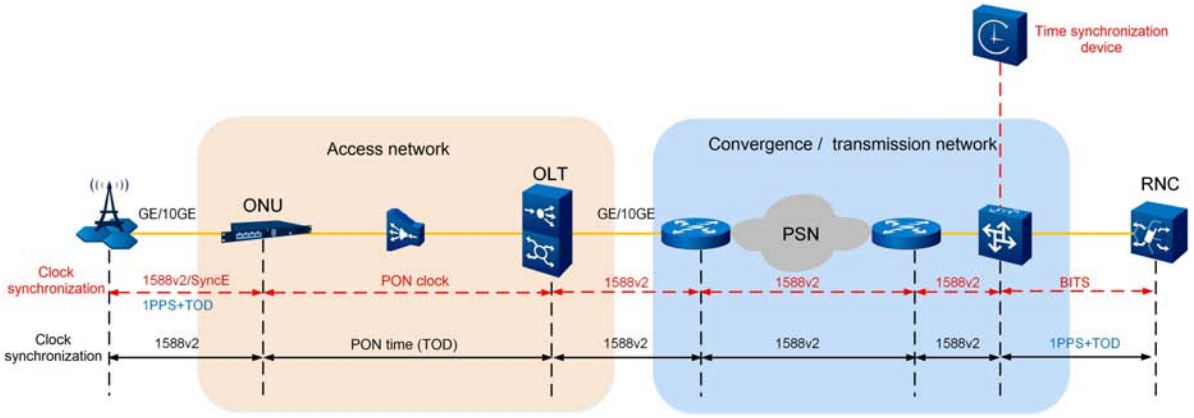


Figure 11-2 Network-wide 1588v2 Deployment

- Bearer network devices are used as Ordinary Clock (OC) devices. A bearer network device receives time signals through a 1PPS+TOD port and uses 1588v2 to synchronize time and clock signals with other bearer network devices.

- The combination of an OLT and an ONU is used as a boundary clock (BC) device. The OLT receives 1588v2 time signals through a GE or 10GE link connected to a bearer network device, and the ONU uses a user-side GE link to transmit the signals to base stations.
- The OLT uses a PON line to transmit the time and clock signals to the ONU in OMCI mode.
- Base stations are used as OC devices:
  - The base stations not supporting 1588v2 synchronization use a 1PPS +TOD port to receive time signals.
  - The base stations supporting 1588v2 synchronization use 1588v2 to synchronize time signals.

11.1.3 Clock or Time Signal Injection to an OLT

Wireless LTE base stations require time synchronization. When devices on a bearer network do not support 1588v2 synchronization, time signals can be injected to an OLT, as shown in Figure 11-3.

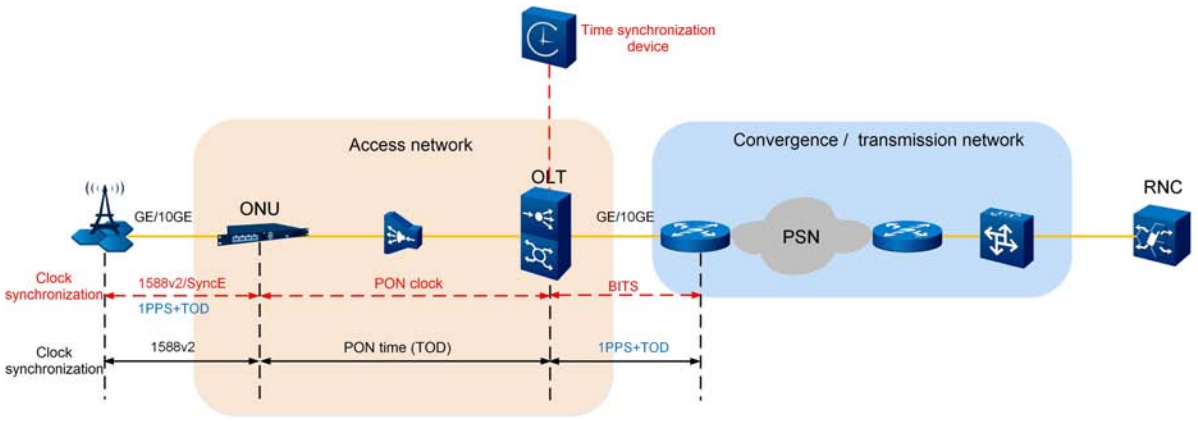


Figure 11-3 Clock or Time Signal Injection to an OLT

- Time signals are injected to an OLT via a 1PPS+TOD port, and BITS clock signals are injected into the OLT via the BITS port.
- The combination of an OLT and an ONU is used as a boundary clock (BC) device. The ONU uses a user-side GE link to transmit the 1588v2 time signals to base stations.

- The OLT uses a PON line to transmit the time and clock signals to the ONU in OMCI mode.
- Base stations are used as OC devices:
  - Base stations not supporting 1588v2 synchronization use a 1PPS+TOD port to receive time signals, and use SyncE to synchronize clock signals.
  - Base stations supporting 1588v2 synchronization use 1588v2 to synchronize time and clock signals.

11.2 Configuring 1588v2 (Based on G.8275.1)

This section introduces how to configure 1588v2 (based on G.8275.1).

11.2.1 Prerequisite

- Time synchronization can be performed only after the clock has been synchronized. For example, clock signals have been synchronized based on SyncE.
- 1588v2 based on G.8275.1 cannot be used together with 1588v2 based on IEEE.

11.2.2 Procedure

1. Set the device type to G.8275.1 T-BC. By default, the BC mode is used, that is, the device complies with IEEE 1588v2 by default and implements 1588v2 based on the default profile. In this case, you need to manually switch the mode to T-BC to implement 1588v2 based on ITU-T G.8275.1.

```
Admin(config)#ptp profile g.8275.1
```

2. Configure the global precision time protocol (PTP) function.

```
Admin(config-g8275-1)#ptp enable
```

3. Specify a time domain for the device. After the configuration, a time domain has a clock source. All the devices in the time domain use the clock source.

```
Admin(config)#ptp domain-number <value>
```

4. Configure a virtual clock ID for the device. The clock ID uniquely identifies a clock node in a time domain. The default value is 00000000-00001234.

```
Admin(config)#ptp local clock-id <value>
```

5. Enable PTP for an Ethernet port. 1588v2 needs to be enabled for Ethernet ports transmitting 1588v2 packets, such as uplink ports of an OLT and user-side ports of an MDU.

```
Admin(config)#ptp port <frameid/slotid/portid> enable
```

6. Set the port to slave state. Then, the time source of the upper-layer device can be traced through this port.

```
Admin(config)#ptp port <frameid/slotid/portid> master-only false
```

7. Enable the 1588 function for GPON ports between the OLT and the MDU.

```
Admin(config)#1588-enable switch enable
```

8. Configure the T-BC time source. The time source can be the T-BC time or BOD time recovered from the network-side GE / 10GE / PON line. If the network does not support T-BC time synchronization, the TOD time can be used.

```
Admin(config)#ptp source <frameid/slotid/portid>
```

9. When the TOD time is used, configure the attributes of the TOD time source, including the ID, class and priority of the time (source).

```
Admin(config)#pptp pps-tod
```

10. Configure the local priority of the time reference source. The best master clock algorithm (BMCA) is supported for automatic selection of time sources. If several time sources have the same time attributes, you can configure the local priority to compare the time source quality. The smaller the local-priority, the higher the priority.

```
Admin(config)#ptp port <frameid/slotid/portid> local-priority
```

11. Configure the step mode for PTP ports. By default, 1588v2 packets carry timestamps in one-step mode. The 1588v2 ports identify Follow_Up packets in two-step mode in the Rx direction for communicating with other products.

```
Admin(config)#ptp port <frameid/slotid/portid> clock-step [one-step|two-step]
```

12. Configure the MAC encapsulation mode for PTP packets to be forwarded by the port. The packets are forwarded in Layer 2 mode. There are two types of destination multicast MAC addresses: unforwardable multicast MAC address (0180C200000E) and forwardable multicast MAC address (011B19000000).

```
Admin(config)#ptp port <frameid/slotid/portid> mac-egress destination-mac <value>
```

13. Configure asymmetric compensation parameters for optical fibers. Asymmetric optical fibers between two devices result in time difference in the Master-to-Slave and Slave-to-Master directions. During site deployment, measure and calculate the time differences in the two directions.

Admin(config)#**ptp port <frameid/slotid/portid> asym-delay attr [positive|negative] value <value>**

11.2.3 Configuration Example

Service Planning

An MDU connects to a 4G base station using a GE port. The MDU connects to an OLT using a GPON uplink port and then to a radio network controller (RNC) over the upper-layer network to carry 4G services over the access network.

The 4G base station requires high precision time synchronization and the 1588v2 time is deployed on the network.

Planning Data

Table 11-2 Planning Data

Equipment	Parameter
OLT	◆ Time domain: 24 ◆ Time source input port: GE uplink port 1/18/6 ◆ Time source output port: GPON user-side port 1/1/3 ◆ MAC encapsulation mode is used for the packets by default (packets are forwarded in Layer 2 mode).
MDU	◆ Time domain: 24 ◆ Time source input port: GPON uplink port ◆ Time source output port: GPON user-side port 5 ◆ MAC encapsulation mode is used for the packets by default (packets are forwarded in Layer 2 mode).

Example

◆ Configuration on the OLT:

Admin(config)#**ptp profile g.8275.1**
Admin(config-g8275-1)#**ptp enable**
Admin(config-g8275-1)#**ptp port 1/18/6 enable**
Admin(config-g8275-1)#**ptp port 1/18/6 master-only false**
Admin(config-g8275-1)#**ptp source 1/18/6**
Admin(config-g8275-1)#**exit**
Admin(config)#**interface pon 1/1/3**
Admin(config-if-pon-1/1/3)#**1588-enable switch enable**
Admin(config-if-pon-1/1/3)#**exit**

```
Admin(config)#
```

◆ Configuration on the MDU:

```
Config\ptp#ptp profile g.8275.1
Config\ptp#ptp enable
Admin(config-if-pon-1/1/3)#onu time-ptp-port cfg onuid 1 port 5 enable-state 1
```

11.3 Configuring 1588v2 (Based on IEEE)

This section introduces how to configure 1588v2 (based on IEEE).

11.3.1 Prerequisite

◆ Time synchronization can be performed only after the clock has been synchronized. For example, clock signals have been synchronized based on SyncE.

◆ 1588v2 based on G.8275.1 cannot be used together with 1588v2 based on IEEE.

11.3.2 Procedure

1. Set the device type to 1588v2 BC. By default, the BC mode is used, that is, the device complies with IEEE 1588v2 by default and implements 1588v2 based on the default profile.

```
Admin(config)#ptp profile 1588v2 or ptp device-type bc
```

2. Configure the global precision time protocol (PTP) function.

```
Admin(config)#ptp enable
```

3. Specify a time domain for the device. After the configuration, a time domain has a clock source. All the devices in the time domain use the clock source.

```
Admin(config)#ptp domain-number <value>
```

4. Configure a virtual clock ID for the device. The clock ID uniquely identifies a clock node in a time domain. The default value is 00000000-00001234.

```
Admin(config)#ptp local clock-id <value>
```

5. Enable automatic source selection for the BMC.

```
Admin(config)#ptp bmc auto
```

6. Set the time synchronization mode to hybrid for 1588v2 devices, which means that PTP packets and the physical-layer clock will be traced alternatively for synchronization.

```
Admin(config)#pptp sync-mode hybrid
```

7. Configure the BC time source. The time source can be the BC time or TOD time recovered from the network-side GE / 10GE / PON line. If the network does not support BC time synchronization, the TOD time can be used.

```
Admin(config)#ptp source <frameid/slotid/portid>
```

8. When the TOD time is used, configure the attributes of the TOD time source, including the ID, class and priority of the time (source).

```
Admin(config)#pptp pps-tod
```

9. Enable PTP for an Ethernet port. 1588v2 needs to be enabled for Ethernet ports transmitting 1588v2 packets, such as uplink ports of an OLT and user-side ports of an MDU.

```
Admin(config)#ptp port <frameid/slotid/portid> enable
```

10. Enable the 1588 function for GPON ports between the OLT and the MDU.

```
Admin(config)#1588-enable switch enable
```

11. Configure the delay measurement mechanism for a PTP port. The default value is e2e. The delay measurement mechanism applied to all the device ports in a 1588v2 synchronization network should be the same.

```
Admin(config)#ptp port <frameid/slotid/portid> delay-mechanism [e2e|p2p]
```

12. Configure the step mode for PTP ports. By default, 1588v2 packets carry timestamps in one-step mode. The 1588v2 ports identify Follow_Up packets in two-step mode in the Rx direction for communicating with other products.

```
Admin(config)#ptp port <frameid/slotid/portid> clock-step [one-step|two-step]
```

13. Configure the interval of sending PTP packets.

    - When 1588v2 frequency synchronization is used, the peer Master is required to send Sync packets at an interval no less than 32 packets/s.
    - When 1588v2 time synchronization is used, the peer Master is required to send Sync packets at an interval no less than 1 packet/s.
    - It is required that the local end device should send Delay_request or Pdelay_request packets at an interval no less than 1 packet/s.

```
Admin(config)#ptp port <frameid/slotid/portid> interval {[announce] [2^-4|2^-3|2^-2|2^-1|2^0|2^1|2^2|2^3|2^4]}*1 {[sync] [2^1|2^0|2^1|2^2|2^3|2^4|2^5|2^6|2^7]}*1 {[delay-req] [2^-4|2^-3|2^-2|2^-1|2^0|2^1|2^2|2^3|2^4]}*1
```

14. Configure the encapsulation mode for PTP packets.

    - Configure the MAC encapsulation mode for PTP packets to be forwarded by the port. The packets are forwarded in Layer 2 mode.

```
Admin(config)#ptp port <frameid/slotid/portid> mac-egress {[destination-mac] <value>}
*1 {[vlan] <0-4095>}*1 {[priority] <0-7>}*1
```

    - Configure the UDP encapsulation mode for 1588v2 packets to be forwarded by the port. The packets are forwarded in Layer 3.

```
Admin(config)#ptp port <frameid/slotid/portid> udp-egress {[destination-mac] <value>}*1
{[source-ip] <A.B.C.D>}*1 {[destination-ip] <A.B.C.D>}*1 {[dscp] <0-63>}*1 {[vlan] <0-4095>}
*1 {[priority] <0-7>}*1
```

15. Configure asymmetric compensation parameters for optical fibers.
    Asymmetric optical fibers between two devices result in time difference in the Master-to-Slave and Slave-to-Master directions. During site deployment, measure and calculate the time differences in the two directions.

```
Admin(config)#ptp port <frameid/slotid/portid> asym-delay attr [positive|negative] value
<value>
```

11.3.3 Configuration Example

Service Planning

An MDU connects to a 4G base station using a GE port. The MDU connects to an OLT via a GPON uplink port and then to a radio network controller (RNC) over the upper-layer network to carry 4G services over the access network.

The 4G base station requires high precision time synchronization and the 1588v2 time is deployed on the network.

Planning Data

Table 11-3 Planning Data

Equipment	Parameter
OLT	◆ Time domain: 0 ◆ Clock and time source input port: GE uplink port 1/18/6 ◆ Clock and time source output port: GPON user-side port 1/1/3 ◆ MAC encapsulation mode is used for the packets by default (packets are forwarded in Layer 2 mode).
MDU	◆ Time domain: 0 ◆ Click and time source input port: GPON uplink port ◆ Clock and time source output port: user-side GE port 5 ◆ MAC encapsulation mode is used for the packets by default (packets are forwarded in Layer 2 mode).

Example

◆ Configuration on the OLT:

```
Admin(config)#ptp profile 1588v2
Admin(config)#ptp enable
Admin(config)#ptp bmc auto
Admin(config)#ptp sync-mode hybrid
Admin(config)#ptp source 1/18/6
Admin(config)#ptp port 1/18/6 enable
Admin(config)#interface pon 1/1/3
Admin(config-if-pon-1/1/3)#1588-enable switch enable
Admin(config-if-pon-1/1/3)#exit
Admin(config)#
```

◆ Configuration on the MDU:

```
Config\ptp#ptp profile 1588v2
Config\ptp#ptp enable
Config\ptp#ptp bmc manual
Admin(config-if-pon-1/1/3)#onu time-ptp-port cfg onuid 1 port 5 enable-state 1
```

11.4 1588v2 (Based on IEEE) Maintenance and Diagnosis

This section introduces how to query clock / time source tracing statuses.

1. Check whether the system reference clock source is a 1588v2 clock source and whether the clock source is functional.

Admin(config)#**show clock selection-process**

```
Admin(config)# show clock selection-process

Assigned synchronization sources
-------------------------------------------------------------------
Index Board    Source      Clk-type  Impedance  State     Init
-------------------------------------------------------------------
0     HSUD     System(T0)  ---       ---        Normal    Yes
1     Unk(26)  External/0  2Mbits    75ohm      Los       Yes
2     Unk(26)  External/1  2Mhz      75ohm      Los       Yes
3     HSUD     1/4/1       Serdes    ---        Los       No
4     ---      ---         ---       ---        ---       ---
5     ---      ---         ---       ---        ---       ---
6     ---      ---         ---       ---        ---       ---
7     ---      ---         ---       ---        ---       ---
8     ---      ---         ---       ---        ---       ---
9     ---      ---         ---       ---        ---       ---

Automatic selected synchronization source for T0, state: 1A
-------------------------------------------------------------------------------------
Index Board    Source      Priority  State     SF        QL-IN     QL-OUT    Selected
-------------------------------------------------------------------------------------
3     HSUD     1/4/1       0         Los       True      QL-FAILED QL-SEC    ---

Last transition record:
01. ---         1A (ql_mode_change)
02. 1/4/1       1A (src_add)

Automatic selected synchronization source for T4, state: 1A
-------------------------------------------------------------------------------------
Index Board    Source      Priority  State     SF        QL-IN     QL-OUT    Selected
-------------------------------------------------------------------------------------

Clock output state: off

Last transition record:
01. ---         1A (ql_mode_change)
```

2. Check whether the system reference time source is a 1588v2 time source and whether the time source is functional.

Admin(config)#**show ptp-info source**

```
Admin(config)# show ptp-info source

PTP BMC Source Information:
-----------------------------------------------------------
Index  Board      Source   State    Selected  LockStatus
-----------------------------------------------------------
1      HSUD       1/4/1    Invalid  ---       ---
2      HSUD       1/4/3    Invalid  ---       ---
-----------------------------------------------------------

Admin(config)#
```

3. Check whether the system time / clock locking status is correct.

Admin(config)#**shshow lock-status**

```
Admin(config)# show lock-status
Clk source lock slot      : ---.
Clk source lock QL vlaue  : G813.
Clk source lock status    : Hold.

1PPS+TOD lock Status      : Unlocked.
PTP lock Status           : Unlocked.
Admin(config)#
```

4. Check the timestamp information of the 1588v2 time source.

```
Admin(config)#show ptp-timestamp

Admin(config)# show ptp-timestamp

PTP TimeStamp Info(ns)[slave]: 1/0/0
-------------------------------------------------------
Sync Tx(T1)           0.0
Sync Rx(T2)           0.0
Sync CorrField        0           M->S Delay     0
Delay_Req Tx(T3)      0.0
Delay_Req Rx(T4)      0.0
Delay_Req CorrField   0           S->M Delay     0
OffsetFromMaster      0           MeanPathDelay  0

Admin(config)#
```

12 Configuring Physical Layer Clock Synchronization

This chapter introduces applications of physical layer clock synchronization for the AN6001-G16.

- Application Scenarios of Physical Layer Clock Synchronization
- Configuring Physical Layer Clock Synchronization
- Maintenance and Diagnosis for Physical Layer Clock Synchronization

12.1 Application Scenarios of Physical Layer Clock Synchronization

Table 12-1 Application Scenarios of Physical Layer Clock Synchronization

Network Scenario	Condition
Restoring the system clock by using an external clock (BITS)	◆ The device needs to be synchronized with the satellite clock. It receives external clock signals via the BITS port for clock synchronization. ◆ The SyncE clock is unavailable. The device receives external clock signals via the BITS port for clock synchronization.
Restoring the system clock by using SyncE	Every device in the bearer network supports SyncE.
Clock output	When the system clock is selected as the output clock, the clock output through the BITS port of the CIOA card is a phase-locked system clock.

12.1.1 Restoring the System Clock by Using an External Clock (BITS)

As shown in Figure 12-1, when the device needs to be synchronized with a satellite clock or when no SyncE clock is available, the device receives external clock signals via the BITS port for clock synchronization.

A BITS device needs to be deployed on CO, and the cost is high.

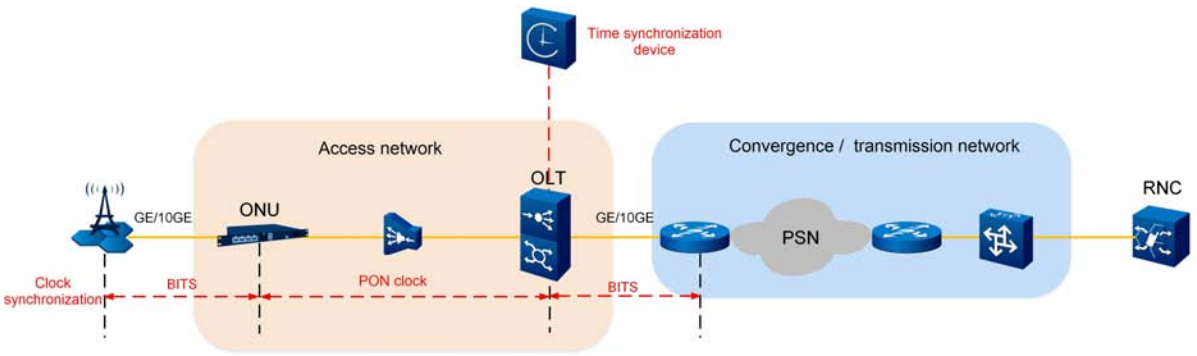


Figure 12-1 Restoring the System Clock by Using an External Clock (BITS)

12.1.2 Restoring the System Clock by Using SyncE

Traditional Ethernet applications do not consider the synchronization requirement. The Ethernet ports adopt the ±100 ppm local oscillators as transmit clocks, and the transmit clocks of various NEs are independent of each other. Accordingly, the clocks are not precise enough.

As shown in Figure 12-2, synchronization Ethernet is a technology that recovers the clock from the bit streams on the Ethernet link and implements synchronization between Ethernets. The implementation mode is similar to that on an SDH/PDH network.

SyncE uses high-precision clock signals as the transit reference in the transmit direction. It restores and extracts the clock signals at the receive end. The physical layer transmits and receives the clock signals and is compatible with traditional Ethernets.

The AN6001-G16 supports the GE / 10GE SyncE application, and can issue the GE / 10GE system clock signals, provided that every device in the bearer network supports SyncE.

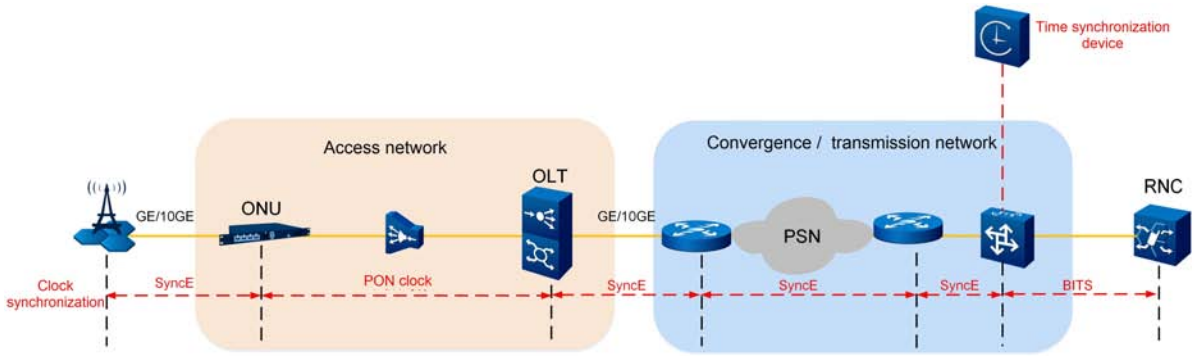


Figure 12-2 Restoring the System Clock by Using SyncE

12.1.3 Clock Output

By specific configuration, the OLT can select an output clock. The output clock can serve as the clock source for other devices.

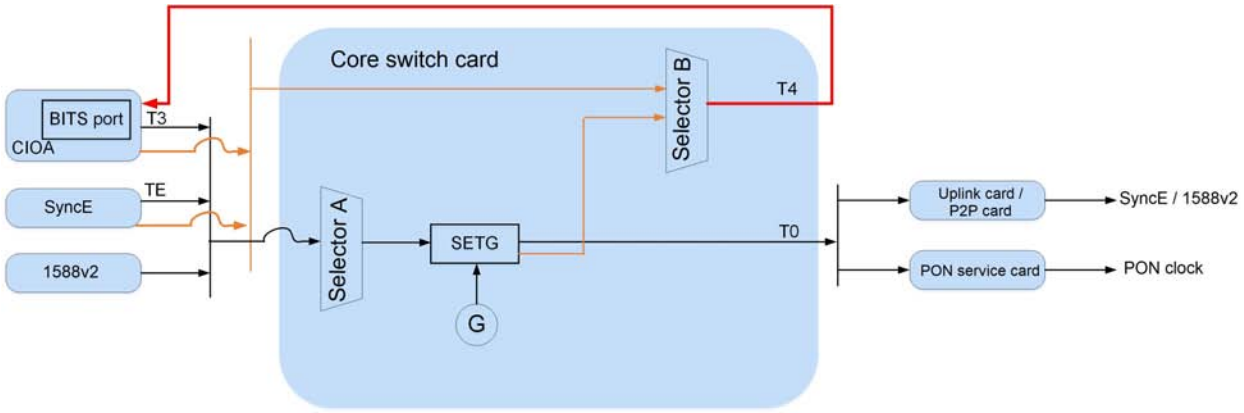


Figure 12-3 Clock Output Application Scenario

As shown in Figure 12-3, the system clock can be output via an ETH (GE / 10GE) / PON / BITS port.

When the system clock is selected as the output clock, the clock output through the BITS port of the CIOA card is a phase-locked system clock.

- TE: Inputs SyncE clock signals via a core switch card or an uplink card.
- T3: Inputs external clock signals via the BITS port of the CIOA card. The 2 Mhz and 2 Mbps signals are supported.
- T4: Outputs external clock signals via the BITS port of the CIOA card. The 2 Mhz and 2 Mbps signals are supported.
- T0: Outputs the system clock. T0 provides a reference clock for service cards to synchronize with the system clock. It can also output SyncE clock signals via an uplink port.
- 1588v2: precision time synchronization protocol, which allows synchronization accuracy within the sub-microsecond range.
- SETG: clock synchronization processing module for tracing an input clock reference source and outputting a stable system clock.
- G: local oscillator, using TCXO or OCXO, requiring a precision of ±4.6 ppm.

- Selector A: T0 system clock output source selection module, which supports clock source selection based on priority or quality level (QL). The input clock sources include
  - BITS clock source: 2 Mbps or 2 Mhz signals received from the CIOA card
  - SyncE clock source
  - 1588v2 time source
- Selector B: T4 external clock output source selection module, which supports clock source selection based on priority or QL. The output clock sources include
  - BITS clock source: 2 Mbps or 2 Mhz signals received from the CIOA card
  - SyncE line clock source
  - System clock source (T0) (recommended)

12.2 Configuring Physical Layer Clock Synchronization

Admin(config)#**show clock source**

```
Admin(config)# show clock source

Assigned Synchronization Sources:
-------------------------------------------------
Index Board    Source      Clk-type  Impedance  State     Init
-------------------------------------------------
0     XXX      System(TO)  ---       ---        Normal    Yes
1     CIOA     External/0  2Mbits    75ohm      Los       Yes
2     CIOA     External/1  2Mhz      75ohm      Los       Yes
3     ---      ---         ---       ---        ---       ---
4     ---      ---         ---       ---        ---       ---
5     ---      ---         ---       ---        ---       ---
6     ---      ---         ---       ---        ---       ---
7     ---      ---         ---       ---        ---       ---
8     ---      ---         ---       ---        ---       ---
9     ---      ---         ---       ---        ---       ---
```

Note:

The BITS and GPS clocks received by the CIOA card on the device are defined as No. 1 and No. 2 clock reference sources. These sources cannot be deleted but can be modified on attributes such as signal type and impedance type.

12.2.1 Restoring the System Clock by Using an External Clock (BITS)

When an external clock needs to be extracted and used as the system clock reference source, you need to configure the BITS clock on the CIOA card as the input reference source for the system clock.

12.2.1.1 Procedure

1. Set the clock synchronization mode to auto. Default value: free.

Admin(config)#**clock sync-mode auto**

2. Enable QL-based source selection. Default value: disable.

Admin(config)#**clock ql-mode enable**

3. Set the QL threshold for the input clock source. Default value: ql-sec.

```
Admin(config)#clock min-ql
```

4. Configure the BITS clock source signal type. Default value: 2 Mbps for BITS, and 2 Mhz for GPS.

```
Admin(config)#clock source <1-2> bits-type
```

5. Configure the SA of the BITS clock source. Default value: SA4.

```
Admin(config)#clock source <1-2> bits-sa
```

6. Configure the BITS clock source and priority. Default value: disable.

```
Admin(config)#clock source t0 <1-2> priority
```

7. Configure the QL of the input clock source. Default value: auto-pick (automatic tracing).

```
Admin(config)#clock source t0 <1-2> ow-ql
```

12.2.1.2 Configuration Example

1. Select the 2 Mbps clock received via the BITS port of the CIOA card on the device as the system clock reference source. Set the clock source priority to 0 (highest), and disable QL-based source selection.

```
Admin(config)#clock sync-mode auto
Admin(config)#clock source t0 1 priority 0
```

2. Select the 2 Mhz clock received via the BITS port of the CIOA card on the device as the system clock reference source. Set the clock source priority to 0 (highest), and disable QL-based source selection.

```
Admin(config)#clock sync-mode auto
Admin(config)#clock source 1 bits-type 2mhz
Admin(config)#clock source t0 1 priority 0
```

12.2.2 Restoring the System Clock by Using SyncE

When a SyncE clock needs to be extracted from an uplink port of a service card and used as the system clock reference source, you need to configure the SyncE clock as the input reference source for the system clock.

12.2.2.1 Prerequisite

Ethernet ports are correctly configured, and can be properly connected to uplink devices.

12.2.2.2 Procedure

1. Set the clock synchronization mode to auto. Default value: free.

```
Admin(config)#clock sync-mode auto
```

2. Enable QL-based source selection. Default value: disable.

```
Admin(config)#clock ql-mode enable
```

3. Set the QL threshold for the input clock source. Default value: ql-sec.

```
Admin(config)#clock min-ql
```

4. Configure the system clock reference source.

   - The system supports up to 10 clock reference sources, and three of them have been initialized by default.
   - Add external reference clock sources to physical entities, and set IDs for these sources.
   - To apply these external clock sources to the system, you also need to execute the clock source t0 <3-9> priority command.
   - A system clock cannot be used as the reference source of another.

```
Admin(config)#clock source <3-9>
```

5. Configure the SyncE clock source and priority. Default value: disable.

```
Admin(config)#clock source t0 <3-9> priority
```

6. Configure the QL of the input clock source. Default value: auto-pick (automatic tracing).

```
Admin(config)#clock source t0 <3-9> ow-ql
```

12.2.2.3 Configuration Example

1. Select the SyncE clock received via port 2 of the service card HU8A in slot 18 of the device as No. 3 clock reference source. Set the clock source priority to 0 (highest), and disable QL-based source selection.

```
Admin(config)#clock sync-mode auto
```

```
Admin(config)#clock source 3 1/18/2
Admin(config)#clock source t0 3 priority 0
```

12.2.3 Outputting the System Clock via the BITS Port

The BITS / SyncE / system clock can be output via the ETH (GE / 10GE) / PON / BITS port and used as the clock source for other devices. This section introduces how to output the system clock via the BITS port of the CIOA card.

12.2.3.1 Prerequisite

Select a reference clock from the physical layer clock, 1588v2 clock, and 1588ACR clock sources. Trace and lock the reference clock to recover the system clock.

12.2.3.2 Procedure

1. Configure clock output via the BITS port of the CIOA card. Set the clock output mode to “fix” (fixed tracing of the system clock).

```
Admin(config)#clock external mode fix
```

2. Configure the output clock signal type. Default value: 2 Mbps.

```
Admin(config)#clock external bits-type
```

3. Set the QL threshold for the output clock source. Default value: ql-sec.

```
Admin(config)#clock external min-ql
```

4. Configure the QL of the output clock. Default value: auto-pick (automatic tracing).

```
Admin(config)#clock ql output system
```

5. Configure the highest quality level of the output clock. Default value: ql-prc.

```
Admin(config)#clock ql output upper-limit
```

12.2.3.3 Configuration Example

1. Select the 2 Mbps clock received via the BITS port of the CIOA card on the device as the system clock reference source. Set the clock source priority to 0 (highest), and disable QL-based source selection. The system clock is output via the CIOA card.

```
Admin(config)#clock sync-mode auto
Admin(config)#clock source t0 1 priority 0
Admin(config)#clock external mode fix
```

12.2.4 Restoring the System Clock by Using the Clock Source Selected According to Priority

When the device has several clock sources with definite precisions, you need to configure priorities (0 to 255; a smaller value means a higher priority) of these clock sources.

Generally, a clock source with higher precision has a higher priority.

12.2.4.1 Procedure

1. Set the clock synchronization mode to auto. Default value: free.

```
Admin(config)#clock sync-mode auto
```

2. Disable QL-based source selection. Default value: disable.

```
Admin(config)#clock ql-mode disable
```

3. Configure the system clock reference source.
   - The system supports up to 10 clock reference sources, and three of them have been initialized by default.
   - Add external reference clock sources to physical entities, and set IDs for these sources.
   - To apply these external clock sources to the system, you also need to execute the clock source t0 <3-9> priority command.
   - A system clock cannot be used as the reference source of the system clock.

```
Admin(config)#clock source <0-9>
```

4. Configure the BITS clock source signal type. Default value: 2 Mbps for BITS, and 2 Mhz for GPS.

```
Admin(config)#clock source <1-2> bits-type
```

5. Configure the SA of the BITS clock source. Default value: SA4.

```
Admin(config)#clock source <1-2> bits-sa
```

6. Configure the clock source priority. Default value: disable.

```
Admin(config)#clock source t0 <0-9> priority
```

12.2.4.2 Configuration Example

1. Configure the clock sources received by the BITS port (2 Mpbs by default) of the CIOA card, and ports 1/18/2 and 1/19/1 of the HU8A cards as the No. 1, 3 and 4 input reference sources for the system clock. Set the priorities of No. 1, 3 and 4 sources to 0, 1, and 2 respectively.

```
Admin(config)#clock sync-mode auto
Admin(config)#clock source 3 1/18/2
Admin(config)#clock source 4 1/19/1
Admin(config)#clock source t0 1 priority 0
Admin(config)#clock source t0 3 priority 1
Admin(config)#clock source t0 4 priority 2
```

12.2.5 Restoring the System Clock by Using a Clock Source Selected According to QL

When the clock signals received from an upper layer device contain QL information, and all the clock sources are selected according to QL, you need to configure restoring the system clock by using a clock source selected according to QL.

12.2.5.1 Procedure

1. Set the clock synchronization mode to auto. Default value: free.

```
Admin(config)#clock sync-mode auto
```

2. Disable QL-based source selection, and use priority-based source selection instead. Default value: disable.

```
Admin(config)#clock ql-mode enable
```

3. Configure the QL threshold for the input clock source.

   - Default value: ql-sec
   - When the QL value of the upper layer clock source is no smaller than the QL threshold for the device, the device will trace the upper layer clock source, or otherwise, be in the clock holdover state.

   ```
   Admin(config)#clock min-ql
   ```

4. Configure the system clock reference source.

   - The system supports up to 10 clock reference sources, and three of them have been initialized by default.
   - Add external reference clock sources to physical entities, and set IDs for these sources.
   - To apply these external clock sources to the system, you also need to execute the clock source t0 <3-9> priority command.
   - A system clock cannot be used as the reference source of the system clock.

```
Admin(config)#clock source <0-9>
```

5. Configure the BITS clock source signal type. Default value: 2 Mbps for BITS, and 2 Mhz for GPS.

```
Admin(config)#clock source <1-2> bits-type
```

6. Configure the SA of the BITS clock source. Default value: SA4.

```
Admin(config)#clock source <1-2> bits-sa
```

7. Configure the clock source priority, which determines the order for selecting a clock source when several clock sources are at the same quality level.

```
Admin(config)#clock source t0 <0-9> priority
```

8. Configure the QL value of the input clock source.

   - When the reference clock source supports QL information, you can set the input QL to auto-pick, which means tracing the received QL information.
   - If the reference clock source does not support QL information, you need to manually configure the QL for the clock source. After this configuration, the device will not trace the received QL information.

```
Admin(config)#clock source t0 <0-9> ow-ql
```

9. Configure the QL value of the output clock. Default value: auto-pick (automatic tracing).

```
Admin(config)#clock ql output
```

10. Configure the highest quality level of the output clock. Default value: ql-prc.

```
Admin(config)#clock ql output upper-limit
```

12.2.5.2 Configuration Example

1. Configure the clock sources received by the BITS port (2 Mpbs signals by default) of the CIOA card, and ports 1/18/2 and 1/19/1 of the HU8A cards as the No. 1 , 3 and 4 input reference sources for the system clock. Set the priority of No. 1, 3 and 4 sources to 0, 1, and 2 respectively, and set the lower QL threshold for the clock sources received to QL-SSU-B.

```
Admin(config)#clock sync-mode auto
Admin(config)#clock ql-mode enable
Admin(config)#clock min-ql ql-ssu-b
Admin(config)#clock source 3 1/18/2
Admin(config)#clock source 4 1/19/1
Admin(config)#clock source t0 1 priority 0
Admin(config)#clock source t0 3 priority 1
Admin(config)#clock source t0 4 priority 2
```

2. Configure the clock sources received by the BITS port (2 Mhz signals by default) of the CIOA card, and ports 1/18/2 and 1/19/1 of the HU8A cards as the No. 1 , 3 and 4 input reference sources for the system clock. Set the priority of No. 1, 3 and 4 sources to 0, 1, and 2 respectively. For No. 1 clock source which does not support QL, manually set its QL to QL-SSU-A, and set the lower QL threshold for the clock sources received to QL-SSU-B.

```
Admin(config)#clock sync-mode auto
Admin(config)#clock ql-mode enable
Admin(config)#clock min-ql ql-ssu-b
Admin(config)#clock source 1 bits-type 2mhz
Admin(config)#clock source 3 1/18/2
Admin(config)#clock source 4 1/19/1
Admin(config)#clock source t0 1 priority 0
Admin(config)#clock source t0 3 priority 1
Admin(config)#clock source t0 4 priority 2
Admin(config)#clock source t0 1 ow-ql ql-ssu-a
```

12.3 Maintenance and Diagnosis for Physical Layer Clock Synchronization

This section introduces how to query physical layer clock synchronization statuses.

1. Query the clock synchronization configurations of the current system.

```
Admin(config)#show clock synchronization
```

2. Query the result of clock synchronization source selection for the current system.

```
Admin(config)#show clock selection-process
```

3. Query the clock synchronization status of the current system.

```
Admin(config)#show clock work-status
```

4. Query the ESMC packet statistics.

```
Admin(config)#show clock esmc-packet statistics（diagnose）
```

13 Configuring the Wi-Fi Service

- Network Scenario
- Configuration Flow
- Configuring the WAN Connection Service at the TL1 Interface
- Configuring the Wi-Fi Service

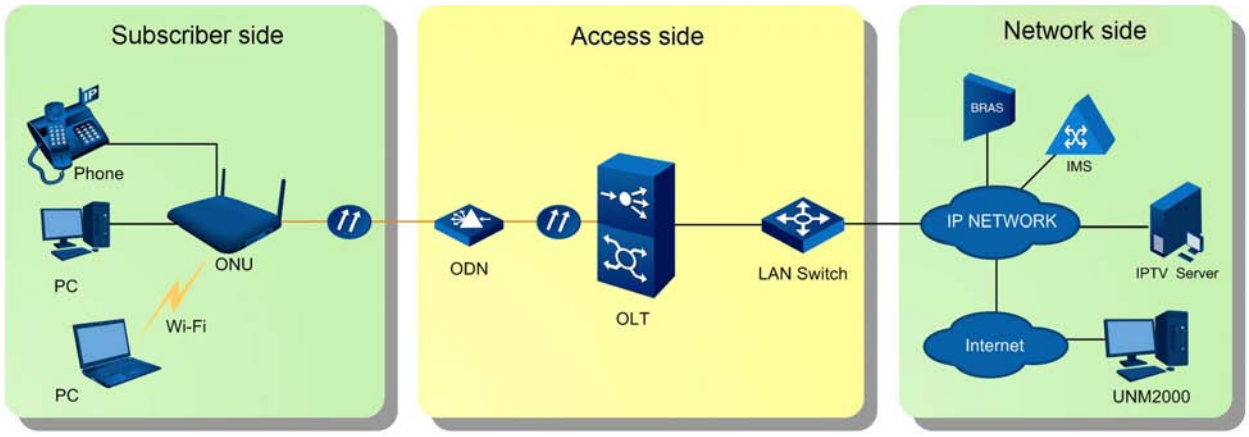
13.1 Network Scenario

Service Planning

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

Network Diagram

The figure below shows the network diagram for the Wi-Fi service on the AN6001-G16.



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

- Uplink direction:

  The ONU is connected to the OLT equipment via the GPON interface to provide integrated access services.

- Downlink direction:

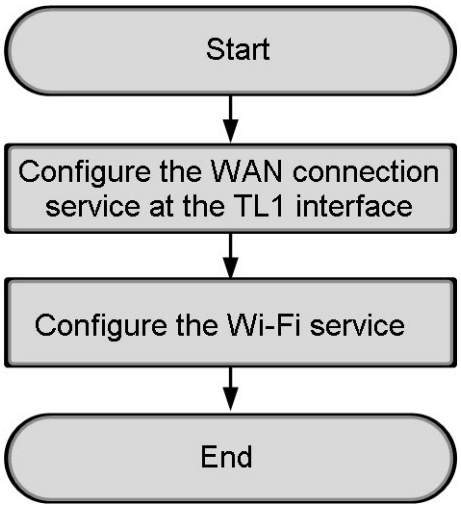
  The ONU is connected to the wireless equipment via the Wi-Fi interface to access the Wi-Fi service.

13.2 Configuration Flow

Prerequisites

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

Configuration Flow



13.3 Configuring the WAN Connection Service at the TL1 Interface

Command Format

```
onu wan-cfg <onuid> index <value> mode [tr069|internet|tr069-internet|
other|multi|voip|voip-internet|iptv|radius|radius-internet|unicast-
iptv|multicast-iptv] type [bridge|route] <vid> <cos> nat [enable|disable]
qos [enable|disable] {vlanmode [tag|transparent] tvlan [enable|disable]
<tvid> <tcos>}*1 {qinq [enable|disable] <stpid> <svlan> <scos>}*1 dsp
{[dhcp]}*1 {[dhcp-remoteid] <dhcp-remoteid>}*1 {[static] ip <A.B.C.D> mask
<A.B.C.D> gate <A.B.C.D> master <A.B.C.D> slave <A.B.C.D>}*1 {[pppoe] proxy
[enable|disable] <username> <password> <servname> [auto|payload|manual]}*1
{[null]}*1 {[active] [enable|disable]}*1 {[service-type] <service-type>}*1
{[entries] <bind-num>}*1 {[fe1|fe2|fe3|fe4|ssid1|ssid2|ssid3|ssid4]}*8
{[ssid5|ssid6|ssid7|ssid8]}*4
onu ipv6-wan-cfg <onuid> index <value> ip-stack-mode [ipv4|ipv6|both] ipv6-
src-type [dhcpv6|slaac] prefix-src-type [delegate|static] {[pppoe-
authmode] [pap|chap|mschap|auto]}*1} {[pppoe-idletime] <value>}*1 {[ipv6-
address] <ip/mask> ipv6-gateway <gateway> ipv6-master-dns <masterdns> ipv6-
slave-dns <slavedns> ipv6-static-prefix <ip/mask>}*1
```

Planning Data

Parameter	Description	Attribute	Example
<onuid>	The ONU authorization No.	Mandatory	1
index <value>	The WAN connection index	Mandatory	1

Parameter	Description	Attribute	Example
mode [tr069|internet|tr069-internet|other|multi|voip|voip-internet|iptv|radius|radius-internet|unicast-iptv|multicast-iptv]	The WAN connection mode	Mandatory	internet
type [bridge|route]	The WAN connection type ◆ bridge: the Layer 2 bridge connection mode ◆ route: the Layer 3 route connection mode	Mandatory	route
<vid>	The VLAN ID for the WAN connection. The value ranges from 1 to 4085, and can be set to 0xffff (indicating null).	Mandatory	1
<cos>	The 802.1p priority for the WAN connection. The value ranges from 0 to 7, and can be set to 0xffff (indicating null).	Mandatory	1
nat [enable|disable]	Enabling or disabling NAT for the WAN connection ◆ enable ◆ disable	Mandatory	enable
qos [enable|disable]	Enabling or disabling the QoS function for the WAN connection ◆ enable ◆ disable	Mandatory	-
vlanmode [tag|transparent]	The VLAN mode	Optional	-
tvlan [enable|disable]	The translation state (enabled or disabled) ◆ enable: enabled ◆ disable: disabled	Optional	-
<tvid>	The translated VLAN ID. The value ranges from 1 to 4085, and can be set to 0xffff (indicating null).	Optional	-
<tcos>	The priority or CoS inside the PON. The value ranges from 0 to 7, and can be set to 0xffff (indicating null).	Optional	-
qinq [enable|disable]	QinQ state ◆ enable: enabled ◆ disable: disabled	Optional	-

Parameter	Description	Attribute	Example
<stpid>	The tag protocol identifier. The value ranges from 0 to 0xfffe.	Optional	-
<svlan>	The SVLAN ID. The value ranges from 1 to 4085, and can be set to 0xffff (indicating null).	Optional	-
<scos>	The priority or CoS inside the PON. The value ranges from 0 to 7, and can be set to 0xffff (indicating null).	Optional	-
{[dhcp]}*1	Indicates whether the DHCP mode is used.	Optional	dhcp
{[dhcp-remoteid] <dhcp-remoteid>}*1	The DHCP remote identifier, a character string no longer than 10 bytes	Optional	-
[static]	Indicates whether the static mode is used.	Optional	-
ip <A.B.C.D>	The static IP address of the WAN connection	Optional	-
mask <A.B.C.D>	The subnet mask of the WAN connection	Optional	-
gate <A.B.C.D>	The default gateway of the WAN connection	Optional	-
master <A.B.C.D>	The preferred DNS of the WAN connection	Optional	-
slave <A.B.C.D>	The standby DNS of the WAN connection	Optional	-
[pppoe]	Indicates whether the PPPOE mode is used.	Optional	-
proxy [enable|disable]	Enables or disables the PPPOE proxy for the WAN connection.	Optional	-
<username>	The user name of the PPPOE connection, which contains no more than 64 characters.	Optional	-
<password>	The password for the PPPOE connection, which contains no more than 64 characters.	Optional	-
<servname>	The name of the PPPOE service, which contains no more than 32 characters.	Optional	-
[auto|payload|manual]	The PPPoE dialing mode ◆ auto: automatically connected ◆ payload: connected when payload is detected ◆ manual: manually connected	Optional	-

Parameter	Description	Attribute	Example
{[service-type] <service-type>}*1	Service type	Optional	-
{[entries] <bind-num>}*1	The quantity of ports bound. The value ranges from 0 to 8. The value 0 indicates deletion, while the values 1 to 8 indicate setting the quantity.	Optional	1
{[fe1|fe2|fe3|fe4|ssid1|ssid2|ssid3|ssid4]}*8	Binding the Ethernet port / SSID port	Optional	fe1
{[ssid5|ssid6|ssid7|ssid8]}*4	Binding the SSID port	Optional	-
ip-stack-mode [ipv4|ipv6|both]	The protocol stack type for the WAN connection	Mandatory	ipv6
ipv6-src-type [dhcpv6|slaac]	The source of the IPv6 address	Mandatory	slaac
prefix-src-type [delegate|static]	The source of the IPv6 address prefix	Mandatory	delegate
{[pppoe-authmode] [pap|chap|mschap|auto]}*1}	PPPoE authentication mode	Optional	-
{[pppoe-idletime] <value>}*1	The wait time for automatic PPPOE disconnection, ranging from 0 to 2000.	Optional	-
[ipv6-address] <ip/mask>	The IPv6 address of the WAN connection	Optional	-
ipv6-gateway <gateway>	The default IPv6 gateway of the WAN connection	Optional	-
ipv6-master-dns <masterdns>	The preferred IPv6 DNS of the WAN connection	Optional	-
ipv6-slave-dns <slavedns>	The standby IPv6 DNS of the WAN connection	Optional	-
ipv6-static-prefix <ip/mask>	The IPv6 prefix pool of the WAN connection	Optional	-

Example

- Configure the WAN connection service for ONU 1 under PON Port 1 in Slot 1 of Subrack 1. Set the WAN connection index to 1, WAN connection mode to "internet", WAN connection type to "route", VLAN ID of WAN connection to 1, and 802.1p priority of WAN connection to 1. Enable the NAT function and DHCP function, and disable the QoS function for the WAN connection. Set the quantity of ports bound to 1, and the port bound is "FE1".

```
Admin(config-if-pon-1/1/1)#onu wan-cfg 1 index 1 mode internet type route 1 1 nat
enable qos disable dsp dhcp entries 1 fe1
Admin(config-if-pon-1/1/1)#
```

- Configure the WAN connection service for ONU 1 under PON Port 1 in Slot 1 of Subrack 1. Set the WAN connection index to 1, the protocol stack type for WAN connection to "ipv6", the IPv6 address source to "slaac", and the prefix source to "delegate".

```
Admin(config-if-pon-1/1/1)#onu ipv6-wan-cfg 1 index 1 ip-stack-mode ipv6 ipv6-src-
type slaac prefix-src-type delegate
Admin(config-if-pon-1/1/1)#
```

13.4 Configuring the Wi-Fi Service

Command Format

Configure the ONU Wi-Fi service.

```
onu wifi attribute <onuid> {[serv-no] <servno>} wifi [enable|disable]
district [etsi|fcc|thailand|philippines|indonesia|brazil|india|armenia|
malaysia|pakistan|russian|china|chile|usa|myanmar|ecuador|colombia|
argentina|stilanka|iran|yemen|saudiarabia|kuwait|iraq] channel <0-165>
{[standard] [802.11b|802.11g|802.11b/g|802.11n|802.11bgn|802.11a|
802.11an|802.11ac]}*1 {[txpower] [<0-40>|<65535>]}*1 {[frequency][2.4ghz|
5.8ghz]}*1 {[freq-bandwidth] [20mhz|40mhz|20mhz/40mhz|80mhz]}*1
```

Configure the ONU WLAN service.

```
onu wifi connection <onuid> {[serv-no] <servno>} index <1-4> ssid [enable|
disable] [<ssid>|null] hide [enable|disable] authmode [open|shared|
wepauto|wpa-psk|wpa|wpa2psk|wpa2|wpa/wpa2|wpa-psk/wpa2psk|wpa-psk/
wpapsk2|waipsk|wai] encrypt-type [none|wep|tkip|aes|tkipaes|wpi] wpakey
[<wpakey>|null] interval <0-4194303> {[radius-serv] [unknown|ipv4|ipv6|
ipv4z|ipv6z|dns] <radius-serv> port <0-65535> pswd [<pswd>|null]}*1 {[wep-
length] [40bit|104bit] key-index <1-4> wep-key [<wep-key1>|null] [<wep-
key2>|null] [<wep-key3>|null] [<wep-key4>|null]}*1 {[wapi-serv-addr] <A.B.
C.D> <0-65535>}*1 {[wifi-connect-num] <num>}*1
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the ONU Wi-Fi service	<onuid>	The ONU authorization No.	Mandatory	1
	{[serv-no] <servno>}	The sequence number of a service.	Optional	1
	wifi [enable| disable]	Enables or disables the Wi-Fi function. ◆ enable: Enable the function. ◆ disable: Disable the function.	Mandatory	enable
	district [etsi|fcc| thailand| philippines| indonesia|brazil| india|armenia| malaysia|pakistan| russian|china|chile| usa |myanmar| ecuador|colombia| argentina|stilanka| iran|yemen| saudiarabia|kuwait| iraq]	The wireless area, i.e., the wireless standard used by the Wi-Fi service. The default setting is "etsi". ◆ etsi: Europe (ETSI) ◆ fcc: North America (FCC) ◆ thailand: THAILAND ◆ philippines: PHILIPPINES ◆ indonesia: INDONESIA ◆ brazil: BRAZIL ◆ india: INDIA ◆ armenia: ARMENIA ◆ malaysia: MALAYSIA ◆ pakistan: PAKISTAN ◆ russian: RUSSIAN FEDERATION ◆ china: CHINA ◆ chile: CHILE ◆ usa: UNITED STATES ◆ myanmar: MYANMAR ◆ ecuador: ECUADOR ◆ colombia: COLOMBIA ◆ argentina: ARGENTINA ◆ stilanka: SRI LANKA ◆ iran: THE ISLAMIC REPUBLIC OF IRAN ◆ yemen: YEMEN ◆ saudiarabia: SAUDI ARABIA ◆ kuwait: KUWAIT ◆ iraq: IRAQ	Mandatory	etsi
	channel <0-165>	The number of the wireless channel occupied by the service.	Mandatory	0

Procedure	Parameter	Description	Attribute	Example
	{[standard] [802.11b|802.11g|802.11b/g|802.11n|802.11bgn|802.11a|802.11an|802.11ac]}*1	The wireless standard. The default setting is "802.11bgn".	Optional	802.11bgn
	{[txpower] [<0-40>|<65535>]}*1	The Tx power (unit: dBm). ◆ 4: 20% ◆ 8: 40% ◆ 12: 60% ◆ 16: 80% ◆ 20: 100% ◆ 24: 120% ◆ 28: 140% ◆ 32: 160% ◆ 36: 180% ◆ 40: 200%	Optional	20
	{[frequency][2.4ghz|5.8ghz]}*1	The operating band.	Optional	2.4ghz
	{[freq-bandwidth] [20mhz|40mhz|20mhz/40mhz|80mhz]}*1	The frequency bandwidth.	Optional	20mhz/40-mhz
Configuring the ONU WLAN service	<onuid>	The ONU authorization No.	Mandatory	1
	{[serv-no] <servno>}	The sequence number of a service.	Optional	1
	index <1-4>	The SSID index. The value ranges from 1 to 4.	Mandatory	1
	ssid [enable|disable]	Enables or disables SSID. ◆ enable ◆ disable	Mandatory	enable
	[<ssid>|null]	The service set identifier, i.e., the name of the wireless local area network used to differentiate networks. Users who pass the identify verification can access the corresponding network. This prevents unauthorized operators from accessing the network. It contains no more than 32 characters.	Mandatory	2

Procedure	Parameter	Description	Attribute	Example
	hide [enable| disable]	Sets whether to hide the SSID. If the SSID is hidden, the user's PC will not find it. However, the user can connect the PC to the wireless network by configuring the SSID manually. ◆ enable: Hide ◆ disable: Not hide	Mandatory	enable
	authmode [open| shared|wepauto|wpa-psk|wpa|wpa2psk| wpa2|wpa/wpa2|wpa-psk/wpa2psk|wpa-psk/wpapsk2|waipsk| wai]	The WLAN authentication mode.	Mandatory	open
	encrypt-type [none| wep|tkip|aes| tkipaes|wpi]	The WLAN encryption type.	Mandatory	none
	wpakey [<wpakey>| null]	The pre-shared key for the WPA encryption mode. WPA is the upgraded version of WEP. Key protection and 802.1x protocols are enhanced in WPA. Set it to NULL or a character string no longer than 64 bytes. This field is valid when the authentication mode is WPAPSK or WPA2PSK.	Mandatory	null
	interval <0-4194303>	The WAP pre-shared key updating interval (unit: second). The value ranges from 0 to 4194303, and the default value is 86400.	Mandatory	86400
	[radius-serv] [unknown|ipv4|ipv6| ipv4z|ipv6z|dns]	The RADIUS server. The common INTERNET address.	Optional	-
	<radius-serv> port <0-65535>	The RADIUS server port. The value ranges from 0 to 65535, and the default value is 0.	Optional	-
	pswd [<pswd>|null]	The RADIUS server password. The value is no longer than 32 bytes.	Optional	-
	[wep-length] [40bit| 104bit]	The WEP key length (unit: bit). This field is valid when the encryption mode is WEP.	Optional	-

Procedure	Parameter	Description	Attribute	Example
	key-index <1-4>	The key index. This field is valid when the encryption mode is WEP. The value ranges from 1 to 4, and the default value is 1.	Optional	-
	wep-key [<wep-key1>| null] [<wep-key2>| null] [<wep-key3>| null] [<wep-key4>| null]	The WEP keys. The values should be NULL or character strings no longer than 32 bytes. ◆ <wep_key1>: the first WEP key ◆ <wep_key2>: the second WEP key ◆ <wep_key3>: the third WEP key ◆ <wep_key4>: the fourth WEP key	Optional	-
	[wapi-serv-addr] <A.B.C.D>	The IP address of the WAPI authentication server.	Optional	-
	<0-65535>	The port of the WAPI authentication server, ranging from 0 to 65535.	Optional	-
	{[wifi-connect-num] <num>}*1	The quantity of Wi-Fi connections. The value ranges from 0 to 32.	Optional	-

Example

1. Enable the Wi-Fi function for ONU 1 under PON Port 1 in Slot 1 of Subrack 1. Set the wireless area to "esti", the channel number to 0; the wireless standard to "802.11bgn", the Tx power to 20 dBm, the frequency to "2.4ghz", and the bandwidth to "20mhz/40mhz".

```
Admin(config-if-pon-1/1/1)#onu wifi attribute 1 serv-no 1 wifi enable district etsi channel 0 standard 802.11bgn txpower 20 frequency 2.4ghz freq-bandwidth 20mhz/40mhz
set hg wifi service ok!
Admin(config-if-pon-1/1/1)#
```

2. Configure the WLAN service for ONU 1 under PON Port 1 in Slot 1 of Subrack 1. Set the SSID index to 1 with the SSID enabled; and set the SSID to 2, with the SSID hidden. Set the WLAN authentication mode to "open"; the WLAN encryption type to "none"; the pre-shared key of WPA encryption mode to "null", and the WPA key updating interval to "86400".

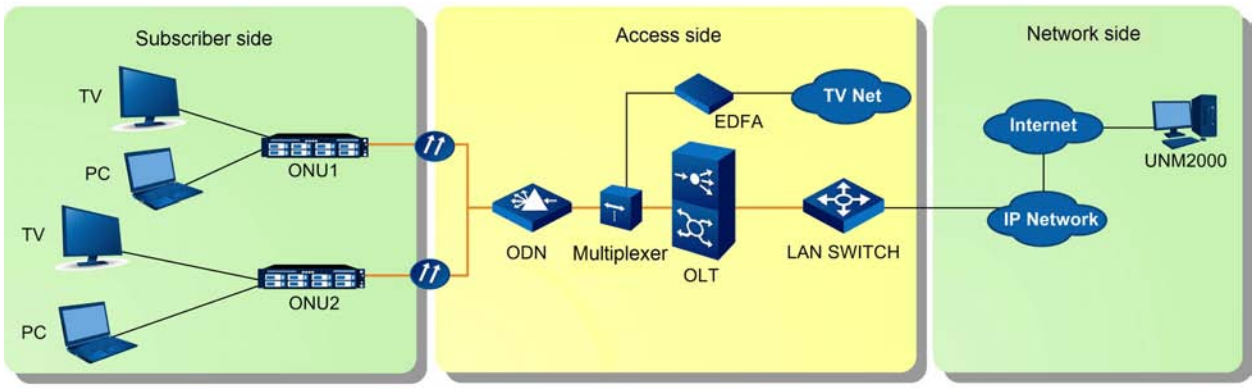
```
Admin(config-if-pon-1/1/1)#onu wifi connection 1 serv-no 1 index 1 ssid enable 2 hide enable authmode open encrypt-type none wpakey null interval 86400
set hg wifi config ok!
Admin(config-if-pon-1/1/1)#
```

14 Configuring the CATV Service

- Network Scenario
- Starting up the CATV Service

14.1 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. The figure below shows the network diagram.



14.2 Starting up the CATV Service

Command Format

```
onu catv <onuid> [enable|disable] {catv-outp-offset <catv-outp-offset>}*1
```

Planning Data

Parameter	Description	Attribute	Example
<onuid>	The ONU authorization No.	Mandatory	3
[enable|disable]	◆ enable ◆ disable	Mandatory	enable
{catv-outp-offset <catv-outp-offset>}*1	The output level adjustment, ranging from -127 to127	Optional	1

Example

```
Admin(config-if-pon-1/1/1)#onu catv 3 enable catv-outp-offset 1
Admin(config-if-pon-1/1/1)#
```

15 Configuring Layer 3 Protocols

This chapter introduces how to configure Layer 3 protocols for the AN6001-G16.

- Configuring ARP Proxy
- Configuring DHCP
- Configuring DHCPv6 Relay

15.1 Configuring ARP Proxy

This section introduces how to configure the ARP proxy for the AN6001-G16.

15.1.1 Background Information

The Address Resolution Protocol (ARP) is an Internet protocol to map IP addresses into MAC addresses. IP address is the network-layer address of a computer. To send the network-layer data packets to the destination computer, the sending device must also know the physical address, i.e. MAC address of the destination computer. Accordingly, ARP is used to resolve a known IP address to a MAC address.

ARP Proxy is implemented as follows: A host sends an ARP request to another host located in the same network segment but not in the same physical network. Then the ARP Proxy-enabled device connected to the two hosts replies to the request. ARP Proxy allows isolated users in a VLAN or different Sub VLANs to communicate with each other. In this way, all the terminal equipment in the same network segment can communicate with each other. Meanwhile, the details of the physical network are unavailable, and the division of networks into subnets is transparent to hosts.

The ARP Proxy is applied in the following aspects:

- Enabling communication inside PON: ARP Proxy allows user traffics to be forwarded and connected based on Layer-3 routing inside the OLT, so that the isolated PON network users can communicate with each other. ARP Proxy specially applies to service scenarios requiring intercommunication such as voice services.
- Reducing upper-layer service flow and delay in network transmission: Layer-3 switching of local service flow can be implemented directly at the OLT to reduce the flow in the upper layer network.
- Simplifying network architecture: The Layer-2 aggregation switch is not needed, and this simplifies network architecture.
- Enhancing network security: The upper layer network cannot learn the MAC addresses on the user side, so that MAC spoofing and broadcast storm can be avoided.

15.1.2 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.

15.1.3 Network Scenario

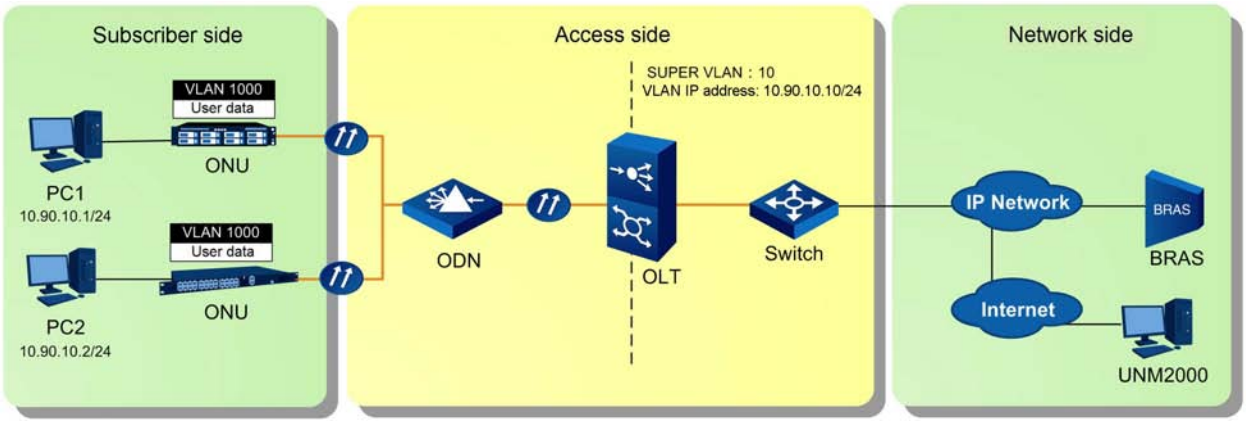
The following introduces how to configure and implement the ARP proxy function between user equipment, taking the most frequently used same-VLAN and same-network segment scenario as an example. The configurations of other scenarios are similar to this.

Service Planning

The OLT equipment 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 OLT equipment and bound with the Sub VLAN. The ARP proxy service is provided through L3 forwarding.

Network Diagram

The figure below shows the network diagram for ARP proxy in the same-VLAN and same-network segment application.



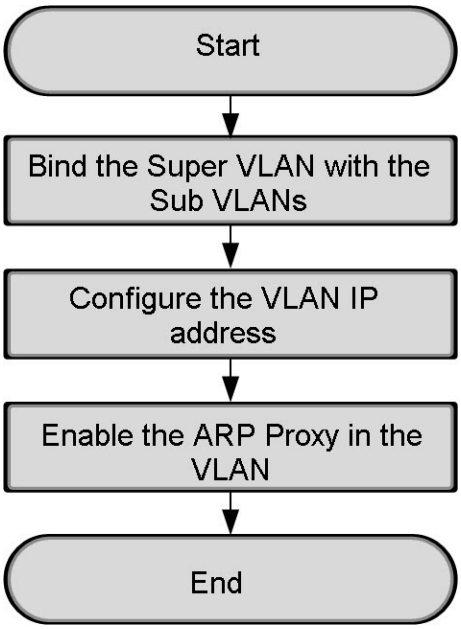
Two subscriber PCs, which belong to the same VLAN with the ID 1000, are connected to the OLT equipment via ONUs.The IP addresses of the two PCs are 10.90.10.1 and 10.90.10.2 respectively. Configure a Super VLAN and a Sub VLAN at the OLT equipment, and bind them together. After the VLAN IP address is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

15.1.4 Configuration Flow

Prerequisites

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

Configuration Flow



15.1.5 Binding the Super VLAN with the Sub VLANs

Command Format

Create a Super VLAN.

```
super-vlan <1 - 4095>
```

Bind the Super VLAN with the Sub VLANs.

```
super-vlan <svid> add sub-vlan <vid-begin> {<vid-end>}*1
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Creating a Super VLAN	super-vlan <1 - 4095>	The Super VLAN ID, ranging from 1 to 4095	Mandatory	10
Binding the Super VLAN with the Sub VLANs	super-vlan <svid>	The Super VLAN ID, ranging from 1 to 4095	Mandatory	10
	sub-vlan <vid-begin>	The starting value of the Sub VLAN ID range. The value ranges from 1 to 4085.	Mandatory	1000
	{<vid-end>}*1	The ending value of the Sub VLAN ID range. The value ranges from 1 to 4085.	Optional	-

Example

1. Create Super VLAN 10.

```
Admin(config)#super-vlan 10
```

2. Bind Super VLAN 10 with Sub VLAN 1000.

```
Admin(config)#super-vlan 10 add sub-vlan 1000
Admin(config)#
```

15.1.6 Configuring the VLAN IP Address

Command Format

```
super-vlan <1-4095> ip <A.B.C.D> mask <A.B.C.D>
```

Planning Data

Parameter	Description	Attribute	Example
super-vlan <1 - 4095>	The Super VLAN ID, ranging from 1 to 4095	Mandatory	10
ip <A.B.C.D>	IP address	Mandatory	10.90.10.10
mask <A.B.C.D>	Subnet mask	Mandatory	255.255.255.0

Example

Set the IP address of Super VLAN 10 to 10.90.10.10 and its subnet mask to 255.255.255.0.

```
Admin(config)#super-vlan 10 ip 10.90.10.10 mask 255.255.255.0
Admin(config)#
```

15.1.7 Enabling the ARP Proxy Function in the VLAN

Command Format

```
arp-switch <supervlan-id> route [enable|disable] inner-subvlan [enable|
disable] among-subvlan [enable|disable]
```

Data Planning

Parameter	Description	Attribute	Example
arp-switch <supervlan-id>	The ID of the Super VLAN to be configured with the ARP proxy switch.	Mandatory	10
route [enable|disable]	Enable or disable the route ARP proxy function.	Mandatory	enable
inner-subvlan [enable|disable]	Enable or disable the intra-Sub VLAN ARP proxy function.	Mandatory	enable
among-subvlan [enable|disable]	Enable or disable the inter-Sub VLAN ARP proxy function.	Mandatory	disable

Example

Configure the ARP proxy function for Super VLAN 10: Enable route ARP and intra-Sub VLAN ARP, and disable inter-Sub VLAN ARP.

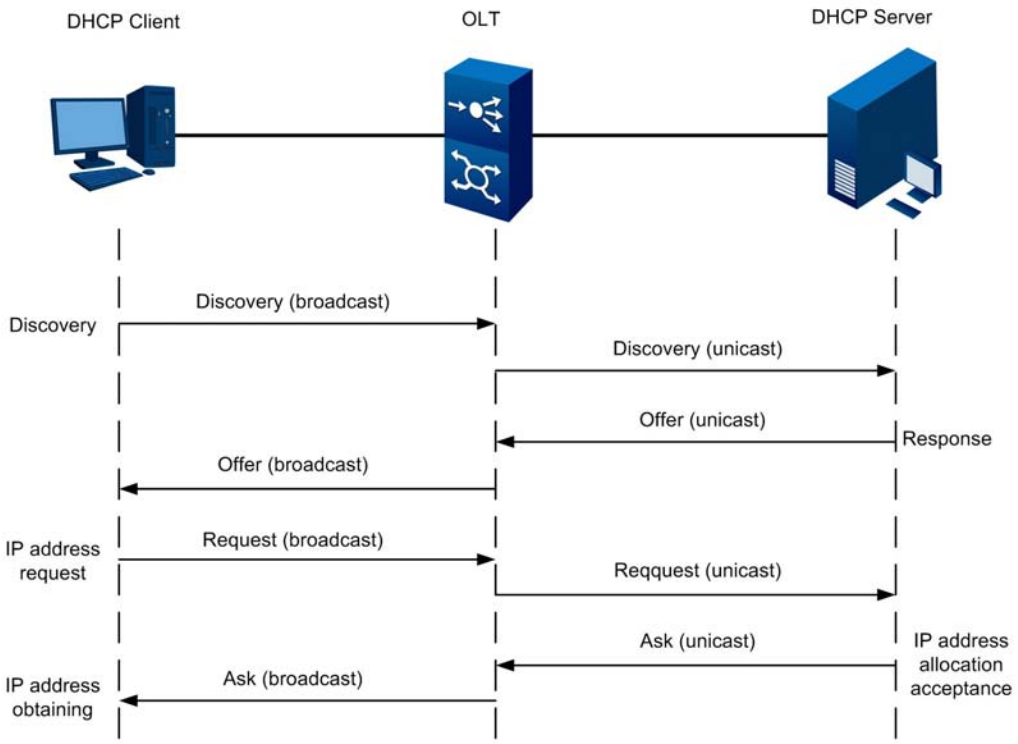
```
Admin(config)#arp-switch 10 route enable inner-subvlan enable among-subvlan disable
Admin(config)#
```

15.2 Configuring DHCP

This section introduces how to configure the DHCP for the AN6001-G16.

15.2.1 Background Information

DHCP Relay allows DHCP packets to be forwarded between the DHCP server and the DHCP clients that are in different network segments. DHCP clients can obtain the IP addresses dynamically allocated by the same DHCP server.



If the DHCP Relay feature is not supported, the DHCP protocol takes effect only when the DHCP clients and the DHCP server are in the same network segment. If they are in different network segments, each network segment requires a DHCP server, which increases deployment costs. The DHCP Relay feature solves this issue. With this feature, one DHCP server can serve multiple DHCP clients in different network segments. This not only reduces deployment costs but also facilitates centralized management of the DHCP clients.

15.2.2 Configuration Rules

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

- When serving as the DHCP Relay, the OLT 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 to convert the users' DHCP broadcast messages into 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 OLT can be configured with up to 16 Super VLANs, and 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.
- When the OLT serves as DHCP proxy only, you need to configure static routing so that the DHCP request can be forwarded to the DHCP server via the gateway.
- When the DHCP Snooping function is enabled for the OLT, 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 will be filtered. In this way, the client end can only obtain the IP address from a legal DHCP server.
- When serving as the DHCP server, the OLT will search for undistributed IP addresses from the address pool after it receives DHCP broadcast messages from users, and then transmit PING packets to check whether these IP addresses have been occupied. After confirming that the IP addresses are available, the OLT will allocate them to the users.

15.2.3 Network Scenario

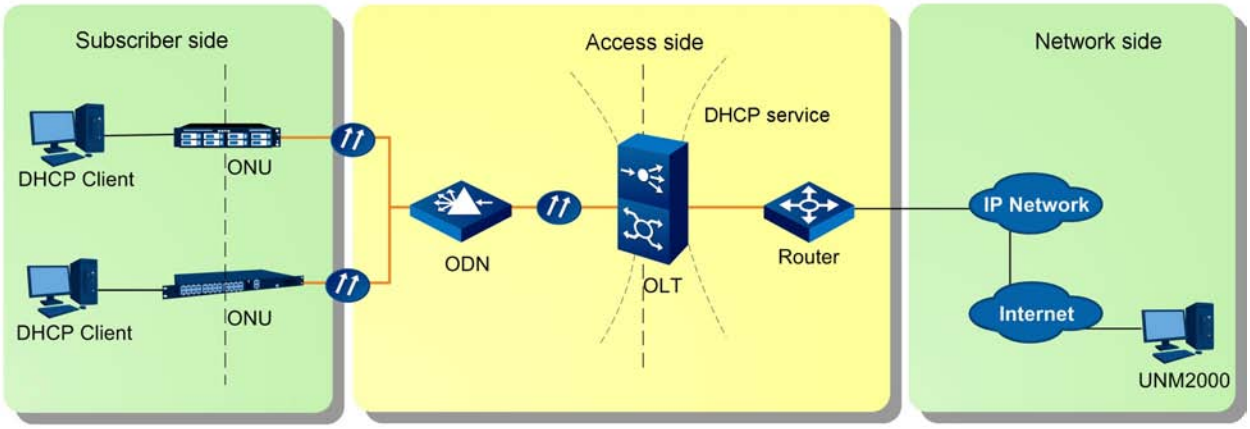
Background Information

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

- When serving as the DHCP proxy only, the OLT converts the broadcast DHCP request messages received from the DHCP Client into unicast messages, and modifies the message parameters such as the 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 OLT converts the broadcast DHCP request messages received from the DHCP Client into the 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 OLT provides the DHCP Option 60 authentication function to enable the Option 60 character authentication for PC1 and PC2 users. Two Super VLANs are provided at the OLT and bound with the Sub VLANs. Accordingly, the authentication service is provided based on proxy forwarding and character identification.
- When serving as the DHCP server and having received the broadcast DHCP request messages from the DHCP client, the OLT directly allocates the IP address in the IP address pool to the user.
- With the DHCP Snooping function enabled, the OLT 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 received from the DHCP server.

Network Diagram

The network diagram for the DHCP service carried by the AN6001-G16 is shown in the figure below.

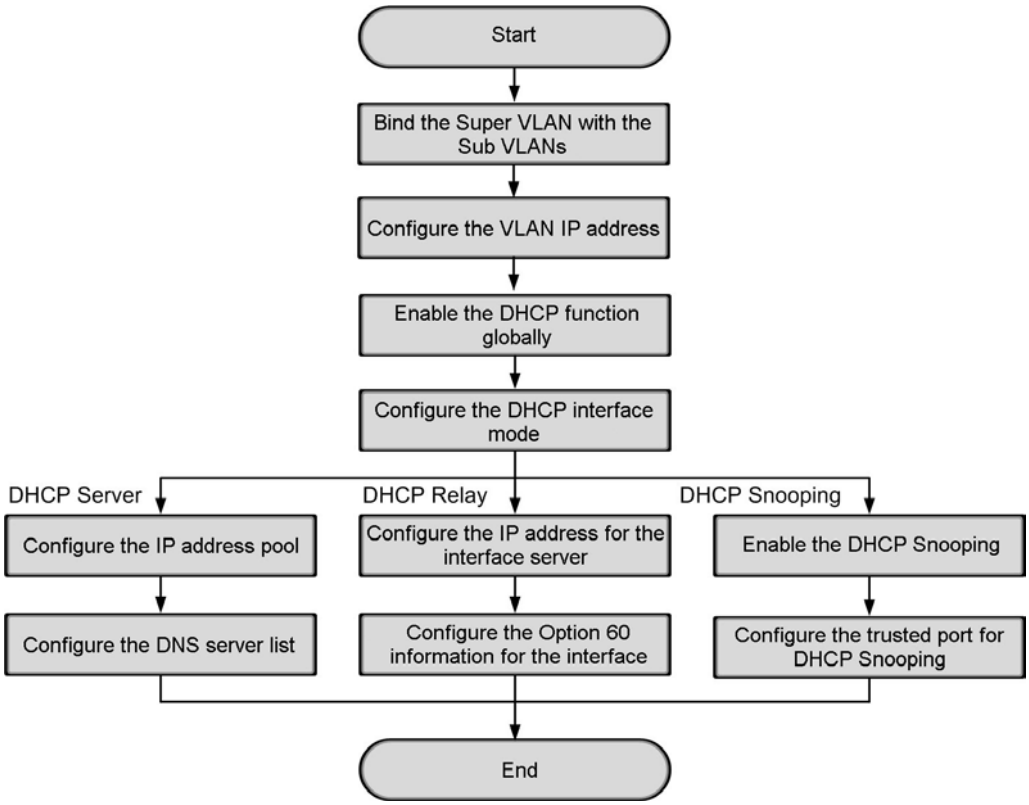


15.2.4 Configuration Flow

Prerequisites

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

Configuration Flow



15.2.5 Binding the Super VLAN with the Sub VLANs

Command Format

Create a Super VLAN.

```
super-vlan <1 - 4095>
```

Bind the Super VLAN with the Sub VLANs.

```
super-vlan <svid> add sub-vlan <vid-begin> {<vid-end>}*1
```

Data Planning

Procedure	Parameter	Description	Attribute	Example
Creating a Super VLAN	`super-vlan <1 - 4095>`	The Super VLAN ID, ranging from 1 to 4095.	Mandatory	8
Binding the Super VLAN with the Sub VLANs	`super-vlan <svid>`	The Super VLAN ID, ranging from 1 to 4095.	Mandatory	8

Procedure	Parameter	Description	Attribute	Example
	sub-vlan <vid-begin>	The starting value of the Sub VLAN ID range. The value ranges from 1 to 4085.	Mandatory	2000
	{<vid-end>}*1	The ending value of the Sub VLAN ID range. The value ranges from 1 to 4085.	Optional	2001

Example

1. Create Super VLAN 8.

```
Admin(config)#super-vlan 8
```

2. Bind Super VLAN 8 with Sub VLANs 2000 and 2001.

```
Admin(config)#super-vlan 8 add sub-vlan 2000 2001
Admin(config)#
```

15.2.6 Configuring the VLAN IP Address

Command Format

```
super-vlan <1-4095> ip <A.B.C.D> mask <A.B.C.D>
```

Planning Data

Parameter	Description	Attribute	Example
super-vlan <1 - 4095>	The Super VLAN ID. The value range: 1 to 4095.	Mandatory	8
ip <A.B.C.D>	IP address	Mandatory	41.1.1.3
mask <A.B.C.D>	Subnet mask	Mandatory	255.255.255.0

Example

Set the IP address of Super VLAN 8 to 41.1.1.3 and its subnet mask to 255.255.255.0.

```
Admin(config)#super-vlan 8 ip 41.1.1.3 mask 255.255.255.0
Admin(config)#
```

15.2.7 Configuring the DHCP Global Switch

Command Format

```
dhcp global [enable|disable]
```

Planning Data

Parameter	Description	Attribute	Example
dhcp global [enable|disable]	Enable or disable the DHCP function globally.	Mandatory	enable

Example

Enable the DHCP function.

```
Admin(config-dhcp)#dhcp global enable
Admin(config-dhcp)#
```

15.2.8 Configuring the DHCP Interface Working Mode

Command Format

```
dhcp super-vlan <svlanid> mode [server|relay|disable]
```

Planning Data

Parameter	Description	Attribute	Example
super-vlan <svlanid>	Super VLAN ID	Mandatory	8
mode [server|relay|disable]	The DHCP mode ◆ server ◆ relay ◆ disable	Mandatory	relay

Example

Set the DHCP interface to the "relay" mode.

```
Admin(config-dhcp)#dhcp super-vlan 8 mode relay
Admin(config-dhcp)#
```

15.2.9 Configuring DHCP Server

This section introduces how to configure the DHCP server.

15.2.9.1 Configuring the IP Address Pool

Command Format

```
dhcp server ip-pool <poolid> begin-ip <ipaddr> end-ip <ipaddr> mask
[<ipaddr>|<mask-length>] gateway <ipaddr>
```

Planning Data

Parameter	Description	Attribute	Example
ip-pool <poolid>	The address pool ID. The value ranges from 1 to 16.	Mandatory	1
begin-ip <ipaddr>	The starting IP address of the address pool	Mandatory	192.168.1.1
end-ip <ipaddr>	The ending IP address of the address pool	Mandatory	192.168.1.20
mask [<ipaddr>| <mask-length>]	The mask of the network segments in the address pool	Mandatory	255.255.255.0
gateway <ipaddr>	The gateway IP address	Mandatory	192.168.1.254

Example

Configure the global address pool of the DHCP server.

```
Admin(config-dhcp)#dhcp server ip-pool 1 begin-ip 192.168.1.1 end-ip 192.168.1.20
mask 255.255.255.0 gateway 192.168.1.254
Admin(config-dhcp)#
```

15.2.9.2 Configuring the DNS Server List

Command Format

```
dhcp server ip-pool <poolid> dns-server <ipaddr>
```

Planning Data

Parameter	Description	Attribute	Example
ip-pool <poolid>	The address pool ID. The value ranges from 1 to 16.	Mandatory	1
dns-server <ipaddr>	Address of the DNS server	Mandatory	10.19.8.10

Example

Set the DNS address of the DHCP server's global address pool 1 to 10.19.8.10.

```
Admin(config-dhcp)#dhcp server ip-pool 1 dns-server 10.19.8.10
Admin(config-dhcp)#
```

15.2.10 Configuring DHCP Relay

This section introduces how to configure the DHCP relay.

15.2.10.1 Configuring the Interface Server Address

Command Format

```
dhcp relay super-vlan <svlanid> server-ip <ipaddr>
```

Planning Data

Parameter	Description	Attribute	Example
super-vlan <svlanid>	Super VLAN ID	Mandatory	8
server-ip <ipaddr>	The IP addresses of the DHCP server	Mandatory	2.2.2.5

Example

Set the IP address of the interface server to 2.2.2.5.

```
Admin(config-dhcp)#dhcp relay super-vlan 8 server-ip 2.2.2.5
Admin(config-dhcp)#
```

15.2.10.2 Configuring Option 60 Information for the Port

Command Format

```
dhcp super-vlan <svlanid> relay-ip <ipaddr> option60 <str>
```

Planning Data

Parameter	Description	Attribute	Example
`super-vlan <svlanid>`	The configured Super VLAN ID. Configure the Layer 3 interface bound with the VLAN ID.	Mandatory	8
`relay-ip <ipaddr>`	The IP address of the Relay. The IP address of the Super VLAN interface.	Mandatory	41.1.1.3
`option60 <str>`	The content of the Option 60 information, which contains no more than 128 characters. Each Super VLAN can be configured with up to 64 Option 60 information entries.	Mandatory	aaaa

Example

Configure the DHCP Relay Option 60 information.

```
Admin(config-dhcp)#dhcp super-vlan 8 relay-ip 41.1.1.3 option60 aaaa
Admin(config-dhcp)#
```

15.2.11 Configuring DHCP Snooping

This section introduces how to configure the DHCP snooping.

15.2.11.1 Enabling the DHCP Snooping Function

Command Format

```
dhcp snooping [enable|disable]
```

Planning Data

Parameter	Description	Attribute	Example
`nooping [enable|disable]`	Enabling / disabling the DHCP Snooping function	Mandatory	enable

Example

```
Admin(config-dhcp)#dhcp snooping enable
Admin(config-dhcp)#
```

15.2.11.2 Configuring the DHCP Snooping Trusted Port

Command Format

```
dhcp snooping {[port] <portlist> [trust|untrust]}*1 {[serv] <ipaddr>
[trust|untrust]}*1
```

Planning Data

Parameter	Description	Attribute	Example
[port] <portlist>	Uplink port No.	Mandatory	19:5
[trust|untrust]	The state of being trusted / untrusted	Mandatory	trust
[serv] <ipaddr>	IP address of the server	Optional	-
[trust|untrust]	The state of being trusted / untrusted	Optional	-

Example

Set the DHCP Snooping trusted port to 19:5.

```
Admin(config-dhcp)#dhcp snooping port 19:5 trust
Admin(config-dhcp)#
```

15.3 Configuring DHCPv6 Relay

This section introduces the background information, network scenario, configuration flow and configuration example of the DHCPv6 Relay.

15.3.1 Background Information

As a DHCPv6 relay device, the OLT converts a Solicit packet requested by a subscriber to a Relay-forward packet through Layer 3 interfaces and sends it to the DHCPv6 server. The OLT then converts the Advertise packet received from the DHCPv6 server to a Relay-reply packet and sends it back to the subscriber.

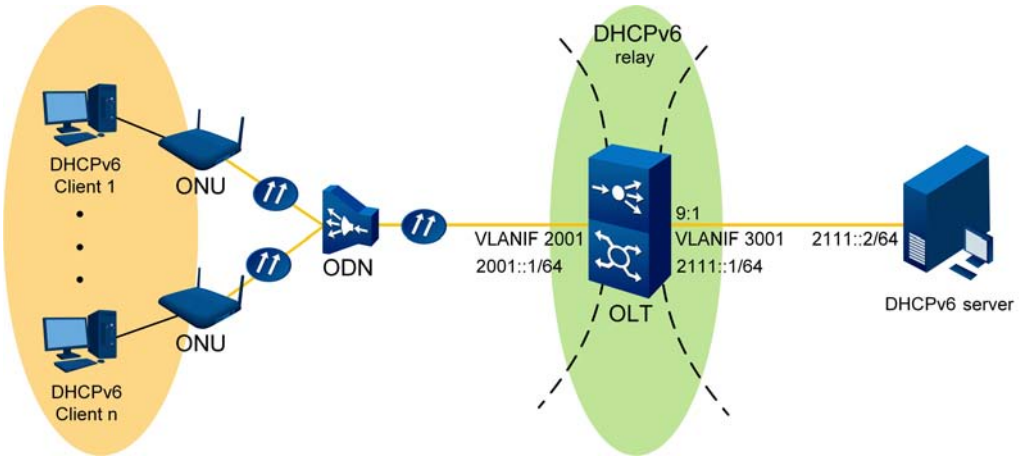
Before configuring DHCPv6 relay on an OLT device, you need to configure a static route or IGP. This ensures that the request packets sent by subscribers are forwarded to the DHCPv6 server.

15.3.2 Network Scenario

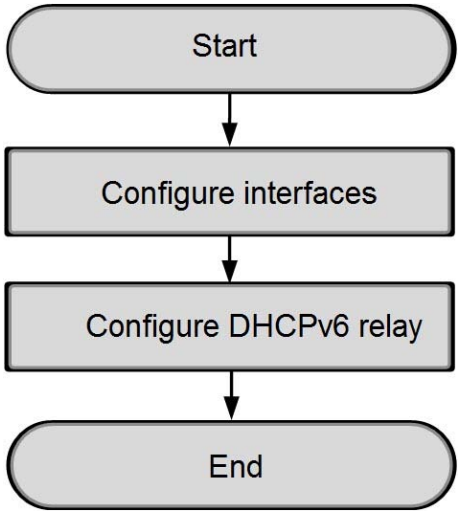
Service Planning

Set the IP address pool of the DHCPv6 server to 2111::/64. Ensure that a route is available for the DHCPv6 server to reach the ONU network segment. Configure the DHCPv6 relay on the OLT. Consequently, the DHCPv6 client obtains the IPv6 address dynamically allocated by the DHCPv6 server after sending a Solicit request.

Network Diagram



15.3.3 Configuration Flow



15.3.4 Configuring Interfaces

Configure Layer 3 interface parameters for the PON ports and uplink ports of the OLTs.

Planning Data

Parameter	Description	Example	
		OLT PON port	OLT uplink port
Start VLAN ID	Start VLAN ID of the uplink interface	2001	3001
End VLAN ID	End VLAN ID of the uplink interface	-	-
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	-	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink interface resides	-	1/9
Uplink interface number	Uplink interface number	-	1

Parameter	Description	Example	
		OLT PON port	OLT uplink port
VLAN ID	VLAN ID of the VLANIF interface	2001	3001
Enable / disable	Enable or disable the IPv6 address of the interface.	enable	enable
VLANIF interface address	IPv6 address of the VLANIF interface	2001::1	2111::1
Subnet mask of the VLANIF interface address	Prefix length of the IPv6 address of the VLANIF interface	64	64

Example

◆ Configure interface parameters for the OLT PON port.

```
Admin(config)#port vlan 2001 allslot
Admin(config)#interface vlanif 2001
Admin(config-vlanif-2001)#ipv6 enable
Admin(config-vlanif-2001)#ipv6 address 2001::1 masklen 64
Admin(config-vlanif-2001)#exit
Admin(config)#
```

◆ Configure interface parameters for the OLT uplink port.

```
Admin(config)#port vlan 3001 tag 1/9 1
Admin(config)#interface vlanif 3001
Admin(config-vlanif-3001)#ipv6 enable
Admin(config-vlanif-3001)#ipv6 address 2111::1 masklen 64
Admin(config-vlanif-3001)#exit
Admin(config)#
```

15.3.5 Configuring DHCPv6 Relay

Configure the DHCPv6 relay on the OLT. Consequently, the DHCPv6 client obtains the IPv6 address dynamically allocated by the DHCPv6 server after sending a Solicit request.

Planning Data

Parameter	Description	Example		
		OLT PON port	OLT uplink port	DHCPv6 server interface
VLANIF interface ID	VLAN ID of the VLANIF interface	2001	3001	-
Interface mode	◆ server ◆ relay ◆ client-stateless	relay	relay	-
Source IP address	IP address of the interface which sends DHCPv6 request packets, in the format of an IPv6 address	2001::1	-	-
Destination IP address	IPv6 address of the DHCPv6 server or the next-hop relay	-	-	2111::2

Configuration example

Enable DHCPv6 and set the interface to the "relay" mode.

```
Admin(config)#dhcpv6
Admin(config-dhcpv6)#dhcpv6 enable
Admin(config-dhcpv6)#dhcpv6 vlanif 2001 mode relay
Admin(config-dhcpv6)#dhcpv6 vlanif 3001 mode relay
Admin(config-dhcpv6)#dhcpv6 relay vlanif 2001 source 2001::1
Admin(config-dhcpv6)#dhcpv6 relay vlanif 3001 destination 2111::2
```

16 Configuring Routing Protocols

This chapter introduces how to configure routing protocols for the AN6001-G16.

- Configuring the IS-IS Routing Protocol
- Configuring the OSPF Routing Protocol
- Configuring the BGP Routing Protocol

16.1 Configuring the IS-IS Routing Protocol

This section introduces the background information, network scenario, configuration flow and configuration example of the IS-IS routing protocol.

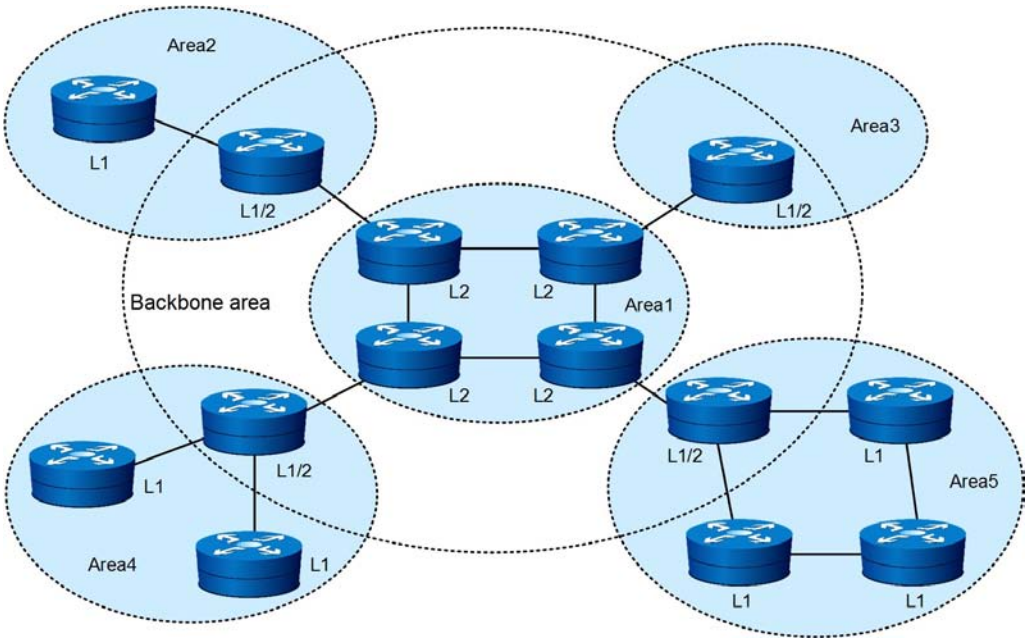
16.1.1 Background Information

The intermediate system-to-intermediate system (IS-IS) protocol is a dynamic routing protocol initially designed by the international organization for standardization (ISO) for its connectionless network protocol (CLNP).

As the TCP/IP protocol is more widely used, the IS-IS is extended and modified to support IP routing. This enables IS-IS to be applied to TCP/IP and OSI environments at the same time. This type of IS-IS is called “integrated IS-IS” or “dual IS-IS”. The IS-IS protocol hereinafter refers to the integrated IS-IS unless otherwise specified.

As an interior gateway protocol (IGP), IS-IS is used in an autonomous system (AS). IS-IS is a link state protocol. It uses the shortest path first (SPF) algorithm to calculate routes.

To support large-scale routing networks, IS-IS uses a two-level hierarchical structure in a routing domain. A routing domain is partitioned into multiple areas. As shown in the figure below, it is a network running the IS-IS protocol. The entire backbone network not only includes all L2 routers in area 1 but also includes L1/2 routers in other areas.



The IS-IS network defines routers of three levels, including Level-1, Level-2 and Level-1-2. The details are as follows:

- Level-1 router: A Level-1 router manages the intra-area routing. It establishes adjacencies only with Level-1 and Level-1-2 routers in the same area. It maintains a Level-1 link state database (LSDB). The LSDB contains the routing information on the local area. If a packet to a destination is outside of this area, Level-1 router will forward it to the nearest Level-1-2 router.
- Level-2 router: A Level-2 router manages the inter-area routing. It can establish adjacencies with Level-2 routers or Level-1-2 routers in the local area and other areas. It maintains a Level-2 LSDB that contains the inter-area routing information.

  All Level-2 routers form the backbone network of a routing domain. They are responsible for communication between areas. Level-2 routers in the routing domain must be in succession to ensure the continuity of the backbone network. Only Level-2 routers can exchange data packets or routing information directly with external routers located outside of the routing domain.

- Level-1-2 router: A router, which is both a Level-1 router and a Level-2 router, is called a Level-1-2 router. It can establish Level-1 adjacencies with Level-1 and Level-1-2 routers in the same area, or establish Level-2 adjacencies with Level-2 and Level-1-2 routers in other areas. A Level-1 router can be connected to other areas only through a Level-1-2 router. A Level-1-2 router maintains two LSDBs. The Level-1 LSDB is used for intra-area routing and the Level-2 LSDB is used for inter-area routing.

16.1.2 Network Scenario

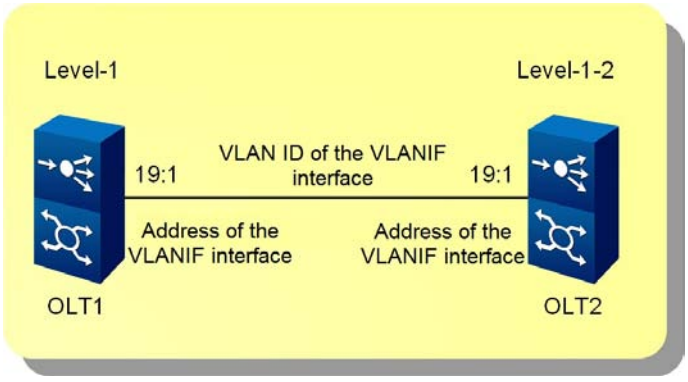
Service Planning

Note:

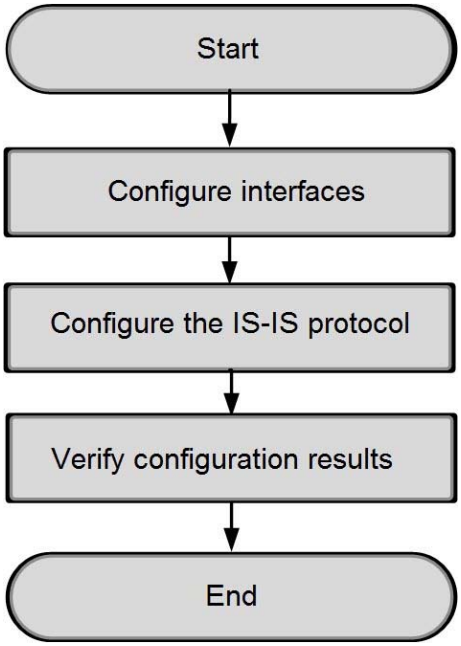
In actual networking, an OLT often serves as a Level-1 router.

Two OLTs are interconnected through the uplink port 19:1. OLT1 is a Level-1 device and OLT2 is a Level-1-2 device. OLT1 and OLT2 communicate with each other through the IS-IS IPv4/IPv6 protocol.

Network Diagram



16.1.3 Configuration Flow



16.1.4 Configuration Example of IS-IS IPv4

This section introduces how to configure the IS-IS IPv4 routing protocol.

16.1.4.1 Configuring Interfaces

Configure Layer 3 interfaces on two OLTs.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
Start VLAN ID	Start VLAN ID of the uplink interface	2016	2016
End VLAN ID	End VLAN ID of the uplink interface	-	-

Parameter	Description	Example	
		OLT1	OLT2
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink interface resides	1/19	1/19
Uplink interface number	Uplink interface number	1	1
VLAN ID	VLAN ID of the VLANIF interface	2016	2016
VLANIF interface address	IPv4 address of the VLANIF interface	30.1.1.10	30.1.1.20
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0

Procedure

1. Configure interface parameters for OLT1 and OLT2.

   ▶ Configure interface parameters for OLT1.

```
Admin(config)#port vlan 2016 tag 1/19 1
Admin(config)#interface vlanif 2016
Admin(config-vlanif-2016)#ipv4 address 30.1.1.10 mask 255.255.255.0
Admin(config-vlanif-2016)#exit
Admin(config)#
```

   ▶ Configure interface parameters for OLT2.

```
Admin(config)#port vlan 2016 tag 1/19 1
Admin(config)#interface vlanif 2016
Admin(config-vlanif-2016)#ipv4 address 30.1.1.20 mask 255.255.255.0
Admin(config-vlanif-2016)#exit
Admin(config)#
```

2. Check configurations of interfaces between OLT1 and OLT2.

   Ping 30.1.1.10 on OLT2.

```
Admin(config)#ping 30.1.1.10
PING 30.1.1.10 : 56 data bytes.
```

```
Press Ctrl-c to Stop.

Reply from 30.1.1.10 : bytes=56: icmp_seq=0 ttl=64 time<10 ms
Reply from 30.1.1.10 : bytes=56: icmp_seq=1 ttl=64 time<10 ms
Reply from 30.1.1.10 : bytes=56: icmp_seq=2 ttl=64 time<10 ms
Reply from 30.1.1.10 : bytes=56: icmp_seq=3 ttl=64 time<10 ms
Reply from 30.1.1.10 : bytes=56: icmp_seq=4 ttl=64 time<10 ms


----30.1.1.10 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 1/1/2
```

16.1.4.2 Configuring the IS-IS Protocol

Configure the IS-IS IPv4 on two OLTs to enable communications on the network.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
IS-IS route process name	Name of the IS-IS route process. It can be a string of characters including upper-case or lower-case letters, digits and underscore (_). Special characters such as # and @ are not allowed.	10	10
IS-IS route process attributes	◆ level-1: responsible for intra-area routes ◆ Level-1-2: responsible for routes of both Level-1 and Level-2 ◆ level-2: responsible for inter-area routes	level-1	level-1-2
IS-IS network entity name	Network entity name of the area in the IS-IS route process	10.0000.0002.0001.00	10.0000.0002.0002.00

Procedure

◆ Configure the IS-IS protocol for OLT1.

```
Admin(config)#router isis 10
Admin(config-isis-10)#is-type level-1
Admin(config-isis-10)#net 10.0000.0002.0001.00
Admin(config-isis-10)#exit
Admin(config)#interface vlanif 2016
```

```
Admin(config-vlanif-2016)#isis ipv4 router 10
```

◆ Configure the IS-IS protocol for OLT2.

```
Admin(config)#router isis 10
Admin(config-isis-10)#is-type level-1-2
Admin(config-isis-10)#net 10.0000.0002.0002.00
Admin(config-isis-10)#exit
Admin(config)#interface vlanif 2016
Admin(config-vlanif-2016)#isis ipv4 router 10
```

16.1.4.3 Verifying Configuration Results

Check configuration results of OLT1 and OLT2. OLT1 and OLT2 can communicate with each other through the IS-IS IPv4 protocol configurations.

◆ Verify the neighbor and route information of the IS-IS route process for OLT1.

```
Admin(config)#show isis neighbors
isis neighbors information :

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 10:  VRF : default
System Id      Interface   SNPA           State Holdtime Type Protocol
0000.0002.0002 vlanif2016  34bf.9011.7788 Up    29       L1   IS-IS
Admin(config)#show ipv4 isis route
isis ipv4 routes information :

Codes: C-connected, E-external, L1-IS-IS level-1, L2-IS-IS level-2
       ia-IS-IS inter area, D-discard, e-external metric

Tag 10:  VRF : default
     Destination         Metric   Next-Hop     Interface      Tag
C    30.1.1.0/24         10       --           vlanif2016      0
```

◆ Verify the neighbor and route information of the IS-IS route process for OLT2.

```
Admin(config)#show isis neighbors
isis neighbors information :

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 10:  VRF : default
```

```
System Id      Interface   SNPA           State Holdtime Type Protocol
0000.0002.0001 vlanif2016  48f9.7ce8.6de1 Up    8        L1   IS-IS
Admin(config)#show ipv4 isis route
isis ipv4 routes information :

Codes: C-connected, E-external, L1-IS-IS level-1, L2-IS-IS level-2
       ia-IS-IS inter area, D-discard, e-external metric

Tag 10:  VRF : default
     Destination         Metric   Next-Hop      Interface      Tag
C    30.1.1.0/24         10       --            vlanif2016      0
```

16.1.5 Configuration Example of IS-IS IPv6

This section introduces how to configure the IS-IS IPv6 routing protocol.

16.1.5.1 Configuring Interfaces

Configure Layer 3 interfaces on two OLTs.

Planning Data

Parameter	Description	Configuration Example	
		OLT1	OLT2
Start VLAN ID	Start VLAN ID of the uplink interface	2014	2014
End VLAN ID	End VLAN ID of the uplink interface	-	-
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink interface resides	1/19	1/19
Uplink interface number	Uplink interface number	1	1
VLAN ID	VLAN ID of the VLANIF interface	2014	2014
Enable / disable	Enable or disable the IPv6 address of the interface.	enable	enable

Parameter	Description	Configuration Example	
		OLT1	OLT2
VLANIF interface address	IPv6 address of the VLANIF interface	2014::2	2014::1
Subnet mask of the VLANIF interface address	Prefix length of the IPv6 address of the VLANIF interface	64	64

Procedure

1. Configure interface parameters for OLT1 and OLT2.

   - Configure interface parameters for OLT1.

```
Admin(config)#port vlan 2014 tag 1/19 1
Admin(config)#interface vlanif 2014
Admin(config-vlanif-2014)#ipv6 enable
Admin(config-vlanif-2014)#ipv6 address 2014::2 masklen 64
Admin(config-vlanif-2014)#exit
Admin(config)#
```

   - Configure interface parameters for OLT2.

```
Admin(config)#port vlan 2014 tag 1/19 1
Admin(config)#interface vlanif 2014
Admin(config-vlanif-2014)#ipv6 enable
Admin(config-vlanif-2014)#ipv6 address 2014::1 masklen 64
Admin(config-vlanif-2014)#exit
Admin(config)#
```

2. Check configurations of interfaces between OLT1 and OLT2.

   Ping 2014::1 on OLT1.

```
Admin(config)#ping -ipv6 2014::1
PING 2014::1 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 2014::1 : bytes=56: icmp_seq=0 time<10 ms
Reply from 2014::1 : bytes=56: icmp_seq=1 time<10 ms
Reply from 2014::1 : bytes=56: icmp_seq=2 time<10 ms
Reply from 2014::1 : bytes=56: icmp_seq=3 time<10 ms
Reply from 2014::1 : bytes=56: icmp_seq=4 time<10 ms


----2014::1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/0/0
```

16.1.5.2 Configuring the IS-IS Protocol

Configure the IS-IS IPv6 protocol on two OLTs to enable communications on the network.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
IS-IS route process name	Name of the IS-IS route process. It can be a string of characters including upper-case or lower-case letters, digits and underscore (_). Special characters such as # and @ are not allowed.	15	15
IS-IS route process attributes	◆ level-1: responsible for intra-area routes ◆ Level-1-2: responsible for routes of both Level-1 and Level-2 ◆ level-2: responsible for inter-area routes	level-1	level-1-2
IS-IS network entity name	Network entity name of the area in the IS-IS route process	15.0000.0001.0002.00	15.0000.0001.0012.00

Procedure

◆ Configure the IS-IS protocol for OLT1.

```
Admin(config)#router isis 15
Admin(config-isis-15)#is-type level-1
Admin(config-isis-15)#net 15.0000.0001.0002.00
Admin(config-isis-15)#exit
Admin(config)#interface vlanif 2014
Admin(config-vlanif-2014)#isis ipv6 router 15
```

◆ Configure the IS-IS protocol for OLT2.

```
Admin(config)#router isis 15
Admin(config-isis-15)#is-type level-1-2
Admin(config-isis-15)#net 15.0000.0001.0012.00
Admin(config-isis-15)#exit
Admin(config)#interface vlanif 2014
Admin(config-vlanif-2014)#isis ipv6 router 15
```

16.1.5.3 Verifying Configuration Results

Check configuration results of OLT1 and OLT2. OLT1 and OLT2 can communicate with each other through the IS-IS IPv6 protocol configurations.

◆ Verify the neighbor and route information of the IS-IS route process for OLT1.

```
Admin(config)#show isis neighbors
isis neighbors information :

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 15:  VRF : default
System Id      Interface   SNPA           State Holdtime Type Protocol
0000.0001.0012 vlanif2014  34bf.9011.7788 Up    28       L1   IS-IS
Admin(config)#show ipv6 isis route
isis ipv6 routes information :

Codes: C-connected, E-external, L1-IS-IS level-1, L2-IS-IS level-2
       ia-IS-IS inter area, D-discard, e-external metric

Tag 15:  VRF : default
C    2014::/64 [10]
      via ::, vlanif2014
```

◆ Verify the neighbor and route information of the IS-IS route process for OLT2.

```
Admin(config)#show isis neighbors
isis neighbors information :

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 15:  VRF : default
System Id      Interface   SNPA           State Holdtime Type Protocol
0000.0001.0002 vlanif2014  48f9.7ce8.6de1 Up    9        L1   IS-IS
Admin(config)#show ipv6 isis route
isis ipv6 routes information :

Codes: C-connected, E-external, L1-IS-IS level-1, L2-IS-IS level-2
       ia-IS-IS inter area, D-discard, e-external metric

Tag 15:  VRF : default
C    2014::/64 [10]
```

```
via ::, vlanif2014
```

16.2 Configuring the OSPF Routing Protocol

This section introduces the background information, network scenario, configuration flow and configuration example of the OSPF routing protocol.

16.2.1 Background Information

Open shortest path first (OSPF) is an interior gateway protocol (IGP) based on the link state. It is generally applied to a single autonomous system (AS). All the OSPF routers in this AS maintain one database that describes the AS structure. This database keeps the states of all links in the routing domain. The OSPF router works out the OSPF routing table according to this database.

Currently, OSPFv2 is applied to IPv4, and OSPFv3 is applied to IPv6.

Features of the OSPF services:

- Wide application: OSPF supports networks of various scales. It can even apply to large-scale data exchange networks with hundreds of routers.
- Fast convergence: When the network topology changes, OSPF immediately sends link state update (LSU) packets to synchronize the change to the link state databases (LSBs) of all routers in the autonomous system.
- Loop-free: OSPF uses the SPF algorithm to calculate loop-free routes based on the collected link status.
- Area division: The network of the AS is divided into areas for easier management. The routes between the areas become more abstract, reducing the occupation of bandwidth in the network.
- Equal route: OSPF supports multiple equal routes to the same destination address.
- Routing hierarchy: OSPF uses four route types: intra-area routes, inter-area routes, Type 1 external routes, and Type 2 external routes, which are listed in descending order of priority.

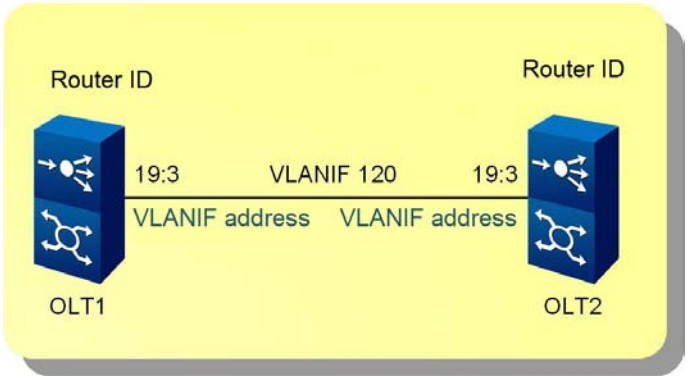
- Authentication: OSPF supports interface-based packet authentication, which ensures security of protocol packet exchange.
- Multicast: OSFP uses multicast addresses to send protocol packets on links supporting multicast. This minimizes the impact on other devices.

16.2.2 Network Scenario

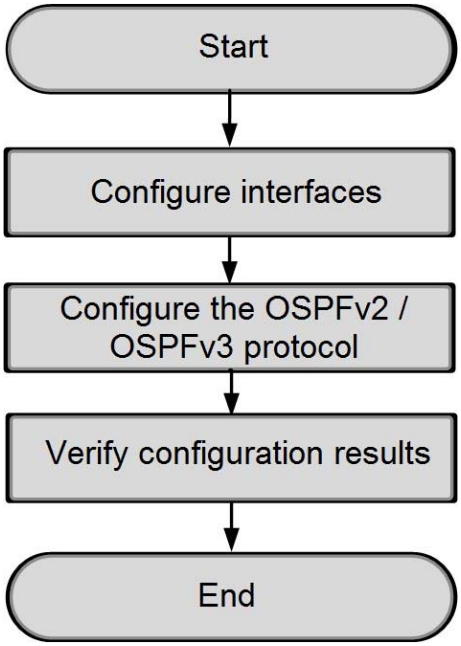
Service Planning

Two OLTs are interconnected through the uplink port 19:3. OLT1 and OLT2 communicate with each other through the OSPFv2 / OSPFv3 protocol configurations.

Network Diagram



16.2.3 Configuration Flow



16.2.4 Configuration Example of OSPFv2

This section introduces how to configure the OSPFv2 routing protocol.

16.2.4.1 Configuring Interfaces

Configure Layer 3 interfaces on two OLTs.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
Start VLAN ID	Start VLAN ID of the uplink port	120	120
End VLAN ID	End VLAN ID of the uplink port	-	-

Parameter	Description	Example	
		OLT1	OLT2
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19
Uplink interface number	Uplink interface number	3	3
VLAN ID	VLAN ID of the VLANIF interface	120	120
VLANIF interface address	IPv4 address of the VLANIF interface	120.1.1.3	120.1.1.2
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0

Procedure

1. Configure interface parameters for OLT1 and OLT2.

   ▶ Configure interface parameters for OLT1.

```
Admin(config)#port vlan 120 tag 1/19 3
Admin(config)#interface vlanif 120
Admin(config-vlanif-120)#ipv4 address 120.1.1.3 mask 255.255.255.0
Admin(config-vlanif-120)#exit
Admin(config)#
```

   ▶ Configure interface parameters for OLT2.

```
Admin(config)#port vlan 120 tag 1/19 3
Admin(config)#interface vlanif 120
Admin(config-vlanif-120)#ipv4 address 120.1.1.2 mask 255.255.255.0
Admin(config-vlanif-120)#exit
Admin(config)#
```

2. Check configurations of interfaces between OLT1 and OLT2.

   Ping 120.1.1.2 on OLT1.

```
Admin(config)#ping 120.1.1.2
PING 120.1.1.2 : 56 data bytes.
Press Ctrl-c to Stop.
```

```
Reply from 120.1.1.2 : bytes=56: icmp_seq=0 ttl=64 time<10 ms
Reply from 120.1.1.2 : bytes=56: icmp_seq=1 ttl=64 time<10 ms
Reply from 120.1.1.2 : bytes=56: icmp_seq=2 ttl=64 time<10 ms
Reply from 120.1.1.2 : bytes=56: icmp_seq=3 ttl=64 time<10 ms
Reply from 120.1.1.2 : bytes=56: icmp_seq=4 ttl=64 time<10 ms


----120.1.1.2 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 4/6/12
```

16.2.4.2 Configuring the OSPFv2 Protocol

Configure the OSPFv2 protocol on two OLTs to enable communications on the network.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
OSPFv2 route process ID	OSPFv2 route process ID. Value range: 1 to 65535	1	1
Router ID	ID of an OSPFv2 router, in the format of an IPv4 address	1.1.1.1	2.2.2.2
Network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	120.1.1.0	120.1.1.0
Subnet mask	Subnet mask of the network IP address	0.0.0.255	0.0.0.255
Area No.	OSPFv2 area number	0	0

Procedure

- Configure the OSPFv2 protocol for OLT1.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 1.1.1.1
Admin(config-ospf-1)#network 120.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#exit
Admin(config)#
```

- Configure the OSPFv2 protocol for OLT2.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 2.2.2.2
Admin(config-ospf-1)#network 120.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#exit
Admin(config)#
```

16.2.4.3 Verifying Configuration Results

Check configuration results of OLT1 and OLT2. Verify that OLT1 and OLT2 communicate with each other through the OSPFv2 protocol configurations.

- Verify neighbor information of the OSPFv2 route process for OLT1.

```
Admin(config)#show ipv4 ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID Pri State       Dead Time Address   Interface Instance ID
2.2.2.2       1 Full/Backup 00:00:34  120.1.1.2 vlanif120      0
```

- Verify neighbor information of the OSPFv2 route process for OLT2.

```
Admin(config)#show ipv4 ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID Pri State       Dead Time Address   Interface Instance ID
1.1.1.1       1 Full/DR     00:00:38  120.1.1.3 vlanif120      0
```

16.2.5 Configuration Example of OSPFv3

This section introduces how to configure the OSPFv3 routing protocol.

16.2.5.1 Configuring Interfaces

Configure Layer 3 interfaces on two OLTs.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
Start VLAN ID	Start VLAN ID of the uplink port	120	120
End VLAN ID	End VLAN ID of the uplink port	-	-

Parameter	Description	Example	
		OLT1	OLT2
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19
Uplink interface number	Uplink interface number	3	3
VLAN ID	VLAN ID of the VLANIF interface	120	120
Enable / disable	Enable or disable the IPv6 address of the interface.	enable	enable
VLANIF interface address	IPv6 address of the VLANIF interface	1200::1	1200::2
Subnet mask of the VLANIF interface address	Prefix length of the IPv6 address of the VLANIF interface	64	64

Procedure

1. Configure interface parameters for OLT1 and OLT2.

   ▶ Configure interface parameters for OLT1.

```
Admin(config)#port vlan 120 tag 1/19 3
Admin(config)#interface vlanif 120
Admin(config-vlanif-120)#ipv6 enable
Admin(config-vlanif-120)#ipv6 address 1200::1 masklen 64
Admin(config-vlanif-120)#exit
Admin(config)#
```

   ▶ Configure interface parameters for OLT2.

```
Admin(config)#port vlan 120 tag 1/19 3
Admin(config)#interface vlanif 120
Admin(config-vlanif-120)#ipv6 enable
Admin(config-vlanif-120)#ipv6 address 1200::2 masklen 64
Admin(config-vlanif-120)#exit
Admin(config)#
```

2. Check configurations of interfaces between OLT1 and OLT2.

   Ping 1200::2 on OLT1.

```
Admin(config)#ping -ipv6 1200::2
PING 1200::2 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 1200::2 : bytes=56: icmp_seq=0 time<10 ms
Reply from 1200::2 : bytes=56: icmp_seq=1 time<10 ms
Reply from 1200::2 : bytes=56: icmp_seq=2 time<10 ms
Reply from 1200::2 : bytes=56: icmp_seq=3 time<10 ms
Reply from 1200::2 : bytes=56: icmp_seq=4 time<10 ms


----1200::2 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 2/4/8
```

16.2.5.2 Configuring the OSPFv3 Protocol

Configure the OSPFv3 protocol on two OLTs to enable communications on the network.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
OSPFv3 process tag number	OSPFv3 process tag number. Value range: 1 to 63 bytes	1	1
Router ID	ID of an OSPFv3 router, in the format of an IPv4 address	11.11.11.11	22.22.22.22
VLAN ID	VLAN ID of the VLANIF interface	120	120
Area No.	OSPFv3 area number	0	0

Procedure

◆ Configure the OSPFv3 protocol for OLT1.

```
Admin(config)#router ipv6 ospf 1
Admin(config-ospfv3-1)#router-id 11.11.11.11
Admin(config-ospfv3-1)#exit
Admin(config)#interface vlanif 120
Admin(config-vlanif-120)#ipv6 router ospf area 0 tag 1
Admin(config-vlanif-120)#exit
```

```
Admin(config)#
```

◆ Configure the OSPFv3 protocol for OLT2.

```
Admin(config)#router ipv6 ospf 1
Admin(config-ospfv3-1)#router-id 22.22.22.22
Admin(config-ospfv3-1)#exit
Admin(config)#interface vlanif 120
Admin(config-vlanif-120)#ipv6 router ospf area 0 tag 1
Admin(config-vlanif-120)#exit
Admin(config)#
```

16.2.5.3 Verifying Configuration Results

Check configuration results of OLT1 and OLT2. Verify that OLT1 and OLT2 communicate with each other through the OSPFv3 protocol configurations.

◆ Verify neighbor information of the OSPFv3 route process for OLT1.

```
Admin(config)#show ospfv3 neighbor
ospfv3 neighbors information :

Total number of full neighbors: 1
OSPFv3 Process (1)
Neighbor ID  Pri   State        Dead Time  Interface  Instance ID
22.22.22.22    1   Full/Backup  00:00:32   vlanif120  0
```

◆ Verify neighbor information of the OSPFv3 route process for OLT2.

```
Admin(config)#show ospfv3 neighbor
ospfv3 neighbors information :

Total number of full neighbors: 1
OSPFv3 Process (1)
Neighbor ID  Pri   State        Dead Time  Interface  Instance ID
11.11.11.11    1   Full/DR      00:00:39   vlanif120  0
```

16.3 Configuring the BGP Routing Protocol

This section introduces the background information, network scenario, configuration flow and configuration example of the BGP routing protocol.

16.3.1 Background Information

The border gateway protocol (BGP) is an inter-AS dynamic routing protocol, which is used to transmit routing information among ASs. BGP is called an internal border gateway protocol (IBGP) when it runs within an AS and called an external border gateway protocol (EBGP) when it runs among ASs.

BGP has the following advantages:

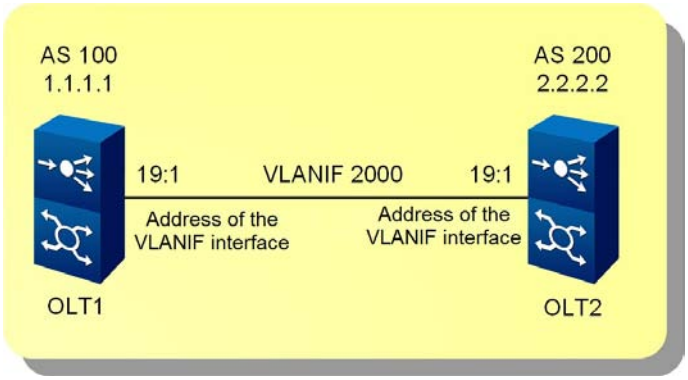
- It is an external gateway protocol (EGP) and is used to select optimal routes and control route propagation.
- It uses the TCP to transport route information at the transport layer, enhancing reliability of the network. It listens to TCP at port 179.
  - It selects routes among areas, requiring high stability of the protocol. Therefore, the TCP guarantees the stability of the BGP.
  - The BGP peers must be logically connected and communicate with each other through TCP. The local port number is random and the destination port number is 179.
- It transmits only the updated routes. This reduces the bandwidth used by BGP to transmit routes and is suitable for transmitting a large amount of routing information on the Internet.
- It supports loop avoidance.
  - Inter-AS: The BGP route carries the AS path information to mark the passing ASs and routes with the local AS number will be discarded. This avoids the inter-AS loop.
  - Intra-AS: The BGP does not advertise the route learned within its AS to its neighbors in the same AS. This avoids intra-AS loop.
- It provides abundant routing policies to flexibly filter and select routes.
- It provides a mechanism to avoid route flaps. This improves the stability of the network.
- It is scalable to support new development of the network.
- It supports classless inter-domain routing (CIDR).
- It is a distance vectoring routing protocol.

16.3.2 Network Scenario

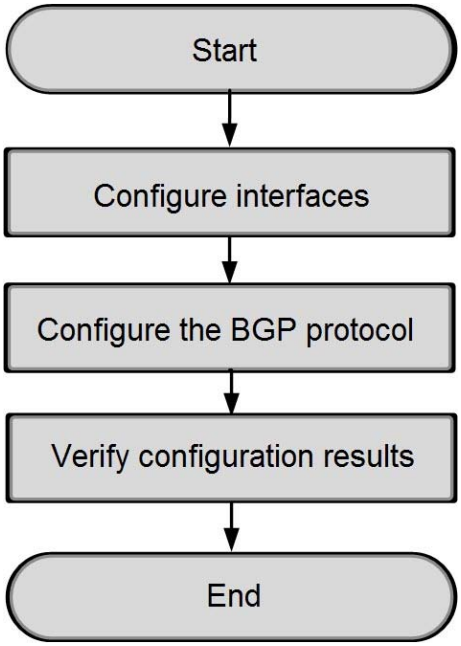
Service Planning

Two OLTs are interconnected through the uplink port 19:1. Create a BGP instance with AS being 100 on OLT1. Create a BGP instance with AS being 200 on OLT2. Configure the BGP IPv4/IPv6 protocol to set up an EBGP connection between OLT1 and OLT2.

Network Diagram



16.3.3 Configuration Flow



16.3.4 Configuration Example of BGP IPv4

This section introduces how to configure the BGP IPv4 routing protocol.

16.3.4.1 Configuring Interfaces

Configure Layer 3 interfaces on two OLTs.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
Start VLAN ID	Start VLAN ID of the uplink interface	2000	2000
End VLAN ID	End VLAN ID of the uplink interface	-	-
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink interface resides	1/19	1/19
Uplink interface number	Uplink interface number	1	1
VLAN ID	VLAN ID of the VLANIF interface	2000	2000
VLANIF interface address	IPv4 address of the VLANIF interface	120.0.2.1	120.0.2.2
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0

Procedure

1. Configure interface parameters for OLT1 and OLT2.

   ▶ Configure interface parameters for OLT1.

```
Admin(config)#port vlan 2000 tag 1/19 1
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#ipv4 address 120.0.2.1 mask 255.255.255.0
Admin(config-vlanif-2000)#exit
```

```
Admin(config)#
```

- Configure interface parameters for OLT2.

```
Admin(config)#port vlan 2000 tag 1/19 1
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#ipv4 address 120.0.2.2 mask 255.255.255.0
Admin(config-vlanif-2000)#exit
Admin(config)#
```

2. Check configurations of interfaces between OLT1 and OLT2.

   Ping 120.0.2.2 on OLT1.

```
Admin(config)#ping 120.0.2.2
PING 120.0.2.2 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 120.0.2.2 : bytes=56: icmp_seq=0 ttl=64 time=11 ms
Reply from 120.0.2.2 : bytes=56: icmp_seq=1 ttl=64 time<10 ms
Reply from 120.0.2.2 : bytes=56: icmp_seq=2 ttl=64 time<10 ms
Reply from 120.0.2.2 : bytes=56: icmp_seq=3 ttl=64 time<10 ms
Reply from 120.0.2.2 : bytes=56: icmp_seq=4 ttl=64 time<10 ms


----120.0.2.2 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 4/5/11
```

16.3.4.2 Configuring the BGP Protocol

Configure the BGP IPv4 protocol on two OLTs to set up an EBGP connection.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
AS number	AS number. Value range: 1 to 4294967295	100	200
BGP route ID	Route ID that is manually configured, in the format of an IPv4 address	1.1.1.1	2.2.2.2
BGP peer	IP address of the BGP neighbor, in the format of an IPv4 address	120.0.2.2	120.0.2.1
	IP address of the BGP neighbor, in the format of an IPv6 address	-	-

Parameter	Description	Example	
		OLT1	OLT2
	Remote AS number of the BGP peer. Value range: 1 to 4294967295	200	100

Example

◆ Configure the BGP protocol for OLT1.

```
Admin(config)#router bgp 100
Admin(config-bgp-100)#bgp router-id 1.1.1.1
Admin(config-bgp-100)#neighbor 120.0.2.2 remote-as 200
Admin(config-bgp-100)#exit
Admin(config)#
```

◆ Configure the BGP protocol for OLT2.

```
Admin(config)#router bgp 200
Admin(config-bgp-200)#bgp router-id 2.2.2.2
Admin(config-bgp-200)#neighbor 120.0.2.1 remote-as 100
Admin(config-bgp-200)#exit
Admin(config)#
```

16.3.4.3 Verifying Configuration Results

Check configuration results of OLT1 and OLT2. Verify that an EBGP connection is set up between OLT1 and OLT2 through the BGP IPv4 protocol configurations.

◆ Verify the BGP neighbor information of OLT1.

```
Admin(config)#show bgp ipv4 summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 14
0 BGP AS-PATH entries
0 BGP community entries

Neighbor  V AS  MsgRcv MsgSen TblVer InQ OutQ    Up/Down State/PfxRcd
120.0.2.2 4 200  2       3      14    0    0  00:00:05              0

Total number of neighbors 1

Total number of Established sessions 1
```

◆ Verify the BGP neighbor information of OLT2.

```
Admin(config)#show bgp ipv4 summary
BGP router identifier 2.2.2.2, local AS number 200
```

```
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor  V AS  MsgRcv MsgSen TblVer InQ OutQ    Up/Down State/PfxRcd
120.0.2.1 4 100   6       6       2    0    0  00:02:07             0

Total number of neighbors 1

Total number of Established sessions 1
```

16.3.5 Configuration Example of BGP IPv6

This section introduces how to configure the BGP IPv6 routing protocol.

16.3.5.1 Configuring Interfaces

Configure Layer 3 interfaces on two OLTs.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
Start VLAN ID	Start VLAN ID of the uplink interface	2000	2000
End VLAN ID	End VLAN ID of the uplink interface	-	-
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink interface resides	1/19	1/19
Uplink interface number	Uplink interface number	1	1
VLAN ID	VLAN ID of the VLANIF interface	2000	2000
Enable / disable	Enable or disable the IPv6 address of the interface.	enable	enable

Parameter	Description	Example	
		OLT1	OLT2
VLANIF interface address	IPv6 address of the VLANIF interface	2020:1::1	2020:1::2
Subnet mask of the VLANIF interface address	Prefix length of the IPv6 address of the VLANIF interface	64	64

Procedure

1. Configure interface parameters for OLT1 and OLT2.

   - Configure interface parameters for OLT1.

```
Admin(config)#port vlan 2000 tag 1/19 1
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#ipv6 enable
Admin(config-vlanif-2000)#ipv6 address 2020:1::1 masklen 64
Admin(config-vlanif-2000)#exit
Admin(config)#
```

   - Configure interface parameters for OLT2.

```
Admin(config)#port vlan 2000 tag 1/19 1
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#ipv6 enable
Admin(config-vlanif-2000)#ipv6 address 2020:1::2 masklen 64
Admin(config-vlanif-2000)#exit
Admin(config)#
```

2. Check configurations of interfaces between OLT1 and OLT2.

   Ping 2020:1::2 on OLT1.

```
Admin(config)#ping -ipv6 2020:1::2
PING 2020:1::2 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 2020:1::2 : bytes=56: icmp_seq=0 time<10 ms
Reply from 2020:1::2 : bytes=56: icmp_seq=1 time<10 ms
Reply from 2020:1::2 : bytes=56: icmp_seq=2 time<10 ms
Reply from 2020:1::2 : bytes=56: icmp_seq=3 time<10 ms
Reply from 2020:1::2 : bytes=56: icmp_seq=4 time<10 ms


----2020:1::2 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 3/4/9
```

16.3.5.2 Configuring the BGP Protocol

Configure the BGP IPv6 protocol on two OLTs to set up an EBGP connection.

Planning Data

Parameter	Description	Example	
		OLT1	OLT2
AS number	AS number. Value range: 1 to 4294967295	100	200
BGP route ID	Route ID that is manually configured, in the format of an IPv4 address	1.1.1.1	2.2.2.2
BGP peer	IP address of the BGP neighbor, in the format of an IPv4 address	-	-
	IP address of the BGP neighbor, in the format of an IPv6 address	2020:1::2	2020:1::1
	Remote AS number of the BGP peer. Value range: 1 to 4294967295	200	100

Procedure

◆ Configure the BGP protocol for OLT1.

```
Admin(config)#router bgp 100
Admin(config-bgp-100)#bgp router-id 1.1.1.1
Admin(config-bgp-100)#neighbor 2020:1::2 remote-as 200
Admin(config-bgp-100)#address-family ipv6 unicast
Admin(config-bgp-100-ipv6)#neighbor 2020:1::2 activate
Admin(config-bgp-100-ipv6)#exit
Admin(config-bgp-100)#exit
Admin(config)#
```

◆ Configure the BGP protocol for OLT2.

```
Admin(config)#router bgp 200
Admin(config-bgp-200)#bgp router-id 2.2.2.2
Admin(config-bgp-200)#neighbor 2020:1::1 remote-as 100
Admin(config-bgp-200)#address-family ipv6 unicast
Admin(config-bgp-200-ipv6)#neighbor 2020:1::1 activate
Admin(config-bgp-200-ipv6)#exit
Admin(config-bgp-200)#exit
Admin(config)#
```

16.3.5.3 Verifying Configuration Results

Check configuration results of OLT1 and OLT2. Verify that an EBGP connection is set up between OLT1 and OLT2 through the BGP IPv6 protocol configurations.

◆ Verify the BGP neighbor information of OLT1.

```
Admin(config)#show bgp ipv6 summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor  V AS   MsgRcv MsgSen TblVer InQ OutQ    Up/Down State/PfxRcd
2020:1::2 4 200   25      31       1    0    0  00:10:02             0

Total number of neighbors 1

Total number of Established sessions 1
```

◆ Verify the BGP neighbor information of OLT2.

```
Admin(config)#show bgp ipv6 summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor  V AS   MsgRcv MsgSen TblVer InQ OutQ    Up/Down State/PfxRcd
2020:1::1 4 100   26      24       1    0    0  00:09:06             0

Total number of neighbors 1

Total number of Established sessions 1
```

17 Configuring MPLS

This section introduces how to configure the MPLS services for the AN6001-G16.

- Configuring a Static LSP
- Configuring LDP LSP
- Configuring RSVP LSP

17.1 Configuring a Static LSP

This section introduces the background information, network scenario, configuration flow and configuration example of the static LSP.

17.1.1 Background

A static LSP is established when the administrator manually assigns labels to forwarding equivalence classes (FECs). On the device of each hop that the packet traverses, the administrator manually specifies the incoming and outgoing labels and establishes label forwarding table entries.

An AN6001-G16 device can serve as an LER or LSR. It can also serve as an ingress node, an intermediate node or an egress node, depending on where the device resides in the network.

Packets can be only forwarded on one LSP unidirectionally. To ensure bidirectional transmission of MPLS services, two static LSPs are required. These two LSPs are in reverse directions with the ingress node and egress node exchanged. Their intermediate nodes can be the same, different, or even omitted, depending on the network demands.

Concepts related to the static LSP are as follows:

Concept	Description
FEC	Forwarding equivalence class. It refers to a group of data streams which have some similarities. These data streams are forwarded by the LSR in the same manner. For the AN6001-G16, FECs can be only classified based on the destination IP address.
Label	A label is a short, fixed-length, and physically contiguous identifier which is used to identify an FEC, usually of local significance. On one device, one label can represent only one FEC.
LSP	Label switched path. It refers to a path that a packet in a particular FEC traverses in an MPLS network.

Concept	Description
LSR	Label switching router. It refers to a network device which can exchange and forward MPLS labels. LSR is also called an MPLS node.
LER	Label edge router. It refers to an LSR on the edge of the MPLS domain. The LER is responsible for classifying the packets that enter the MPLS domain to FECs and adding labels to these FECs for forwarding in the MPLS domain. When the packets leave the MPLS domain, the FECs pop up the labels, resume the original packets, and then are forwarded accordingly.

The static LSP has the following features:

- For the static LSP, the label distribution protocol (LDP) is not used and control packets need not be exchanged, so less resource is occupied. Therefore, the static LSP is applied to stable small-scale networks with a simple topology architecture.
- The static LSP cannot be dynamically adjusted according to the topology change of the network. Normally, the administrator manually adjusts it.

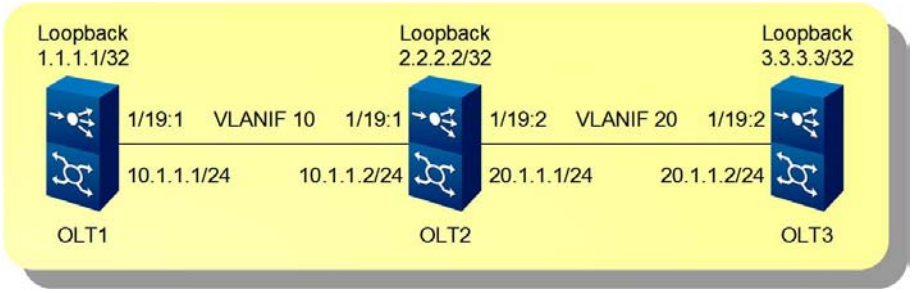
17.1.2 Network Scenario

Service Planning

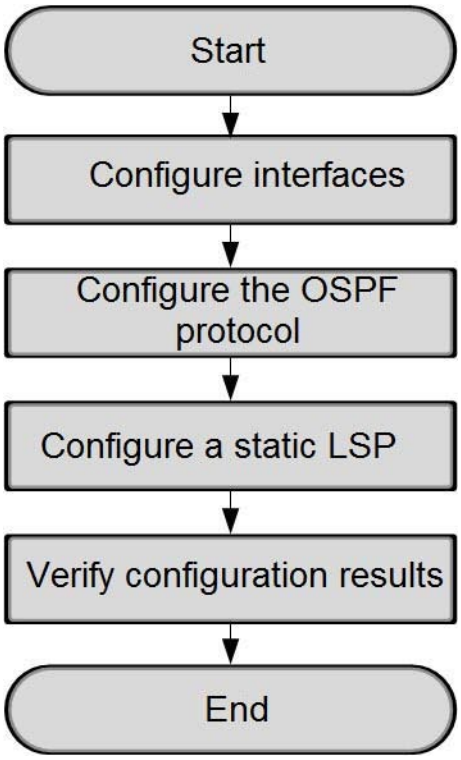
Three OLT devices are interconnected through uplink ports. Each sets up an adjacency and communicates with another through the OSPF protocol. A static LSP is configured between OLT1 and OLT3 to carry label services.

- LSP1 is a path from OLT1 to OLT3. The ingress node, transit node and egress node are OLT1, OLT2 and OLT3, respectively.
- LSP2 is a path from OLT3 to OLT1. The ingress node, transit node and egress node are OLT3, OLT2 and OLT1, respectively.

Network Diagram



17.1.3 Configuration Flow



17.1.4 Configuration Example

This section introduces how to configure the static LSP.

17.1.4.1 Configuring Interfaces

Configure Layer 3 interfaces on three OLTs.

Planning Data

Parameter	Description	Example			
		OLT1	OLT2		OLT3
Start VLAN ID	Start VLAN ID of the uplink port	10	10	20	20
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19	1/19	1/19
Port No.	Number of the uplink port	1	1	2	2
VLAN ID	VLAN ID of the VLANIF interface	10	10	20	20
VLANIF interface address	IPv4 address of the VLANIF interface	10.1.1.1	10.1.1.2	20.1.1.1	20.1.1.2
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Loopback interface address	IPv4 address of the loopback interface on the device	1.1.1.1	2.2.2.2		3.3.3.3
Subnet mask of the loopback interface address	Subnet mask of the IPv4 address of the loopback interface on the device	255.255.255.255	255.255.255.255		255.255.255.255

Procedure

1. Configure interface parameters for the ingress node OLT1.

```
Admin(config)#port vlan 10 tag 1/19 1
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#ipv4 address 10.1.1.1 mask 255.255.255.0
Admin(config-vlanif-10)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 1.1.1.1 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

2. Configure interface parameters for the transit node OLT2.

```
Admin(config)#port vlan 10 tag 1/19 1
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#ipv4 address 10.1.1.2 mask 255.255.255.0
Admin(config-vlanif-10)#exit
Admin(config)#port vlan 20 tag 1/19 2
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.1 mask 255.255.255.0
Admin(config-vlanif-20)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 2.2.2.2 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

3. Configure interface parameters for the egress node OLT3.

```
Admin(config)#port vlan 20 tag 1/19 2
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.2 mask 255.255.255.0
Admin(config-vlanif-20)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 3.3.3.3 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

17.1.4.2 Configuring the OSPF Protocol

Configure the OSPF protocol on three OLTs to enable communications between devices on the backbone network.

Planning Data

Parameter	Description	Example		
		OLT1	OLT2	OLT3
Instance number	OSPF instance number	1	1	1

Parameter	Description	Example						
		OLT1		OLT2			OLT3	
Router ID	Router ID of the OSPF, displayed in the format of an IP address	1.1.1.1		2.2.2.2			3.3.3.3	
Network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	10.1.1.0	1.1.1.1	10.1.1.0	20.1.1.0	2.2.2.2	20.1.1.0	3.3.3.3
Subnet mask	Subnet mask of the network IP address	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.0
Area No.	OSPF area number	0	0	0	0	0	0	0

Procedure

1. Configure the OSPF protocol for OLT1.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 1.1.1.1
Admin(config-ospf-1)#network 10.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 1.1.1.1 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

2. Configure the OSPF protocol for OLT2.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 2.2.2.2
Admin(config-ospf-1)#network 10.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 2.2.2.2 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

3. Configure the OSPF protocol for OLT3.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 3.3.3.3
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 3.3.3.3 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

4. Check the configuration result of the OSPF protocol.

1) OLT1 can ping 3.3.3.3 successfully.

```
Admin(config)#ping 3.3.3.3
PING 3.3.3.3 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 3.3.3.3 : bytes=56: icmp_seq=0 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

2) OLT3 can ping 1.1.1.1 successfully.

```
Admin(config)#ping 1.1.1.1
PING 1.1.1.1 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 1.1.1.1 : bytes=56: icmp_seq=0 ttl=63 time=10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

17.1.4.3 Configuring a Static LSP

A static LSP is manually configured by an administrator. It can work normally only when all the LSRs along the static LSP are configured. The LSR label distribution of the static LSP must obey the following principles: The value of the outgoing label of the previous node is equal to the value of the incoming label of the succeeding node.

The following uses LSP1 (OLT1→OLT2→OLT3) for example to introduce the configuration method.

Planning Data

Parameter	Description	Example		
		OLT1	OLT2	OLT3
Destination IP address	FEC and mask	3.3.3.3/32	3.3.3.3/32	-
Next-hop IP address	Next-hop IPv4 address of LSP	10.1.1.2	20.1.1.2	-
Incoming label	Incoming label of FEC	-	100	200
Ingress	Ingress of FEC	-	vlanif 10	vlanif 20
Outgoing label	Outgoing label of FEC	100	200	-
Egress	Egress of FEC	vlanif 10	vlanif 20	-

Procedure

1. Configure a static LSP for the ingress node OLT1.

```
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#mpls enable
Admin(config-vlanif-10)#exit
Admin(config)#mpls ftn-entry 3.3.3.3/32 100 10.1.1.2 vlanif10
```

2. Configure a static LSP for the intermediate node OLT2.

```
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#mpls enable
Admin(config-vlanif-10)#exit
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#exit
Admin(config)#mpls ilm-entry 100 vlanif10 swap 200 vlanif20 20.1.1.2 3.3.3.3/32
```

3. Configure a static LSP for the egress node OLT3.

```
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#exit
Admin(config)#mpls ilm-entry 200 vlanif20 pop
```

17.1.4.4 Verifying Configuration Results

Check the static LSP configuration results of three OLTs, including the static LSP table entries, FTN table entries and ILM table entries.

1. Check the configuration result of the ingress node OLT1.

   1) Check the static LSP table entries of OLT1.

```
Admin(config)#show static-lsp
!static-lsp config ----------------------------------------
!
mpls ftn-entry 3.3.3.3/32 100 10.1.1.2 vlanif10
!
!
!
!static-lsp config end!-------------------------------------
```

   2) Check the FTN table entries of OLT1.

```
Admin(config)#show mpls ftn-table 3.3.3.3/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 3.3.3.3/32, id: 4, row status: Active, state: Installed
  Owner: CLI, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: be
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 7
      Owner: CLI, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 7, owner: CLI, Stale: NO, out intf: vlanif10, out label: 100
    Nexthop addr: 10.1.1.2        cross connect ix: 7, op code: Push
```

2. Check the configuration result of the intermediate node OLT2.

    1) Check the static LSP table entries of OLT2.

```
Admin(config)#show static-lsp
!static-lsp config ----------------------------------------
!
!
mpls ilm-entry 100 vlanif10 swap 200 vlanif20 20.1.1.2 3.3.3.3/32
!
!
!static-lsp config end!-------------------------------------
```

    2) Check the ILM table entries of OLT2.

```
Admin(config)#show mpls ilm-table
Show MPLS ILM table :
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC        ILM-ID  In-Label  Out-Label  In-Intf   Out-Intf  Nexthop    LSP-Type
 K>   3.3.3.3/32 7       100       200        vlanif10  vlanif20  20.1.1.2   LSP_DEFAULT
```

3. Check the configuration result of the egress node OLT3.

    1) Check the static LSP table entries of OLT3.

```
Admin(config)#show static-lsp
!static-lsp config ----------------------------------------
!
!
mpls ilm-entry 200 vlanif20 pop
!
!
!static-lsp config end!-------------------------------------
```

    2) Check the ILM table entries of the intermediate node OLT3.

```
Admin(config)#show mpls ilm-table
Show MPLS ILM table :
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC        ILM-ID  In-Label  Out-Label  In-Intf   Out-Intf  Nexthop    LSP-Type
 K>   0.0.0.0/0  5       200       N/A        vlanif20  N/A       127.0.0.1  LSP_DEFAULT
```

17.2 Configuring LDP LSP

This section introduces the background information, network scenario, configuration flow and configuration example of the LDP LSP.

17.2.1 Background Information

The LDP protocol is an MPLS label distribution protocol defined by the IETF. The LDP stipulates various types of packets for the label distribution process, and the related processing. The LSRs form an LSP that crosses the entire MPLS domain according to the local forwarding table, which correlates the incoming label, next-hop node, and outcoming label of each specific FEC.

The dynamic LSP can be created through LDP on the AN6001-G16.

Concepts related to the LDP are as follows:

Concept	Description
LDP adjacency	It indicates a TCP connection established after two LSRs transmit Hello messages to each other. ◆ Local adjacency: Indicates the adjacencies discovered by link Hello messages. ◆ Remote adjacency: Indicates the adjacencies discovered by target Hello messages.
LDP peers	They indicate two LSRs which have LDP sessions between them and use the LDP to switch label messages after the TCP connection is established. The LDP peers obtain labels from each other through LDP sessions.
LDP session	It indicates the process where two LDP peers switch labels with each other. The LDP session is a connection established based on the TCP. ◆ LDP local session: A session established between two LSRs which are adjacent. ◆ LDP remote session: A session established between two LSRs which can be adjacent or non-adjacent.

The LDP has the following features:

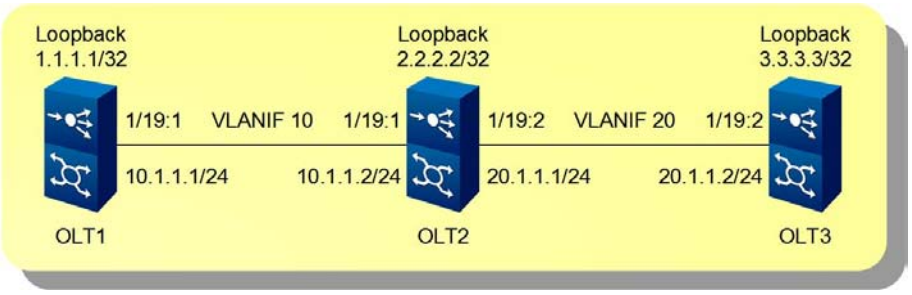
- Simple network and configurations
- LSP established by routing topology
- Large-capacity LSP

17.2.2 Network Scenario

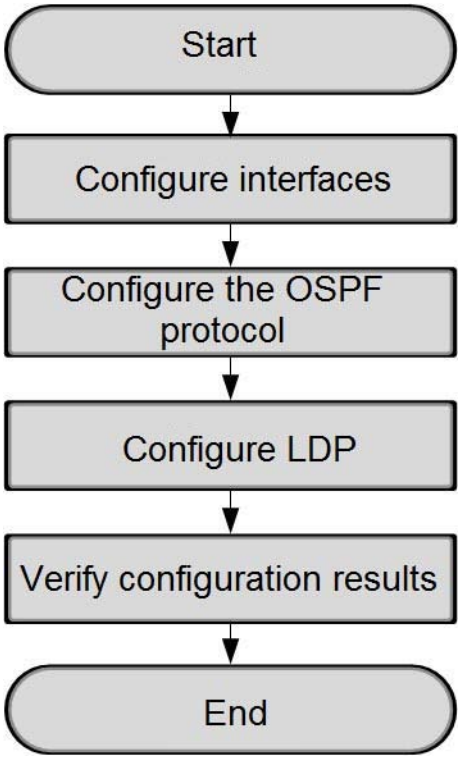
Service Planning

Three OLT devices are interconnected through uplink ports. Each sets up an adjacency and communicates with another through the OSPF protocol. A public network tunnel is configured through LDP between OLT1 and OLT3 to carry label services, and distribute and switch labels.

Network Diagram



17.2.3 Configuration Flow



17.2.4 Configuration Example

This section introduces how to configure the LDP LSP.

17.2.4.1 Configuring Interfaces

Configure Layer 3 interfaces on three OLTs.

Planning Data

Parameter	Description	Example			
		OLT1	OLT2		OLT3
Start VLAN ID	Start VLAN ID of the uplink port	10	10	20	20
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19	1/19	1/19
Port No.	Number of the uplink port	1	1	2	2
VLAN ID	VLAN ID of the VLANIF interface	10	10	20	20
VLANIF interface address	IPv4 address of the VLANIF interface	10.1.1.1	10.1.1.2	20.1.1.1	20.1.1.2
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Parameter	Description	Example		
		OLT1	OLT2	OLT3
Loopback interface address	IPv4 address of the loopback interface on the device	1.1.1.1	2.2.2.2	3.3.3.3
Subnet mask of the loopback interface address	Subnet mask of the IPv4 address of the loopback interface on the device	255.255.255.255	255.255.255.255	255.255.255.255

Procedure

1. Configure interface parameters for OLT1.

```
Admin(config)#port vlan 10 tag 1/19 1
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#ipv4 address 10.1.1.1 mask 255.255.255.0
Admin(config-vlanif-10)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 1.1.1.1 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

2. Configure interface parameters for OLT2.

```
Admin(config)#port vlan 10 tag 1/19 1
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#ipv4 address 10.1.1.2 mask 255.255.255.0
Admin(config-vlanif-10)#exit
Admin(config)#port vlan 20 tag 1/19 2
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.1 mask 255.255.255.0
Admin(config-vlanif-20)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 2.2.2.2 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

3. Configure interface parameters for OLT3.

```
Admin(config)#port vlan 20 tag 1/19 2
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.2 mask 255.255.255.0
Admin(config-vlanif-20)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 3.3.3.3 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

17.2.4.2 Configuring the OSPF Protocol

Configure the OSPF protocol on three OLTs to enable communications between devices on the backbone network.

Planning Data

Parameter	Description	Example						
		OLT1		OLT2			OLT3	
Instance number	OSPF instance number	1		1			1	
Router ID	Router ID of the OSPF, displayed in the format of an IP address	1.1.1.1		2.2.2.2			3.3.3.3	
Network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	10.1.1.0	1.1.1.1	10.1.1.0	20.1.1.0	2.2.2.2	20.1.1.0	3.3.3.3
Subnet mask	Subnet mask of the network IP address	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.0
Area No.	OSPF area number	0	0	0	0	0	0	0

Procedure

1. Configure the OSPF protocol for OLT1.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 1.1.1.1
Admin(config-ospf-1)#network 10.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 1.1.1.1 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

2. Configure the OSPF protocol for OLT2.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 2.2.2.2
Admin(config-ospf-1)#network 10.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 2.2.2.2 0.0.0.0 area 0
```

```
Admin(config-ospf-1)#exit
```

3. Configure the OSPF protocol for OLT3.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 3.3.3.3
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 3.3.3.3 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

4. Check the configuration result of the OSPF protocol.

   1) OLT1 can ping 3.3.3.3 successfully.

```
Admin(config)#ping 3.3.3.3
PING 3.3.3.3 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 3.3.3.3 : bytes=56: icmp_seq=0 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 3.3.3.3 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

   2) OLT3 can ping 1.1.1.1 successfully.

```
Admin(config)#ping 1.1.1.1
PING 1.1.1.1 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 1.1.1.1 : bytes=56: icmp_seq=0 ttl=63 time=10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 1.1.1.1 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

17.2.4.3 Configuring LDP Sessions

Configure MPLS LDP sessions between three OLTs. The LDP LSP is automatically created after the LDP session is set up.

Planning Data

Parameter	Description	Example		
		OLT1	OLT2	OLT3
Router ID	Router identifier	1.1.1.1	2.2.2.2	3.3.3.3
LDP transport address	Source transport address in LDP Hello messages, in the format of an IPv4 address	1.1.1.1	2.2.2.2	3.3.3.3

Parameter	Description	Example			
		OLT1	OLT2		OLT3
VLAN ID	VLAN ID of the VLANIF interface	10	10	20	20
Interface LDP enabling	Enable the IP address format of the LDP for an interface	ipv4	ipv4		ipv4
LDP remote address	IP address of the LDP remote peer, in the format of an IPv4 address	3.3.3.3	-		1.1.1.1

Procedure

1. Configure LDP local and remote sessions for OLT1.

```
Admin(config)#router ldp
Admin(config-router)#router-id 1.1.1.1
Admin(config-router)#transport-address ipv4 1.1.1.1
Admin(config-router)#exit
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#mpls enable
Admin(config-vlanif-10)#ldp enable ipv4
Admin(config-vlanif-10)#exit
Admin(config)#router ldp
Admin(config-router)#targeted-peer ipv4 3.3.3.3
Admin(config-router)#exit
```

2. Configure LDP local sessions for OLT2.

```
Admin(config)#router ldp
Admin(config-router)#router-id 2.2.2.2
Admin(config-router)#transport-address ipv4 2.2.2.2
Admin(config-router)#exit
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#mpls enable
Admin(config-vlanif-10)#ldp enable ipv4
Admin(config-vlanif-10)#exit
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#ldp enable ipv4
Admin(config-vlanif-20)#exit
```

3. Configure LDP local and remote sessions for OLT3.

```
Admin(config)#router ldp
Admin(config-router)#router-id 3.3.3.3
Admin(config-router)#transport-address ipv4 3.3.3.3
```

```
Admin(config-router)#exit
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#ldp enable ipv4
Admin(config-vlanif-20)#exit
Admin(config)#router ldp
Admin(config-router)#targeted-peer ipv4 1.1.1.1
Admin(config-router)#exit
```

17.2.4.4 Verifying Configuration Results

Check LDP configuration results for three OLTs, including LDP parameters and LDP session states.

1. Check the configuration result of OLT1.

   1) Check the LDP parameters of OLT1.

```
Admin(config)#show ldp param
Show LDP :
Router ID                : 1.1.1.1
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 0           : 1.1.1.1 (in use)
Import BGP routes        : No
```

   2) Check the LDP session states of OLT1, including states of local and remote sessions.

```
Admin(config)#show mpls ldp session
```

```
show mpls ldp session :
Peer IP Address           IF Name    My Role    State       KeepAlive
3.3.3.3                   vlanif10   Passive   OPERATIONAL   30
2.2.2.2                   vlanif10   Passive   OPERATIONAL   30
```

3) Check the FTN table entries from OLT1 to OLT3.

```
Admin(config)# show mpls ftn-table 3.3.3.3/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 3.3.3.3/32, id: 3, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, Stale: NO, out intf: vlanif10, out label:
52481
    Nexthop addr: 10.1.1.2        cross connect ix: 4, op code: Push
```

2. Check the configuration result of OLT2.

1) Check the LDP parameters of OLT2.

```
Admin(config)#show ldp param
Show LDP :
Router ID                : 2.2.2.2
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 0           : 2.2.2.2 (in use)
Import BGP routes        : No
```

2) Check the LDP session states of OLT2.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address           IF Name    My Role    State       KeepAlive
3.3.3.3                   vlanif20   Passive   OPERATIONAL   30
```

```
1.1.1.1                    vlanif10    Active     OPERATIONAL    30
```

3) Check the FTN table entries of OLT2.

- Check the FTN table entries from OLT2 to OLT1.

```
Admin(config)# show mpls ftn-table 1.1.1.1/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 1.1.1.1/32, id: 3, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, Stale: NO, out intf: vlanif10, out label: 3
    Nexthop addr: 10.1.1.1        cross connect ix: 4, op code: Push
```

- Check the FTN table entries from OLT2 to OLT3.

```
Admin(config)# show mpls ftn-table 3.3.3.3/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 3.3.3.3/32, id: 1, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, Stale: NO, out intf: vlanif20, out label: 3
    Nexthop addr: 20.1.1.2        cross connect ix: 2, op code: Push
```

4) Check the ILM table entries of OLT2.

```
Admin(config)#show mpls ilm-table
Show MPLS ILM table :
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC         ILM-ID  In-Label  Out-Label  In-Intf   Out-Intf  Nexthop    LSP-Type
 >    3.3.3.3/32  6       52481     3          N/A       vlanif20  20.1.1.2   LSP_DEFAULT
 >    1.1.1.1/32  8       52480     3          N/A       vlanif10  10.1.1.1   LSP_DEFAULT
```

3. Check the configuration result of OLT3.

1) Check the LDP parameters of OLT3.

```
Admin(config)#show ldp param
Show LDP :
Router ID                : 3.3.3.3
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
```

```
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 0           : 3.3.3.3 (in use)
Import BGP routes        : No
```

2) Check the LDP session states of OLT3, including states of local and remote sessions.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address          IF Name    My Role    State       KeepAlive
2.2.2.2                  vlanif20   Active     OPERATIONAL   30
1.1.1.1                  vlanif20   Active     OPERATIONAL   30
```

3) Check the FTN table entries from OLT3 to OLT1.

```
Admin(config)# show mpls ftn-table 1.1.1.1/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 1.1.1.1/32, id: 1, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, Stale: NO, out intf: vlanif20, out label: 52480
    Nexthop addr: 20.1.1.1        cross connect ix: 7, op code: Push
```

17.3 Configuring RSVP LSP

This section introduces the background information, network scenario, configuration flow and configuration example of the RSVP LSP.

17.3.1 Background Information

Resource Reservation Protocol (RSVP) is a signaling protocol that is used to reserve resources on a network. As a network control protocol, RSVP works at the transmission layer, but does not participate in the transmission of application data. The RSVP signaling can carry the constraint parameters such as the bandwidth of the LSP, certain explicit routes, and color.

MPLS RSVP sets up label switched path (LSP) tunnels along specified paths to reserve resources. This enables network traffic to avoid the node where congestion occurs to balance network traffic.

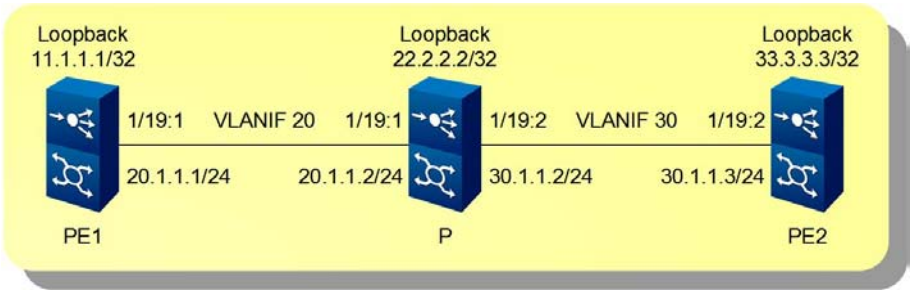
Dynamic LSPs can be created through RSVP on the AN6001-G16.

17.3.2 Network Scenario

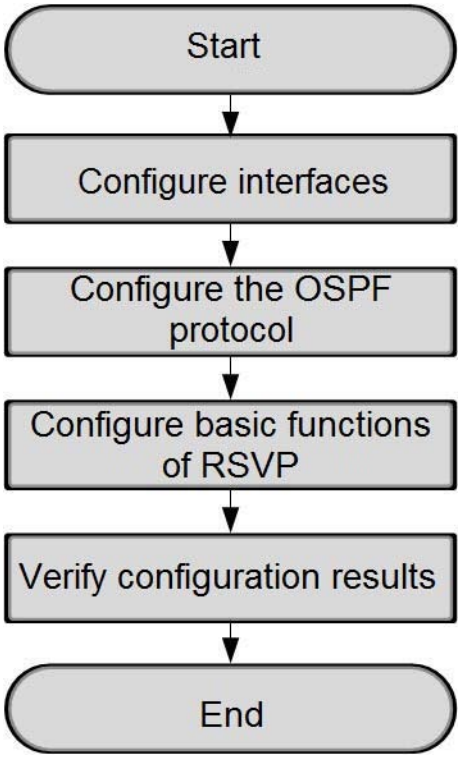
Service Planning

Three OLT devices are interconnected through uplink ports. Each sets up an adjacency and communicates with another through the OSPF protocol. PE1 and PE2 are edge routers on the backbone network. P is the core router on the backbone network. A public network tunnel is configured through RSVP between PE1 and PE2 to carry label services, and distribute and switch labels.

Network Diagram



17.3.3 Configuration Flow



17.3.4 Configuration Example

This section introduces how to configure the MPLS RSVP.

17.3.4.1 Configuring Interfaces

Configure interfaces on PE1, P and PE2.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
Start VLAN ID	Start VLAN ID of the uplink port	20	20	30	30

Parameter	Description	Example			
		PE1	P		PE2
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19	1/19	1/19
Port No.	Number of the uplink port	1	1	2	2
VLAN ID	VLAN ID of the VLANIF interface	20	20	30	30
VLANIF interface address	IPv4 address of the VLANIF interface	20.1.1.1	20.1.1.2	30.1.1.2	30.1.1.3
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Loopback interface address	IPv4 address of the loopback interface on the device	11.1.1.1	22.2.2.2		33.3.3.3
Subnet mask of the loopback interface address	Subnet mask of the IPv4 address of the loopback interface on the device	255.255.255.255	255.255.255.255		255.255.255.255

Procedure

1. Configure interface parameters for PE1.

```
Admin(config)#port vlan 20 tag 1/19 1
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.1 mask 255.255.255.0
Admin(config-vlanif-20)#exit
```

```
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 11.1.1.1 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

2. Configure interface parameters for P.

```
Admin(config)#port vlan 20 tag 1/19 1
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ip address 20.1.1.2 mask 255.255.255.0
Admin(config-vlanif-20)#exit
Admin(config)#port vlan 30 tag 1/19 2
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#ip address 30.1.1.2 mask 255.255.255.0
Admin(config-vlanif-30)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 22.2.2.2 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

3. Configure interface parameters for PE2.

```
Admin(config)#port vlan 30 tag 1/19 2
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#ipv4 address 30.1.1.3 mask 255.255.255.0
Admin(config-vlanif-30)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 33.3.3.3 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

17.3.4.2 Configuring the OSPF Protocol

Configure the OSPF protocol on PE1, P and PE2 to enable communications between devices on the backbone network.

Planning Data

Parameter	Description	Example		
		PE1	P	PE2
Instance number	OSPF instance number	1	1	1
Router ID	ID of the OSPF router, displayed in the format of an IP address	11.1.1.1	22.2.2.2	33.3.3.3

Parameter	Description	Example						
		PE1		P			PE2	
Interface network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	20.1.1.0	11.1.1.1	20.1.1.0	30.1.1.0	22.2.2.2	30.1.1.0	33.3.3.3
Subnet mask	Subnet mask	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.0
Domain IP address	IP address of the OSPF area to which the uplink port belongs. It is represented in dotted decimal notation.	0	0	0	0	0	0	0

Procedure

1. Configure the OSPF protocol for PE1.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 11.1.1.1
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 11.1.1.1 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

2. Configure the OSPF protocol for P.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 22.2.2.2
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 30.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 22.2.2.2 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

3. Configure the OSPF protocol for PE2.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 33.3.3.3
Admin(config-ospf-1)#network 30.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 33.3.3.3 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

4. Check the configuration result of the OSPF protocol.

1) PE1 can ping 33.3.3.3 successfully.

```
Admin(config)#ping 33.3.3.3
PING 33.3.3.3 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 33.3.3.3 : bytes=56: icmp_seq=0 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

2) PE2 can ping 11.1.1.1 successfully.

```
Admin(config)#ping 11.1.1.1
PING 11.1.1.1 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 11.1.1.1 : bytes=56: icmp_seq=0 ttl=63 time=10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

17.3.4.3 Configuring Basic Functions of RSVP

Configuring RSVP functions enables network traffic to avoid the node where congestion occurs to balance network traffic.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
VLAN ID	VLAN ID of the interface	20	20	30	30
Trunk name	Trunk name	test	-	-	test1
LSP egress node address	IPv4 address of the LSP egress node	33.3.3.3	-	-	11.1.1.1
LSP ingress node address	IPv4 address of the LSP ingress node	11.1.1.1	-	-	33.3.3.3

Procedure

1. Configure RSVP functions for PE1.

```
Admin(config)#router rsvp
```

```
Admin(config-rsvp)#cspf disable
Admin(config-rsvp)#exit
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#rsvp enable
Admin(config-vlanif-20)#exit
Admin(config)#rsvp-trunk test ipv4
Admin(config-rsvp-trunk-test)#to 33.3.3.3
Admin(config-rsvp-trunk-test)#from 11.1.1.1
Admin(config-rsvp-trunk-test)#exit
```

2. Configure RSVP functions for P.

```
Admin(config)#router rsvp
Admin(config-rsvp)#cspf disable
Admin(config-rsvp)#exit
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#rsvp enable
Admin(config-vlanif-20)#exit
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#mpls enable
Admin(config-vlanif-30)#rsvp enable
Admin(config-vlanif-30)#exit
```

3. Configure RSVP functions for PE2.

```
Admin(config)#router rsvp
Admin(config-rsvp)#cspf disable
Admin(config-rsvp)#exit
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#mpls enable
Admin(config-vlanif-30)#rsvp enable
Admin(config-vlanif-30)#exit
Admin(config)#rsvp-trunk test1 ipv4
Admin(config-rsvp-trunk-test1)#to 11.1.1.1
Admin(config-rsvp-trunk-test1)#from 33.3.3.3
Admin(config-rsvp-trunk-test1)#exit
```

17.3.4.4 Verifying Configuration Results

Check RSVP configuration results of PE1, P and PE2.

1. Check the RSVP session on PE1.

```
Admin(config)#show rsvp session
Ingress RSVP:
To        From      State  Pri Rt  Style Labelin  Labelout  LSPName  Direction
33.3.3.3  11.1.1.1  Up     Yes 1 1 SE    -        53120     test     Unidir
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
To        From      State  Pri Rt  Style Labelin  Labelout  LSPName  Direction
11.1.1.1  33.3.3.3  Up     Yes 1 1 SE    3        -         test1    Unidir
Total 1 displayed, Up 1, Down 0.
```

2. Check the RSVP session on P.

```
Admin(config)#show rsvp session
Transit RSVP:
To        From      State  Pri Rt  Style Labelin  Labelout  LSPName  Direction
11.1.1.1  33.3.3.3  Up     Yes 1 1 SE    53121    3         test1    Unidir
33.3.3.3  11.1.1.1  Up     Yes 1 1 SE    53120    3         test     Unidir
Total 2 displayed, Up 2, Down 0.
```

3. Check the RSVP session on PE2.

```
Admin(config)#show rsvp session
Ingress RSVP:
To        From      State  Pri Rt  Style Labelin  Labelout  LSPName  Direction
11.1.1.1  33.3.3.3  Up     Yes 1 1 SE    -        53121     test1    Unidir
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
To        From      State  Pri Rt  Style Labelin  Labelout  LSPName  Direction
33.3.3.3  11.1.1.1  Up     Yes 1 1 SE    3        -         test     Unidir
Total 1 displayed, Up 1, Down 0.
```

18 Configuring VPN

This chapter introduces how to configure the VPN services for the AN6001-G16.

- Configuring VPWS
- Configuring VPLS
- Configuring BGP / MPLS IPv4 VPN

18.1 Configuring VPWS

This section introduces the background information, network scenario, configuration flow and configuration example of the VPWS.

18.1.1 Background

Virtual Private Wire Service (VPWS) is a Layer 2 virtual private network (VPN) technology for point-to-point transmission. It implements one-to-one mappings between attachment circuits (ACs) and pseudo wires (PWs). By means of binding local ACs, PWs and the opposite ACs, the virtual circuits are formed to transparently transmit Layer 2 services between subscribers. As a virtual private line technology, the VPWS supports almost all the link layer protocols.

Concepts related to the VPWS network are as follows:

Concept	Description
AC	Attachment circuit, a connection between subscribers and service providers, that is, a link between a CE and a PE. The AC interfaces supported by the AN6001-G16 include uplink ports and PON ports.
PW	Pseudo wire or virtual link, a bidirectional virtual connection between two VSIs residing on two PEs. It consists of a pair of unidirectional MPLS VCs transmitting in opposite directions. It is also called “an emulated circuit”.
Tunnel	A connection between a local PE and a remote PE, used to transparently transmit data between PEs. A tunnel can carry multiple PWs.
PW signaling	A type of signaling protocol used to negotiate PWs.

The VPWS has the following features:

- Extended operators’ network functions and service capabilities. The operator only needs one network to provide MPLS L2VPN services. Besides, the VPWS uses the MPLS-related enhanced technologies, such as traffic engineering and QoS, to provide different services of different levels. This meets various customer demands.
- Higher scalability.

- In a non-MPLS ATM or FR network, Layer 2 VPN is provided by VC. For each AC, both the provider edge device (PE) and the provider core device (P) on the network need to maintain their complete VC information. Therefore, operators need to set up multiple VCs when they need to connect their devices to multiple CEs on a PE. Much VC information then needs to be maintained on PE and P devices.
- In an MPLS L2VPN network, multiple VCs share one LSP through the label stack technology. Therefore, only one LSP entry needs to be maintained on the P device. This improves scalability of the system.

- Clear division of management and responsibility. In an MPLS L2VPN network, operators only provide Layer 2 connectivity. Subscribers are responsible for Layer 3 connectivity, such as routing. If subscribers configure incorrectly and a route flap occurs, the stability of the operator's network is not affected.
- Multiple protocols supported. Since operators only provide Layer 2 connectivity, subscribers can use any of Layer 3 protocols, such as IPv4 and IPv6.
- Smooth upgrade of the network. With VPWS, subscribers do not even learn the existence of the MPLS L2VPN. When operators upgrade the network from the traditional Layer 2 VPN such as ATM and FR to the MPLS L2VPN, subscribers do not need to update any configurations, except that there may be data loss for a short time during network switching.

18.1.2 Network Scenario

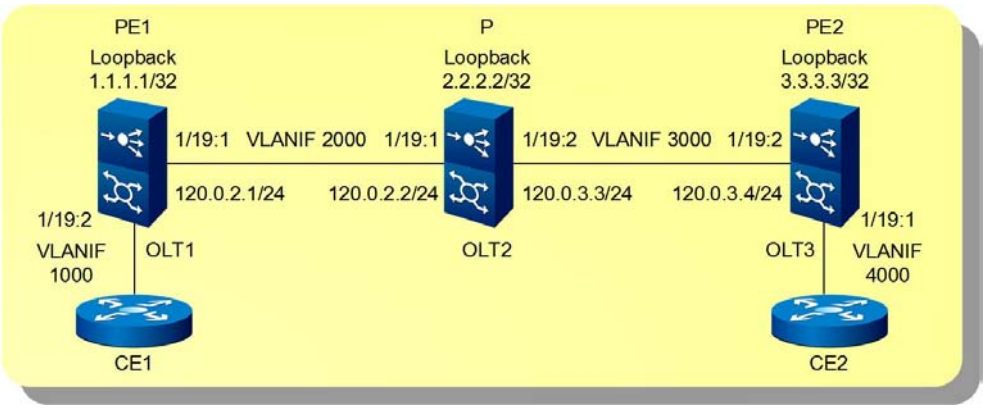
Service Planning

Three OLTs are interconnected through uplink ports. Each sets up an adjacency and communicates with another through the OSPF protocol. Serving as edge routers on the backbone network, PE1 and PE2 use uplink ports to connect to CE1 and CE2 respectively to access VPN services. P serves as the core router on the backbone network to achieve routing and expedited forwarding.

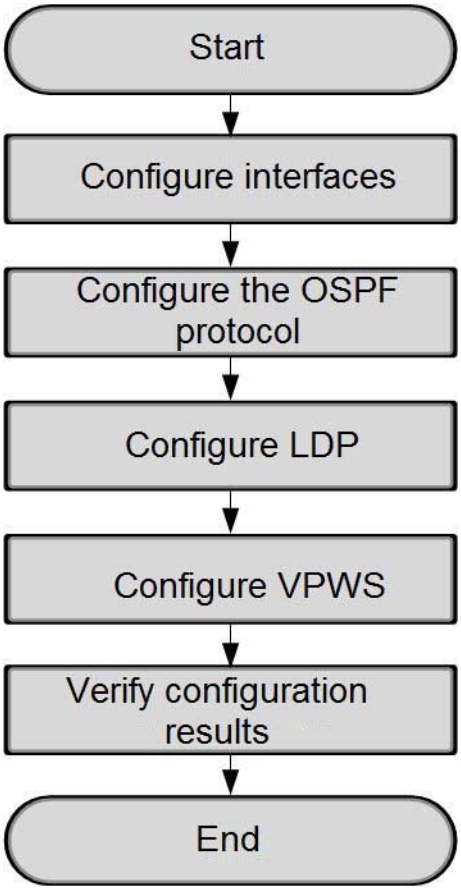
Note:

The AC interfaces supported by the AN6001-G16 include uplink ports and PON ports. In this scenario, the devices use the uplink ports as the AC interfaces.

Network Diagram



18.1.3 Configuration Flow



18.1.4 Configuration Example

This section introduces how to configure the VPWS.

18.1.4.1 Configuring Interfaces

Configure interfaces on PE1, P and PE2.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
Start VLAN ID	Start VLAN ID of the uplink interface	2000	2000	3000	3000

Parameter	Description	Example			
		PE1	P		PE2
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink interface resides	1/19	1/19	1/19	1/19
Port No.	Number of the uplink port	1	1	2	2
VLAN ID	VLAN ID of the VLANIF interface	2000	2000	3000	3000
VLANIF interface address	IPv4 address of the VLANIF interface	120.0.2.1	120.0.2.2	120.0.3.3	120.0.3.4
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Loopback interface address	IPv4 address of the loopback interface on the device	1.1.1.1	2.2.2.2		3.3.3.3
Subnet mask of the loopback interface address	Subnet mask of the IPv4 address of the loopback interface on the device	255.255.255.255	255.255.255.255		255.255.255.255

Procedure

1. Configure interface parameters for PE1.

```
Admin(config)#port vlan 2000 tag 1/19 1
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#ipv4 address 120.0.2.1 mask 255.255.255.0
Admin(config-vlanif-2000)#exit
```

```
Admin(config)#interface loopback 1
Admin(config-if-loopback-1)#ipv4 address 1.1.1.1 mask 255.255.255.255
Admin(config-if-loopback-1)#exit
```

2. Configure interface parameters for P.

```
Admin(config)#port vlan 2000 tag 1/19 1
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#ipv4 address 120.0.2.2 mask 255.255.255.0
Admin(config-vlanif-2000)#exit
Admin(config)#port vlan 3000 tag 1/19 2
Admin(config)#interface vlanif 3000
Admin(config-vlanif-3000)#ipv4 address 120.0.3.3 mask 255.255.255.0
Admin(config-vlanif-3000)#exit
Admin(config)#interface loopback 2
Admin(config-if-loopback-2)#ipv4 address 2.2.2.2 mask 255.255.255.255
Admin(config-if-loopback-2)#exit
```

3. Configure interface parameters for PE2.

```
Admin(config)#port vlan 3000 tag 1/19 2
Admin(config)#interface vlanif 3000
Admin(config-vlanif-3000)#ipv4 address 120.0.3.4 mask 255.255.255.0
Admin(config-vlanif-3000)#exit
Admin(config)#interface loopback 3
Admin(config-if-loopback-3)#ipv4 address 3.3.3.3 mask 255.255.255.255
Admin(config-if-loopback-3)#exit
```

18.1.4.2 Configuring the OSPF Protocol

Configure the OSPF protocol on PE1, P and PE2 to enable communications between devices on the backbone network.

Planning Data

Parameter	Description	Example		
		PE1	P	PE2
Instance number	OSPF instance number	10	10	10
Router ID	Router ID of the OSPF, displayed in the format of an IP address	1.1.1.1	2.2.2.2	3.3.3.3

Parameter	Description	Example						
		PE1		P			PE2	
Network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	120.0.2.0	1.1.1.1	120.0.2.0	120.0.3.0	2.2.2.2	120.0.3.0	3.3.3.3
Subnet mask	Subnet mask of the network IP address	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.0
Area No.	OSPF area number	0	0	0	0	0	0	0

Procedure

1. Configure the OSPF protocol for PE1.

```
Admin(config)#router ospf 10
Admin(config-ospf-10)#router-id 1.1.1.1
Admin(config-ospf-10)#network 120.0.2.0 0.0.0.255 area 0
Admin(config-ospf-10)#network 1.1.1.1 0.0.0.0 area 0
Admin(config-ospf-10)#exit
```

2. Configure the OSPF protocol for P.

```
Admin(config)#router ospf 10
Admin(config-ospf-10)#router-id 2.2.2.2
Admin(config-ospf-10)#network 120.0.2.0 0.0.0.255 area 0
Admin(config-ospf-10)#network 120.0.3.0 0.0.0.255 area 0
Admin(config-ospf-10)#network 2.2.2.2 0.0.0.0 area 0
Admin(config-ospf-10)#exit
```

3. Configure the OSPF protocol for PE2.

```
Admin(config)#router ospf 10
Admin(config-ospf-10)#router-id 3.3.3.3
Admin(config-ospf-10)#network 120.0.3.0 0.0.0.255 area 0
Admin(config-ospf-10)#network 3.3.3.3 0.0.0.0 area 0
Admin(config-ospf-10)#exit
```

18.1.4.3 Configuring LDP Sessions

Set up LDP sessions between PEs. If PEs are not directly connected, you need to set up MPLS LDP remote sessions.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
Router ID	Router identifier	1.1.1.1	2.2.2.2		3.3.3.3
LDP transport address	Source transport address in LDP Hello messages, in the format of an IPv4 address	1.1.1.1	2.2.2.2		3.3.3.3
VLAN ID	VLAN ID of the VLANIF interface	2000	2000	3000	3000
Interface LDP enabling	Enable the IP address format of the LDP for an interface	ipv4	ipv4		ipv4
LDP remote address	IP address of the targeted peer, in the format of an IPv4 address	3.3.3.3	-		1.1.1.1

Procedure

1. Configure LDP local and remote sessions for PE1.

```
Admin(config)#router ldp
Admin(config-router)#router-id 1.1.1.1
Admin(config-router)#transport-address ipv4 1.1.1.1
Admin(config-router)#exit
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#mpls enable
Admin(config-vlanif-2000)#ldp enable ipv4
Admin(config-vlanif-2000)#exit
Admin(config)#router ldp
Admin(config-router)#targeted-peer ipv4 3.3.3.3
Admin(config-router)#exit
```

2. Configure LDP local sessions for P.

```
Admin(config)#router ldp
Admin(config-router)#router-id 2.2.2.2
Admin(config-router)#transport-address ipv4 2.2.2.2
Admin(config-router)#exit
Admin(config)#interface vlanif 2000
Admin(config-vlanif-2000)#mpls enable
Admin(config-vlanif-2000)#ldp enable ipv4
Admin(config-vlanif-2000)#exit
Admin(config)#interface vlanif 3000
Admin(config-vlanif-3000)#mpls enable
Admin(config-vlanif-3000)#ldp enable ipv4
```

```
Admin(config-vlanif-3000)#exit
```

3. Configure LDP local and remote sessions for PE2.

```
Admin(config)#router ldp
Admin(config-router)#router-id 3.3.3.3
Admin(config-router)#transport-address ipv4 3.3.3.3
Admin(config-router)#exit
Admin(config)#interface vlanif 3000
Admin(config-vlanif-3000)#mpls enable
Admin(config-vlanif-3000)#ldp enable ipv4
Admin(config-vlanif-3000)#exit
Admin(config)#router ldp
Admin(config-router)#targeted-peer ipv4 1.1.1.1
Admin(config-router)#exit
```

18.1.4.4 Configuring VPWS Services

Set point-to-point connections so that PE devices can communicate with each other.

Planning Data

Parameter	Description	Example	
		PE1	PE2
VC name	Name of VPWS VC	test	test
VC ID	ID of VPWS VC	1	1
Peer IP	IPv4 address of the PW remote peer	3.3.3.3	1.1.1.1
PW encapsulation mode	◆ tagged: encapsulated in Tag mode ◆ raw: encapsulated in Raw mode	tagged	tagged
VLAN ID	VLAN ID of the AC interface	1000	4000
Tag processing mode of VLAN	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number of the card where the AC interface resides	1/19	1/19

Parameter	Description	Example	
		PE1	PE2
Port No.	Number of the AC port	2	1
AC access mode	Packet encapsulation mode for AC ◆ vlan: VLAN access ◆ ethernet: Ethernet access	vlan	vlan

Procedure

1. Configure VPWS services for PE1 and bind VPWS VC to the AC interface.

```
Admin(config)#mpls l2-circuit test 1 3.3.3.3 mode tagged
Admin(config)#port vlan 1000 tag 1/19 2
Admin(config)#interface vlanif 1000
Admin(config-vlanif-1000)#mpls-l2-circuit test vlan
Admin(config-vlanif-1000)#exit
```

2. Configure VPWS services for PE2 and bind VPWS VC to the AC interface.

```
Admin(config)#mpls l2-circuit test 1 1.1.1.1 mode tagged
Admin(config)#port vlan 4000 tag 1/19 1
Admin(config)#interface vlanif 4000
Admin(config-vlanif-4000)#mpls-l2-circuit test vlan
Admin(config-vlanif-4000)#exit
```

18.1.4.5 Verifying Configuration Results

Check VPWS configuration results for the three devices.

◆ Check the VPWS configuration results of PE1 and PE2, including the OSPF neighbor information, LDP session information, VC forwarding table and FTN table. The ways to verify the configuration results for PE1 and PE2 are the same. The following uses PE1 for example.

1) Check the OSPF neighbor information of PE1.

```
Admin(config)#show ipv4 ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID  Pri  State        Dead Time  Address    Interface   Instance ID
2.2.2.2        1  Full/Backup  00:00:32   120.0.2.2  vlanif2000      0
```

2) Check the LDP session information of PE1. The LDP sessions are set up between PE1 and PE2, and between PE1 and P. Both sessions are operational. Their adjacency relations are set up correctly.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address           IF Name    My Role    State       KeepAlive
3.3.3.3                   vlanif2000 Passive    OPERATIONAL   30
2.2.2.2                   vlanif2000 Passive    OPERATIONAL   30
```

3) Check the FTN table with mappings between PE1 and PE2. You can view the outer label information.

```
Admin(config)#show mpls ftn-table 3.3.3.3/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 3.3.3.3/32, id: 2, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, Stale: NO, out intf: vlanif2000, out label: 52481
    Nexthop addr: 120.0.2.2        cross connect ix: 2, op code: Push
```

4) Check the VPWS VC forwarding table of PE1. You can view the inner label information.

```
Admin(config)#show mpls vc-table
vc-table information :
VC-ID Vlan-ID Inner-Vlan-ID Access-Intf Network-Intf Out Label Tunnel-Label Tunnel-name Nexthop Status
111   1000    N/A           vlanif1000  vlanif2000   53762     52481        N/A         3.3.3.3 Active
```

- Check the configuration result of P, including the OSPF neighbor information, LDP session information, FTN table and ILM table.

1) Check the OSPF neighbor information of P.

```
Admin(config)#show ipv4 ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID  Pri  State        Dead Time  Address    Interface   Instance ID
1.1.1.1        1  Full/DR      00:00:32   120.0.2.1  vlanif2000      0
3.3.3.3        1  Full/DR      00:00:39   120.0.3.4  vlanif3000      0
```

2) Check the LDP session information of P. The LDP sessions are set up between P and PE1, and between P and PE2. Both sessions are operational. Their adjacency relations are set up correctly.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address           IF Name    My Role    State       KeepAlive
1.1.1.1                   vlanif2000 Active     OPERATIONAL   30
```

```
3.3.3.3                    vlanif3000 Passive    OPERATIONAL    30
```

3) Check the FTN table of P, including the FECs of PE1 and PE2.

```
Admin(config)#show mpls ftn-table
Show MPLS FTN table :
 Primary FTN entry with FEC: 1.1.1.1/32, id: 2, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,    Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 24, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, Stale: NO, out intf: vlanif2000, out label: 3
    Nexthop addr: 120.0.2.1        cross connect ix: 24, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 1, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,    Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 23, in intf: - in label: 0 out-segment ix: 5
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: LDP, Stale: NO, out intf: vlanif3000, out label: 3
    Nexthop addr: 120.0.3.4        cross connect ix: 23, op code: Push
```

Check the ILM table of P, including the FECs of PE1 and PE2.

```
Admin(config)#show mpls ilm-table
Show MPLS ILM table :
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC         ILM-ID  In-Label  Out-Label  In-Intf  Out-Intf    Nexthop     LSP-Type
 >    3.3.3.3/32  39      52481     3          N/A      vlanif3000  120.0.3.4   LSP_DEFAULT
 >    1.1.1.1/32  40      52480     3          N/A      vlanif2000  120.0.2.1   LSP_DEFAULT
```

18.2 Configuring VPLS

This section introduces the background information, network scenario, configuration flow and configuration example of the VPLS.

18.2.1 Background

Virtual Private LAN Service (VPLS) is a Layer 2 VPN technology for emulating a LAN. In VPLS, an NE can be regarded as a virtual switching instance (VSI) for each L2VPN. This VSI helps achieve many-to-many mappings between ACs and PWs, and connect multiple Ethernet LANs to enable them to work as one LAN. With such VPLS technology, service providers provide Ethernet-based multipoint services to subscribers through the MPLS backbone network.

Concepts related to the VPLS network are as follows:

Concept	Description
AC	Attachment circuit, a connection between subscribers and service providers, that is, a link between a CE and a PE. The AC interfaces supported by the AN6001-G16 include uplink ports and PON ports.
VSI	Virtual switch instance, an instance through which the physical access links of VPLS can be mapped to the virtual links. Each VSI provides an independent VPLS service. These services are then forwarded based on MAC addresses and VLAN tags as Layer 2 packets. The VSI works as an Ethernet bridge and can terminate a PW.
PW	Pseudo wire or virtual link, a bidirectional virtual connection between two VSIs residing on two PEs. It consists of a pair of unidirectional MPLS VCs transmitting in opposite directions. It is also called “an emulated circuit”.
Tunnel	A connection between a local PE and a remote PE, used to transparently transmit data between PEs. A tunnel can carry multiple PWs.

The VPLS has the following features:

- The VPLS integrates multiple technologies such as IP/MPLS and L2VPN Ethernet switching to support point-to-point, point-to-multipoint, and multipoint-to-multipoint services. It also supports carrier-class Ethernet services in large-scale networks.
- The VPLS uses Ethernet interfaces on the UNI side and helps deploy services fast and flexibly.
- The VPLS enables subscribers to control and maintain the route policy of the network, simplifying network management of operators.
- All the subscriber routers, that is, CEs, in a VPLS are on the same subnet, which makes it easier to plan IP addressing.
- Subscribers do not need to learn the existence of VPLS, or participate in IP addressing or routing.

18.2.2 Network Scenario

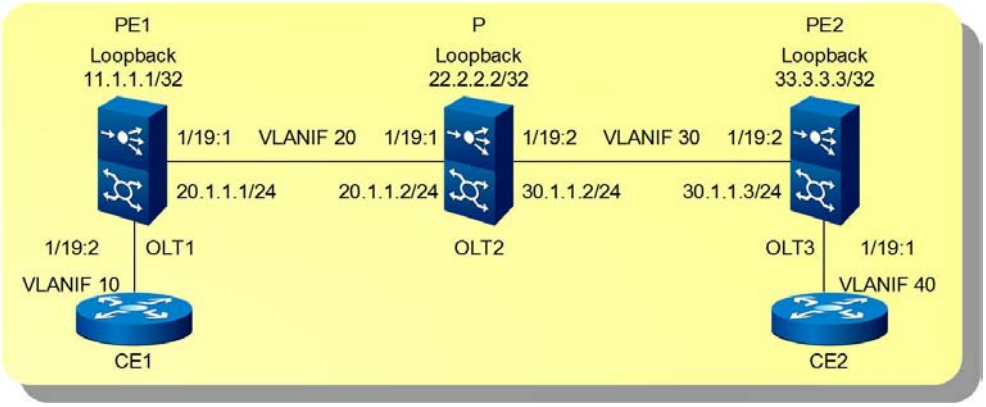
Service Planning

Three OLTs are interconnected through uplink ports. Each sets up an adjacency and communicates with another through the OSPF protocol. Serving as edge routers on the backbone network, PE1 and PE2 use uplink ports to connect to CE1 and CE2 respectively to access VPN services. P serves as the core router on the backbone network to achieve routing and expedited forwarding.

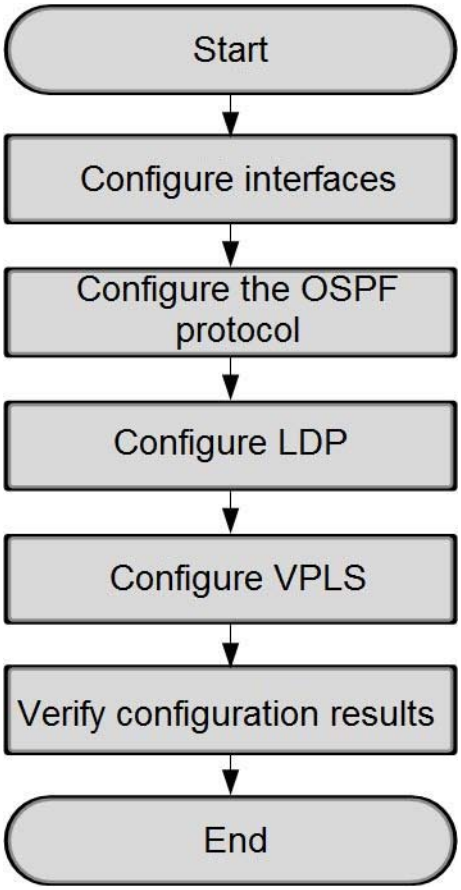
Note:

The AC interfaces supported by the AN6001-G16 include uplink ports and PON ports. In this scenario, the devices use the uplink ports as the AC interfaces.

Network Diagram



18.2.3 Configuration Flow



18.2.4 Configuration Example

This section introduces how to configure the VPLS.

18.2.4.1 Configuring Interfaces

Configure interfaces on PE1, P and PE2.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
Start VLAN ID	Start VLAN ID of the uplink port	20	20	30	30

Parameter	Description	Example			
		PE1	P		PE2
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19	1/19	1/19
Port No.	Number of the uplink port	1	1	2	1
VLAN ID	VLAN ID of the VLANIF interface	20	20	30	30
VLANIF interface address	IPv4 address of the VLANIF interface	20.1.1.1	20.1.1.2	30.1.1.2	30.1.1.3
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Loopback interface address	IPv4 address of the loopback interface on the device	11.1.1.1	22.2.2.2		33.3.3.3
Subnet mask of the loopback interface address	Subnet mask of the IPv4 address of the loopback interface on the device	255.255.255.255	255.255.255.255		255.255.255.255

Procedure

1. Configure interface parameters for PE1.

```
Admin(config)#port vlan 20 tag 1/19 1
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.1 mask 255.255.255.0
Admin(config-vlanif-20)#exit
```

```
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 11.1.1.1 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

2. Configure interface parameters for P.

```
Admin(config)#port vlan 20 tag 1/19 1
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#ipv4 address 20.1.1.2 mask 255.255.255.0
Admin(config-vlanif-20)#exit
Admin(config)#port vlan 30 tag 1/19 2
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#ipv4 address 30.1.1.2 mask 255.255.255.0
Admin(config-vlanif-30)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 22.2.2.2 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

3. Configure interface parameters for PE2.

```
Admin(config)#port vlan 30 tag 1/19 2
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#ipv4 address 30.1.1.1 mask 255.255.255.0
Admin(config-vlanif-30)#exit
Admin(config)#interface loopback 9
Admin(config-if-loopback-9)#ipv4 address 33.3.3.3 mask 255.255.255.255
Admin(config-if-loopback-9)#exit
```

18.2.4.2 Configuring the OSPF Protocol

Configure the OSPF protocol on PE1, P and PE2 to enable communications between devices on the backbone network.

Planning Data

Parameter	Description	Example		
		PE1	P	PE2
Instance number	OSPF instance number	1	1	1
Router ID	Router ID of the OSPF, displayed in the format of an IP address	11.1.1.1	22.2.2.2	33.3.3.3

Parameter	Description	Example						
		PE1		P			PE2	
Network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	20.1.1.0	11.1.1.1	20.1.1.0	30.1.1.0	22.2.2.2	30.1.1.0	33.3.3.3
Subnet mask	Subnet mask of the network IP address	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.0
Area No.	OSPF area number	0	0	0	0	0	0	0

Procedure

1. Configure the OSPF protocol for PE1.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 11.1.1.1
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 11.1.1.1 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

2. Configure the OSPF protocol for P.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 22.2.2.2
Admin(config-ospf-1)#network 20.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 30.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 22.2.2.2 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

3. Configure the OSPF protocol for PE2.

```
Admin(config)#router ospf 1
Admin(config-ospf-1)#router-id 33.3.3.3
Admin(config-ospf-1)#network 30.1.1.0 0.0.0.255 area 0
Admin(config-ospf-1)#network 33.3.3.3 0.0.0.0 area 0
Admin(config-ospf-1)#exit
```

4. Check the configuration result of the OSPF protocol.

   1) PE1 can ping 33.3.3.3 successfully.

```
Admin(config)#ping 33.3.3.3
PING 33.3.3.3 : 56 data bytes.
Press Ctrl-c to Stop.
```

```
Reply from 33.3.3.3 : bytes=56: icmp_seq=0 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 33.3.3.3 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

2) PE2 can ping 11.1.1.1 successfully.

```
Admin(config)#ping 11.1.1.1
PING 11.1.1.1 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 11.1.1.1 : bytes=56: icmp_seq=0 ttl=63 time=10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=1 ttl=63 time<10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=2 ttl=63 time<10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=3 ttl=63 time<10 ms
Reply from 11.1.1.1 : bytes=56: icmp_seq=4 ttl=63 time<10 ms
```

18.2.4.3 Configuring LDP Sessions

To enable communications between all the PEs in a VPLS network through PWs, you need to set up an LDP session between any two PEs. If PEs are not directly connected, you need to set up MPLS LDP remote sessions.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
Router ID	Router identifier	11.1.1.1	22.2.2.2		33.3.3.3
LDP transport address	Source transport address in LDP Hello messages, in the format of an IPv4 address	11.1.1.1	22.2.2.2		33.3.3.3
VLAN ID	VLAN ID of the VLANIF interface	20	20	30	30
Interface LDP enabling	Enable the IP address format of the LDP for an interface	ipv4	ipv4		ipv4
LDP remote address	IP address of the targeted peer, in the format of an IPv4 address	33.3.3.3	-		11.1.1.1

Procedure

1. Configure LDP local and remote sessions for PE1.

```
Admin(config)#router ldp
```

```
Admin(config-router)#router-id 11.1.1.1
Admin(config-router)#transport-address ipv4 11.1.1.1
Admin(config-router)#exit
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#ldp enable ipv4
Admin(config-vlanif-20)#exit
Admin(config)#router ldp
Admin(config-router)#targeted-peer ipv4 33.3.3.3
Admin(config-router)#exit
```

2. Configure LDP local sessions for P.

```
Admin(config)#router ldp
Admin(config-router)#router-id 22.2.2.2
Admin(config-router)#transport-address ipv4 22.2.2.2
Admin(config)#interface vlanif 20
Admin(config-vlanif-20)#mpls enable
Admin(config-vlanif-20)#ldp enable ipv4
Admin(config-vlanif-20)#exit
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#mpls enable
Admin(config-vlanif-30)#ldp enable ipv4
Admin(config-vlanif-30)#exit
```

3. Configure LDP local and remote sessions for PE2.

```
Admin(config)#router ldp
Admin(config-router)#router-id 33.3.3.3
Admin(config-router)#transport-address ipv4 33.3.3.3
Admin(config-router)#exit
Admin(config)#interface vlanif 30
Admin(config-vlanif-30)#mpls enable
Admin(config-vlanif-30)#ldp enable ipv4
Admin(config-vlanif-30)#exit
Admin(config)#router ldp
Admin(config-router)#targeted-peer ipv4 11.1.1.1
Admin(config-router)#exit
```

18.2.4.4 Configuring VPLS Services

Create a VPLS instance and bind an AC interface on a PE to it. In this way, traffic on a CE can connect to the VPLS network through this AC interface.

Planning Data

Parameter	Description	Example	
		PE1	PE2
Instance name	Name of the VPLS instance	test	test
Instance ID	ID of the VPLS instance	2	2
Peer IP	IP address of the PW remote peer	33.3.3.3	11.1.1.1
VLAN ID	VLAN ID of the AC interface	10	40
Tag processing mode of VLAN	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag
Subrack No./slot No.	Subrack number and slot number of the card where the AC interface resides	1/19	1/19
Port No.	Number of the AC port	2	1
AC access mode	Packet encapsulation mode for AC ◆ vlan: VLAN access ◆ ethernet: Ethernet access	vlan	vlan

Procedure

1. Configure VPLS services for PE1.

```
Admin(config)#mpls vpls test 2
Admin(config-vpls-test)#signaling ldp
Admin(config-vpls-ldpsig-test)#vpls-peer 33.3.3.3
Admin(config-vpls-ldpsig-test)#exit
Admin(config-vpls-test)#exit
Admin(config)#port vlan 10 tag 1/19 2
Admin(config)#interface vlanif 10
Admin(config-vlanif-10)#mpls-vpls test vlan
Admin(config-vlanif-10)#exit
```

2. Configure VPLS services for PE2.

```
Admin(config)#mpls vpls test 2
Admin(config-vpls-test)#signaling ldp
Admin(config-vpls-ldpsig-test)#vpls-peer 11.1.1.1
```

```
Admin(config-vpls-ldpsig-test)#exit
Admin(config-vpls-test)#exit
Admin(config)#port vlan 40 tag 1/19 1
Admin(config)#interface vlanif 40
Admin(config-vlanif-40)#mpls-vpls test vlan
Admin(config-vlanif-40)#exit
```

18.2.4.5 Verifying Configuration Results

Check VPLS configuration results of the three devices.

- Check the VPLS configuration results of PE1 and PE2, including the OSPF neighbor information, LDP session information, VPLS label forwarding information and FTN table. The ways to verify the configuration results for PE1 and PE2 are the same. The following uses PE1 for example.

  1) Check the OSPF neighbor information of PE1.

```
Admin(config)#show ipv4 ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID  Pri  State        Dead Time  Address    Interface   Instance ID
22.2.2.2       1  Full/Backup  00:00:31   20.1.1.2   vlanif20        0
```

  2) Check the LDP session information of PE1. The LDP sessions are set up between PE1 and PE2, and between PE1 and P. Both sessions are operational. Their adjacency relations are set up correctly.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address           IF Name    My Role    State       KeepAlive
33.3.3.3                  vlanif20   Passive   OPERATIONAL   30
22.2.2.2                  vlanif20   Passive   OPERATIONAL   30
```

  3) Check the FTN table with mappings between PE1 and PE2. You can view the outer label information.

```
Admin(config)#show mpls ftn-table 33.3.3.3/32
Show MPLS FTN table :
 Primary FTN entry with FEC: 33.3.3.3/32, id: 3, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,    Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, Stale: NO, out intf: vlanif20, out label: 52481
    Nexthop addr: 20.1.1.2        cross connect ix: 2, op code: Push
```

4) Check the VPLS label forwarding information of PE1. You can view the inner label information.

```
Admin(config)#show mpls vpls mesh
vpls mesh information :
VPLS-ID Peer Addr Tunnel-Label Tunnel-name In-Label Network-Intf Out-Label Lkps/St PW-INDEX SIG-Protocol Status
123     33.3.3.3  52481        N/A         52483    vlanif20     53763     2/Up    2        LDP          Active
```

- Check the configuration result of P, including the OSPF neighbor information, LDP session information, FTN table and ILM table.

1) Check the OSPF neighbor information of P.

```
Admin(config)#show ipv4 ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID  Pri  State        Dead Time  Address    Interface   Instance ID
11.1.1.1       1  Full/DR      00:00:35   20.1.1.1   vlanif20        0
33.3.3.3       1  Full/Backup  00:00:31   30.1.1.3   vlanif30        0
```

2) Check the LDP session information of P. The LDP sessions are set up between P and PE1, and between P and PE2. Both sessions are operational. Their adjacency relations are set up correctly.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address          IF Name    My Role    State       KeepAlive
33.3.3.3                 vlanif30   Passive    OPERATIONAL   30
11.1.1.1                 vlanif20   Active     OPERATIONAL   30
```

3) Check the FTN table of P, including the FECs of PE1 and PE2.

```
Admin(config)#show mpls ftn-table
Show MPLS FTN table :
 Primary FTN entry with FEC: 1.1.1.1/32, id: 2, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 24, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, Stale: NO, out intf: vlanif2000, out label: 3
    Nexthop addr: 120.0.2.1        cross connect ix: 24, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 1, row status: Active, state: Installed
  Owner: LDP, Stale: NO, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
  Primary:  Cross connect ix: 23, in intf: - in label: 0 out-segment ix: 5
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: LDP, Stale: NO, out intf: vlanif3000, out label: 3
    Nexthop addr: 120.0.3.4        cross connect ix: 23, op code: Push
```

4) Check the ILM table of P, including the FECs of PE1 and PE2.

```
Admin(config)#show mpls ilm-table
Show MPLS ILM table :
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC          ILM-ID  In-Label  Out-Label  In-Intf  Out-Intf   Nexthop    LSP-Type
 >    33.3.3.3/32 42      52481     3          N/A      vlanif30   30.1.1.3   LSP_DEFAULT
 >    11.1.1.1/32 41      52480     3          N/A      vlanif20   20.1.1.1   LSP_DEFAULT
```

18.3 Configuring BGP / MPLS IPv4 VPN

This section introduces the background information, network scenario, configuration flow and configuration example of the BGP / MPLS IPv4 VPN routing protocol.

18.3.1 Background Information

BGP/MPLS IPv4 VPN is a type of Layer 3 virtual private networks (L3VPN). It uses the border gateway protocol (BGP) to advertise VPN routes and uses multiprotocol label switch (MPLS) to forward VPN packets on backbone networks of service providers (SPs).

BGP/MPLS IPv4 VPN consists of CE, PE and P.

- CE (Customer Edge): It provides interfaces for direct connection to the service provider (SP) network. A CE can be a router, switch, or host. Usually, CE does not learn the existence of VPN. It does not support MPLS, either.
- PE (Provider Edge): It refers to an edge device on the service provider network, which is directly connected to the CE. In MPLS networks, all the operations related to VPN are performed on PEs. This requires high performance of PEs.
- P (Provider): It refers to a backbone device on the service provider's network, which is not directly connected to CEs. Ps only need to have the basic MPLS forwarding capability, and do not need to maintain the VPN information.

PEs and Ps are managed by service providers. CE devices are normally managed by subscribers, unless subscribers authorize the management privilege to the service provider. A PE device can connect to multiple CE devices. A CE device can connect to multiple PE devices provided by one or different service providers.

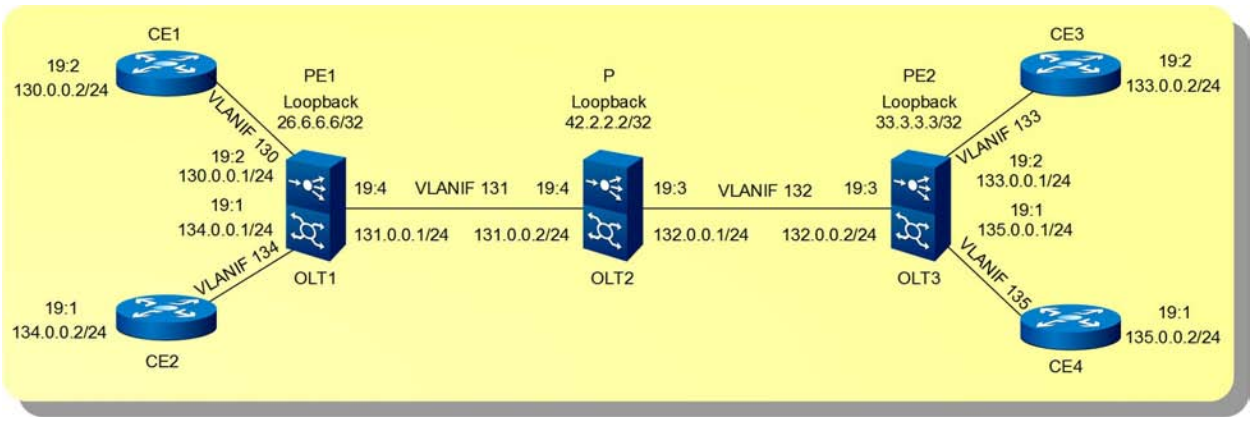
18.3.2 Network Scenario

Service Planning

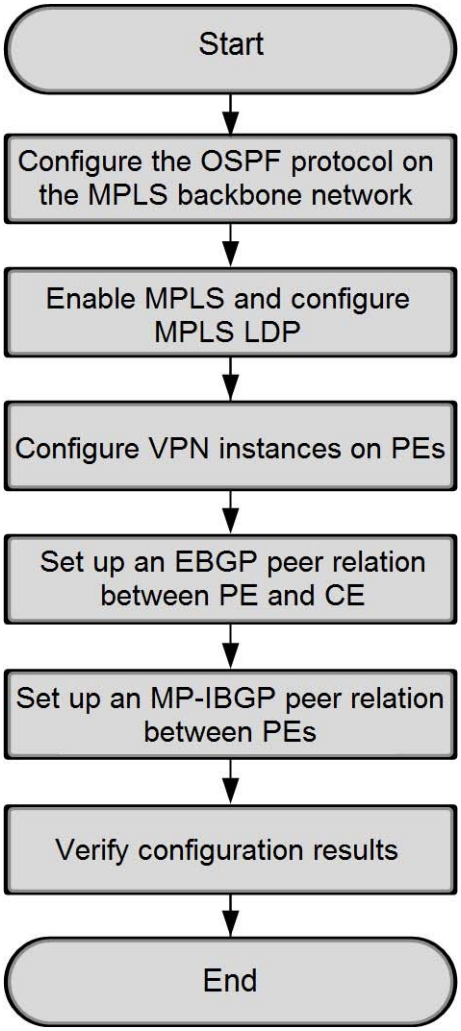
Three OLTs serve as PE1, P and PE2, respectively. They are interconnected with each other through uplink ports. PE1 and PE2 are edge routers on the backbone network. PE1 connects to CE1 and CE2 through uplink ports. PE2 connects to CE3 and CE4 through uplink ports. As the core router on the backbone network, P implements routing and expedited forwarding. CE1 and CE3, belonging to vpna, connect to the research and development area of the headquarter and that of the branch respectively. CE2 and CE4, belonging to vpnb, connect to the non-research and development area of the headquarter and that of the branch respectively. Deploying BGP/MPLS IP VPN enables safe intercommunication between the headquarter and the branches. This deployment also isolates the data in the research and development area from that in the non-research and development area.

1. Configure the OSPF protocol on PE1, P and PE2 to enable communications between devices on the backbone network.
2. Enable MPLS on PE1, P and PE2 and configure MPLS LDP protocols. Then, the MPLS LSP public tunnels are set up to transmit VPN data.
3. Configure VPN instances on PE1 and PE2. The VPN-target attributes of vpna and vpnb are 111:1 and 222:2, respectively. This enables data communication within a VPN and data isolation among different VPNs. Meanwhile, bind the ports connected to CEs to the corresponding VPN instances to connect VPN subscribers.
4. Configure EBGP between PEs and CEs to exchange VPN routing information.
5. Configure MP-IBGP between PE1 and PE2 to exchange VPN routing information.

Network Diagram



18.3.3 Configuration Flow



18.3.4 Configuration Example

This section introduces how to configure the BGP/MPLS IPv4 VPN.

18.3.4.1 Configuring the OSPF Protocol on the MPLS Backbone Network

Configure interfaces and the OSPF protocol for PE1, P and PE2. In this way, devices on the backbone network communicate with each other.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
Start VLAN ID	Start VLAN ID of the uplink port	131	131	132	132
End VLAN ID	End VLAN ID of the uplink port	-	-	-	-
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag
Subrack No. /slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19	1/19	1/19

Parameter	Description	Example						
		PE1		P			PE2	
Uplink port number	Uplink port number	4		4	3		3	
VLAN ID	VLAN ID of the VLANIF interface	131		131	132		132	
VLANIF interface address	IPv4 address of the VLANIF interface	131.0.0.1		131.0.0.2	132.0.0.1		132.0.0.2	
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0		255.255.255.0	255.255.255.0		255.255.255.0	
Loopback interface address	IPv4 address of the loopback interface on the device	26.6.6.6		42.2.2.2			33.3.3.3	
Subnet mask of the loopback interface address	Subnet mask of the IPv4 address of the loopback interface on the device	255.255.255.255		255.255.255.255			255.255.255.255	
OSPF route process ID	OSPF route process ID	130		130			130	
Network IP address	Network IP address of the interface that needs to run the OSPF protocol. This network should be an IP network configured with VLANIF interfaces.	131.0.0.0	26.6.6.6	131.0.0.0	132.0.0.0	42.2.2.2	132.0.0.0	33.3.3.3
Subnet mask	Subnet mask of the network IP address	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.255	0.0.0.0	0.0.0.255	0.0.0.0
Area No.	OSPF area number	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Procedure

- Configure interfaces and the OSPF protocol for PE1.

  1) Configure interface parameters for PE1.

```
Admin(config)#port vlan 131 tag 1/19 4
Admin(config)#interface vlanif 131
```

```
Admin(config-vlanif-131)#ipv4 address 131.0.0.1 mask 255.255.255.0
Admin(config-vlanif-131)#exit
Admin(config)#interface loopback 1
Admin(config-if-loopback-1)#ipv4 address 26.6.6.6 mask 255.255.255.255
Admin(config-if-loopback-1)#exit
Admin(config)#
```

2) Configure the OSPF protocol for PE1.

```
Admin(config)#router ospf 130
Admin(config-ospf-130)#network 131.0.0.0 0.0.0.255 area 0.0.0.0
Admin(config-ospf-130)#network 26.6.6.6 0.0.0.0 area 0.0.0.0
Admin(config-ospf-130)#exit
Admin(config)#
```

◆ Configure interfaces and the OSPF protocol for P.

1) Configure interface parameters for P.

```
Admin(config)#port vlan 131 tag 1/19 4
Admin(config)#interface vlanif 131
Admin(config-vlanif-131)#ipv4 address 131.0.0.2 mask 255.255.255.0
Admin(config-vlanif-131)#exit
Admin(config)#port vlan 132 tag 1/19 3
Admin(config)#interface vlanif 132
Admin(config-vlanif-132)#ipv4 address 132.0.0.1 mask 255.255.255.0
Admin(config-vlanif-132)#exit
Admin(config)#interface loopback 1
Admin(config-if-loopback-1)#ipv4 address 42.2.2.2 mask 255.255.255.255
Admin(config-if-loopback-1)#exit
Admin(config)#
```

2) Configure the OSPF protocol for P.

```
Admin(config)#router ospf 130
Admin(config-ospf-130)#network 131.0.0.0 0.0.0.255 area 0.0.0.0
Admin(config-ospf-130)#network 132.0.0.0 0.0.0.255 area 0.0.0.0
Admin(config-ospf-130)#network 42.2.2.2 0.0.0.0 area 0.0.0.0
Admin(config-ospf-130)#exit
Admin(config)#
```

◆ Configure interface parameters and the OSPF protocol for PE2.

1) Configure interface parameters for PE2.

```
Admin(config)#port vlan 132 tag 1/19 3
Admin(config)#interface vlanif 132
Admin(config-vlanif-132)#ipv4 address 132.0.0.2 mask 255.255.255.0
Admin(config-vlanif-132)#exit
Admin(config)#interface loopback 1
```

```
Admin(config-if-loopback-1)#ipv4 address 33.3.3.3 mask 255.255.255.255
Admin(config-if-loopback-1)#exit
Admin(config)#
```

2) Configure the OSPF protocol for PE2.

```
Admin(config)#router ospf 130
Admin(config-ospf-130)#network 132.0.0.0 0.0.0.255 area 0.0.0.0
Admin(config-ospf-130)#network 33.3.3.3 0.0.0.0 area 0.0.0.0
Admin(config-ospf-130)#exit
Admin(config)#
```

18.3.4.2 Enabling MPLS and Configuring MPLS LDP

Enable MPLS on PE1, P and PE2 and configure MPLS LDP protocols. Then, the MPLS LSP public tunnels are set up to transmit VPN data.

Planning Data

Parameter	Description	Example			
		PE1	P		PE2
VLAN ID	VLAN ID of the VLANIF interface	131	131	132	132
Router ID	Router identifier	26.6.6.6	42.2.2.2		33.3.3.3
LDP transport address	Source transport address in LDP Hello messages, in the format of an IPv4 address	26.6.6.6	42.2.2.2		33.3.3.3
Interface LDP enabling	Enable the IP address format of the LDP for an interface	ipv4	ipv4		ipv4

Procedure

◆ Enable MPLS and configure MPLS LDP for PE1.

```
Admin(config)#interface vlanif 131
Admin(config-vlanif-131)#mpls enable
Admin(config-vlanif-131)#exit
Admin(config)#router ldp
Admin(config-router)#router-id 26.6.6.6
Admin(config-router)#transport-address ipv4 26.6.6.6
Admin(config-router)#exit
Admin(config)#interface vlanif 131
Admin(config-vlanif-131)#ldp enable ipv4
Admin(config-vlanif-131)#exit
```

```
Admin(config)#
```

◆ Enable MPLS and configure MPLS LDP for P.

```
Admin(config)#interface vlanif 131
Admin(config-vlanif-131)#mpls enable
Admin(config-vlanif-131)#exit
Admin(config)#interface vlanif 132
Admin(config-vlanif-132)#mpls enable
Admin(config-vlanif-132)#exit
Admin(config)#router ldp
Admin(config-router)#router-id 42.2.2.2
Admin(config-router)#transport-address ipv4 42.2.2.2
Admin(config-router)#exit
Admin(config)#interface vlanif 131
Admin(config-vlanif-131)#ldp enable ipv4
Admin(config-vlanif-131)#exit
Admin(config)#interface vlanif 132
Admin(config-vlanif-132)#ldp enable ipv4
Admin(config-vlanif-132)#exit
Admin(config)#
```

◆ Enable MPLS and configure MPLS LDP for PE2.

```
Admin(config)#interface vlanif 132
Admin(config-vlanif-132)#mpls enable
Admin(config-vlanif-132)#exit
Admin(config)#router ldp
Admin(config-router)#router-id 33.3.3.3
Admin(config-router)#transport-address ipv4 33.3.3.3
Admin(config-router)#exit
Admin(config)#interface vlanif 132
Admin(config-vlanif-132)#ldp enable ipv4
Admin(config-vlanif-132)#exit
Admin(config)#
```

18.3.4.3 Configuring VPN Instances on PEs

Configure VPN instances on PE1 and PE2, and connect CEs to PEs.

Planning Data

Parameter	Description	Example			
		PE1		PE2	
VPN route forwarding instance	Name of the VPN route forwarding instance	vpna	vpnb	vpna	vpnb
RD value	An exclusive RD value for VRF	100:1	100:2	200:1	200:2
import extended community attribute	Extended community attribute of the route in the ingress direction	111:1	222:2	111:1	222:2
export extended community attribute	Extended community attribute of the route to the destination VPN in the egress direction	111:1	222:2	111:1	222:2
VLAN ID	VLAN ID of the VLANIF interface	130	134	133	135
VLANIF interface address	IPv4 address of the VLANIF interface	130.0.0.1	134.0.0.1	133.0.0.1	135.0.0.1
Subnet mask of the VLANIF interface address	Subnet mask of the IPv4 address of the VLANIF interface	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Start VLAN ID	Start VLAN ID of the uplink port	130	134	133	135
End VLAN ID	End VLAN ID of the uplink port	-	-	-	-
VLAN tag processing for uplink services	◆ untag: In this mode, tags of uplink packets are stripped automatically when they pass a port and the packets are further transmitted in untagged mode, while downlink untagged packets are added with corresponding tags when they pass the port. ◆ tag: In this mode, tags of the uplink / downlink data packets are not processed when they pass the port.	tag	tag	tag	tag

Parameter	Description	Example			
		PE1		PE2	
Subrack No./slot No.	Subrack number and slot number for the card where the uplink port resides	1/19	1/19	1/19	1/19
Uplink port number	Uplink port number	2	1	2	1

Procedure

- Configure the interface and VPN instance for PE1.
  - Configure the interface and VPN instance for PE1, and connect CE1 to PE1.

```
Admin(config)#ip vrf vpna
Admin(config-vrf-vpna-1)#rd 100:1
Admin(config-vrf-vpna-1)#route-target import 111:1
Admin(config-vrf-vpna-1)#route-target export 111:1
Admin(config-vrf-vpna-1)#exit
Admin(config)#interface vlanif 130
Admin(config-vlanif-130)#ip vrf forwarding vpna
Admin(config-vlanif-130)#ipv4 address 130.0.0.1 mask 255.255.255.0
Admin(config-vlanif-130)#exit
Admin(config)#port vlan 130 tag 1/19 2
Admin(config)#
```

  - Configure the interface and VPN instance for PE1, and connect CE2 to PE1.

```
Admin(config)#ip vrf vpnb
Admin(config-vrf-vpnb-1)#rd 100:2
Admin(config-vrf-vpnb-1)#route-target import 222:2
Admin(config-vrf-vpnb-1)#route-target export 222:2
Admin(config-vrf-vpnb-1)#exit
Admin(config)#interface vlanif 134
Admin(config-vlanif-134)#ip vrf forwarding vpnb
Admin(config-vlanif-134)#ipv4 address 134.0.0.1 mask 255.255.255.0
Admin(config-vlanif-134)#exit
Admin(config)#port vlan 134 tag 1/19 1
Admin(config)#
```

- Configure the interface and VPN instance for PE2.
  - Configure the interface and VPN instance for PE2, and connect CE3 to PE2.

```
Admin(config)#ip vrf vpna
```

```
Admin(config-vrf-vpna-1)#rd 200:1
Admin(config-vrf-vpna-1)#route-target import 111:1
Admin(config-vrf-vpna-1)#route-target export 111:1
Admin(config-vrf-vpna-1)#exit
Admin(config)#interface vlanif 133
Admin(config-vlanif-133)#ip vrf forwarding vpna
Admin(config-vlanif-133)#ipv4 address 133.0.0.1 mask 255.255.255.0
Admin(config-vlanif-133)#exit
Admin(config)#port vlan 133 tag 1/19 2
Admin(config)#
```

- Configure the interface and VPN instance for PE2, and connect CE4 to PE2.

```
Admin(config)#ip vrf vpnb
Admin(config-vrf-vpnb-1)#rd 200:2
Admin(config-vrf-vpnb-1)#route-target import 222:2
Admin(config-vrf-vpnb-1)#route-target export 222:2
Admin(config-vrf-vpnb-1)#exit
Admin(config)#interface vlanif 135
Admin(config-vlanif-135)#ip vrf forwarding vpnb
Admin(config-vlanif-135)#ipv4 address 135.0.0.1 mask 255.255.255.0
Admin(config-vlanif-135)#exit
Admin(config)#port vlan 135 tag 1/19 1
Admin(config)#
```

18.3.4.4 Setting up an EBGP Peer Relation Between PE and CE

Set up an EBGP peer relation between PE and CE to create a VPN route.

Planning Data

Parameter	Description	Example							
		PE1		PE2		CE1	CE2	CE3	CE4
AS number	AS number. Value range: 1 to 4294967295	65210		65210		65200	45200	55200	35200
VPN route forwarding instance	Name of the VPN route forwarding instance	vpna	vpnb	vpna	vpnb	-	-	-	-
BGP peer	IP address of the BGP neighbor, in the format of an IPv4 address	130.0.0.2	134.0.0.2	133.0.0.2	135.0.0.2	130.0.0.1	134.0.0.1	133.0.0.1	135.0.0.1

Parameter	Description	Example							
		PE1		PE2		CE1	CE2	CE3	CE4
	IP address of the BGP neighbor, in the format of an IPv6 address	-	-	-	-	-	-	-	-
	Remote AS number of the BGP peer. Value range: 1 to 4294967295	65200	45200	55200	35200	65210	65210	65210	65210

Procedure

◆ Configure the BGP protocol for PE1.

```
Admin(config)#router bgp 65210
Admin(config-bgp-65210)#address-family ipv4 vrf vpna
Admin(config-bgp-65210-ipv4-vpna)#redistribute connected
Admin(config-bgp-65210-ipv4-vpna)#neighbor 130.0.0.2 remote-as 65200
Admin(config-bgp-65210-ipv4-vpna)#neighbor 130.0.0.2 activate
Admin(config-bgp-65210-ipv4-vpna)#exit
Admin(config-bgp-65210)#address-family ipv4 vrf vpnb
Admin(config-bgp-65210-ipv4-vpnb)#address-family ipv4 vrf vpnb
Admin(config-bgp-65210-ipv4-vpnb)#redistribute connected
Admin(config-bgp-65210-ipv4-vpnb)#neighbor 134.0.0.2 remote-as 45200
Admin(config-bgp-65210-ipv4-vpnb)#neighbor 134.0.0.2 activate
Admin(config-bgp-65210-ipv4-vpnb)#exit
Admin(config-bgp-65210)#exit
Admin(config)#
```

◆ Configure the BGP protocol for PE2.

```
Admin(config)#router bgp 65210
Admin(config-bgp-65210)#address-family ipv4 vrf vpna
Admin(config-bgp-65210-ipv4-vpna)#redistribute connected
Admin(config-bgp-65210-ipv4-vpna)#neighbor 133.0.0.2 remote-as 55200
Admin(config-bgp-65210-ipv4-vpna)#neighbor 133.0.0.2 activate
Admin(config-bgp-65210-ipv4-vpna)#exit
Admin(config-bgp-65210)#address-family ipv4 vrf vpnb
Admin(config-bgp-65210-ipv4-vpnb)#redistribute connected
Admin(config-bgp-65210-ipv4-vpnb)#neighbor 135.0.0.2 remote-as 35200
Admin(config-bgp-65210-ipv4-vpnb)#neighbor 135.0.0.2 activate
Admin(config-bgp-65210-ipv4-vpnb)#exit
Admin(config-bgp-65210)#exit
```

```
Admin(config)#
```

◆ Configure the BGP protocol for CE1.

```
Admin(config)#router bgp 65200
Admin(config-bgp-65200)#neighbor 130.0.0.1 remote-as 65210
Admin(config-bgp-65200)#address-family ipv4
Admin(config-bgp-65200-ipv4)#redistribute connected
Admin(config-bgp-65200-ipv4)#exit
Admin(config-bgp-65200)#exit
Admin(config)#
```

◆ Configure the BGP protocol for CE2.

```
Admin(config)#router bgp 45200
Admin(config-bgp-45200)#neighbor 134.0.0.1 remote-as 65210
Admin(config-bgp-45200)#address-family ipv4
Admin(config-bgp-45200-ipv4)#redistribute connected
Admin(config-bgp-45200-ipv4)#exit
Admin(config-bgp-45200)#exit
Admin(config)#
```

◆ Configure the BGP protocol for CE3.

```
Admin(config)#router bgp 55200
Admin(config-bgp-55200)#neighbor 133.0.0.1 remote-as 65210
Admin(config-bgp-55200)#address-family ipv4
Admin(config-bgp-55200-ipv4)#redistribute connected
Admin(config-bgp-55200-ipv4)#exit
Admin(config-bgp-55200)#exit
Admin(config)#
```

◆ Configure the BGP protocol for CE4.

```
Admin(config)#router bgp 35200
Admin(config-bgp-35200)#neighbor 135.0.0.1 remote-as 65210
Admin(config-bgp-35200)#address-family ipv4
Admin(config-bgp-35200-ipv4)#redistribute connected
Admin(config-bgp-35200-ipv4)#exit
Admin(config-bgp-35200)#exit
Admin(config)#
```

18.3.4.5 Setting up an MP-IBGP Peer Relation Between PEs

Set up an MP-IBGP peer relation between PE1 and PE2 to exchange VPN route information.

Planning Data

Parameter	Description	Example	
		PE1	PE2
AS number	AS number. Value range: 1 to 4294967295	65210	65210
BGP peer	IP address of the BGP neighbor, in the format of an IPv4 address	33.3.3.3	26.6.6.6
	IP address of the BGP neighbor, in the format of an IPv6 address	-	-
	Remote AS number of the BGP peer. Value range: 1 to 4294967295	65210	65210
Packet transmission source IP address	IP address of the packet transmission source for the BGP neighbor	26.6.6.6	33.3.3.3

Procedure

- Configure the BGP protocol for PE1.

```
Admin(config)#router bgp 65210
Admin(config-bgp-65210)#neighbor 33.3.3.3 remote-as 65210
Admin(config-bgp-65210)#neighbor 33.3.3.3 update-source 26.6.6.6
Admin(config-bgp-65210)#address-family vpnv4 unicast
Admin(config-bgp-65210-vpnv4)#neighbor 33.3.3.3 activate
Admin(config-bgp-65210-vpnv4)#exit
Admin(config-bgp-65210)#exit
Admin(config)#
```

- Configure the BGP protocol for PE2.

```
Admin(config)#router bgp 65210
Admin(config-bgp-65210)#neighbor 26.6.6.6 remote-as 65210
Admin(config-bgp-65210)#neighbor 26.6.6.6 update-source 33.3.3.3
Admin(config-bgp-65210)#address-family vpnv4 unicast
Admin(config-bgp-65210-vpnv4)#neighbor 26.6.6.6 activate
Admin(config-bgp-65210-vpnv4)#exit
Admin(config-bgp-65210)#exit
Admin(config)#
```

18.3.4.6 Verifying Configuration Results

1. Check configuration results of PE1, P and PE2. Verify that the devices on the backbone network communicate with each other through the OSPF configuration. The following takes PE1 for example.

Set up OSPF adjacencies between PE1, P and PE2. The adjacency states are “Full” and each can learn the route of Loopback1 from one another.

```
Admin(config)#show ipv4 ospf neighbor
Total number of full neighbors: 1
OSPF process 130 VRF(default):
Neighbor ID  Pri  State    Dead Time  Address    Interface  Instance ID
42.2.2.2       1  Full/DR  00:00:39   131.0.0.2  vlanif131  0
Admin(config)#show ipv4 route ospf
Ipv4 routes information :
IP Route Table for VRF "default"
O       33.3.3.3/32 [110/30] via 131.0.0.2, vlanif131, 00:32:52
O       42.2.2.2/32 [110/20] via 131.0.0.2, vlanif131, 00:32:52
O       132.0.0.0/24 [110/20] via 131.0.0.2, vlanif131, 00:32:52
```

2. Check MPLS LDP configuration results of PE1, P and PE2. The following uses PE1 for example.

   Set up LDP sessions between PE1 and P, and between P and PE2. Set **State** to **OPERATIONAL**.

```
Admin(config)#show mpls ldp session
show mpls ldp session :
Peer IP Address      IF Name    My Role    State      KeepAlive
42.2.2.2             vlanif131  Passive   OPERATIONAL   30
33.3.3.3             vlanif131  Passive   OPERATIONAL   30
```

3. Check VPN instance configuration results of PE1 and PE2. All PEs ping the connected CEs successfully. The following uses PE1 for example.

```
Admin(config)#show ip vrf
VRF     ID    Router-id    R D     Interfaces
vpna    1                 100:1     vlanif130

vpnb    2                 100:2     vlanif134
Admin(config)#ping -v vpna 130.0.0.2
PING 130.0.0.2 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 130.0.0.2 : bytes=56: icmp_seq=0 ttl=64 time<10 ms
Reply from 130.0.0.2 : bytes=56: icmp_seq=1 ttl=64 time<10 ms
Reply from 130.0.0.2 : bytes=56: icmp_seq=2 ttl=64 time<10 ms
Reply from 130.0.0.2 : bytes=56: icmp_seq=3 ttl=64 time<10 ms
Reply from 130.0.0.2 : bytes=56: icmp_seq=4 ttl=64 time<10 ms
```

4. Check BGP neighbor information of PE1, PE2, CE1, CE2, CE3 and CE4. The following uses PE1 for example.

Set up a BGP peer relation between PE and CE. Set **BGP state** to **Established**.

```
Admin(config)#show bgp neighbors
BGP neighbor is 130.0.0.2, vrf vpna, remote AS 65200, local AS 65210,
external link
  BGP version 4, remote router ID 192.0.0.1
  BGP state = Established, up for 00:38:05
  Last read 00:38:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised
    Address family IPv4 Unicast: advertised
  Received 79 messages, 0 notifications, 0 in queue
  Sent 80 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 130.0.0.1, Local port: 63820
Foreign host: 130.0.0.2, Foreign port: 179
Nexthop: 130.0.0.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

5. Check BGP neighbor information of PE1 and PE2. The following uses PE1 for example.

   Set up a BGP peer relation between PE1 and PE2. Set **BGP state** to **Established**.

```
Admin(config)#show bgp neighbors
BGP neighbor is 33.3.3.3, remote AS 65210, local AS 65210, internal link
  BGP version 4, remote router ID 33.3.3.3
  BGP state = Established, up for 00:38:12
  Last read 00:38:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
    Address family VPNv4 Unicast: advertised and received
  Received 79 messages, 0 notifications, 0 in queue
  Sent 80 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is 26.6.6.6
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AIGP is enabled
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AIGP is enabled
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 26.6.6.6, Local port: 179
Foreign host: 33.3.3.3, Foreign port: 63978
Nexthop: 26.6.6.6
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 130.0.0.2, vrf vpna, remote AS 65200, local AS 65210,
external link
  BGP version 4, remote router ID 192.0.0.1
  BGP state = Established, up for 00:38:05
  Last read 00:38:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised
    Address family IPv4 Unicast: advertised
  Received 79 messages, 0 notifications, 0 in queue
  Sent 80 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
```

```
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 130.0.0.1, Local port: 63820
Foreign host: 130.0.0.2, Foreign port: 179
Nexthop: 130.0.0.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

6. Check the route to the opposite CE. The following uses PE1 for example.

```
Admin(config)#show ipv4 route vrf vpna
Ipv4 routes information :
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "vpna"
C       130.0.0.0/24 is directly connected, vlanif130
B       133.0.0.0/24 [200/0] via 33.3.3.3, 00:00:04

Gateway of last resort is not set
Admin(config)#show ipv4 route vrf vpnb
Ipv4 routes information :
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "vpnb"
C       134.0.0.0/24 is directly connected, vlanif134
B       135.0.0.0/24 [200/0] via 33.3.3.3, 00:10:04

Gateway of last resort is not set
```

7. CEs in the same VPN can ping each other successfully. However, CEs in different VPNs fail to ping each other. In the following example, CE1 can ping CE3 successfully but fails to ping CE4.

```
Admin(config)#ping 133.0.0.2
PING 133.0.0.2 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 133.0.0.2 : bytes=56: icmp_seq=0 ttl=62 time=12 ms
Reply from 133.0.0.2 : bytes=56: icmp_seq=1 ttl=62 time<10 ms
Reply from 133.0.0.2 : bytes=56: icmp_seq=2 ttl=62 time<10 ms
Reply from 133.0.0.2 : bytes=56: icmp_seq=3 ttl=62 time<10 ms
Reply from 133.0.0.2 : bytes=56: icmp_seq=4 ttl=62 time<10 ms


----133.0.0.2 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 6/7/12
Admin(config)#ping 135.0.0.2
PING 135.0.0.2 : 56 data bytes.
Press Ctrl-c to Stop.

Request time out.
Request time out.
Request time out.
Request time out.
Request time out.


----135.0.0.2 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

19 Configuring Layer 2 / Layer 3 Protocols

- Configuring the MSTP Service
- Configuring the LACP
- Configuring the ERPS
- Configuring the PON Protection

19.1 Configuring the MSTP Service

19.1.1 Background Information

In the Layer 2 switching network, a loop in the network causes infinite loop and proliferation of packets, which leads to broadcast storm and occupies all bandwidth available so that the network becomes unusable. As defined by the IEEE 802.1s, the MSTP (Multiple Spanning Tree Protocol) is compatible with STP and RSTP, and can compensate for the defects of them.

The MSTP is applied to the access network as follows:

- The MSTP features fast convergence, and allows the traffics in different VLANs to be forwarded along their own paths, so as to provide a better load balancing mechanism for redundancy links.
- The MSTP prunes a loop network into a loop-free tree network. This helps avoid infinite loop and proliferation of packets.

19.1.2 Network Scenario

Service Planning

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

Network Diagram

Figure 19-1 shows the network diagram for the MSTP services.

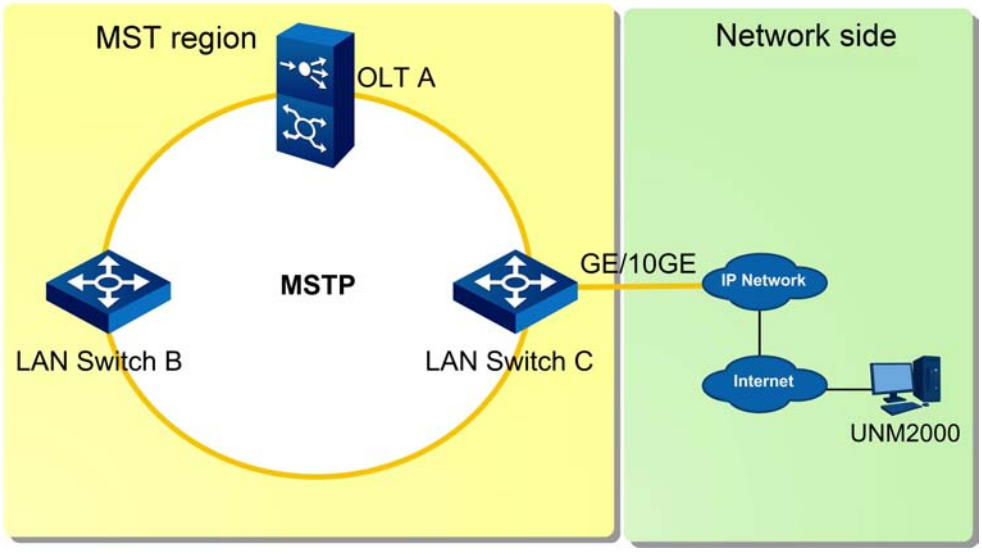


Figure 19-1 Network Diagram for the MSTP Service

A is the OLT equipment running the MSTP in the MST region; B and C are switches; and C is the root of the region.

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.

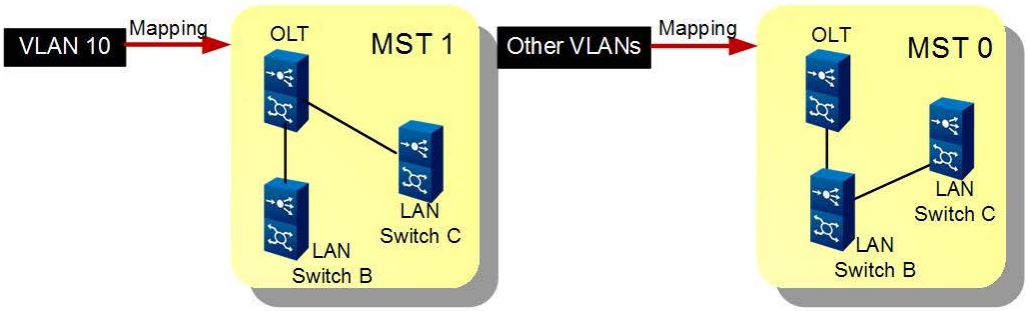


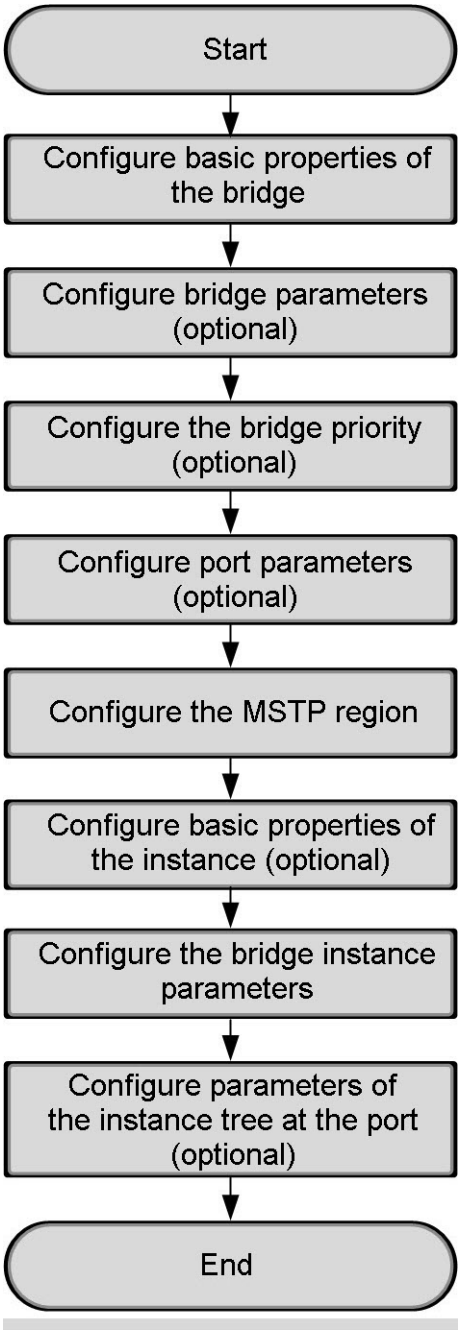
Figure 19-2 Mappings Between Spanning Trees and VLANs

19.1.3 Configuration Flow

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

Note:

Default values are recommended for the optional configuration items.



19.1.4 Configuring Basic Properties of the Bridge

Command Format

Enable / disable the STP function.

```
stp [enable|disable]
stp port <frameid/slotid/portid> [enable|disable]
stp link-aggregation <group-id> [enable|disable]
```

Configure the STP protocol mode.

```
stp mode [mstp|rstp|stp]
```

Configure the MSTP region name.

```
stp region-name <name>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Enabling / disabling the STP function	stp [enable|disable]	The STP function switch.	Mandatory	enable
	port <frameid/slo-tid/portid>	Subrack No. / slot No. / PON port No.	Mandatory	1/19/1
	link-aggregation <group-id>	The Trunk group ID. The value ranges from 1 to 16.	Mandatory	1
Configuring the STP protocol mode	stp mode [mstp|rstp|stp]	The STP protocol mode.	Mandatory	mstp
Configuring the MSTP region name	region-name <name>	The MSTP region name. The value contains 1 to 32 characters. The default setting is the MAC address of the current equipment.	Mandatory	fiberhome

Example

1. Enable the STP globally.

```
Admin(config)#stp enable
```

2. Enable the STP for PON Port 1 in Slot 19 of Subrack 1.

```
Admin(config)#stp port 1/19/1 enable
```

3. Enable the STP for Trunk group 1.

```
Admin(config)#stp link-aggregation 1 enable
```

4. Set the STP protocol mode to MSTP.

```
Admin(config)#stp mode mstp
```

5. Set the MSTP region name to "fiberhome".

```
Admin(config)#stp region-name fiberhome
Admin(config)#
```

19.1.5 Configuring Bridge Parameters (Optional)

Command Format

```
stp timer forward-delay <time>
stp timer hello <time>
stp timer max-age <time>
stp time-factor <factor>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the bridge parameter forward-time	forward-delay <time>	Forward delay (unit: second). The value ranges from 4 to 30.	Mandatory	20
Configuring the bridge parameter hello-time	hello <time>	The Hello message interval (unit: second). The value ranges from 1 to 10.	Mandatory	5
Configuring the bridge parameter max-age	max-age <time>	The maximum interval for root bridge messages (unit: second). The value ranges from 6 to 40.	Optional	20
Configuring the bridge parameter time-factor	time-factor <factor>	The maximum number of hops for protocol packets. The value ranges from 1 to 40.	Optional	25

Example

1. Set the bridge parameter "forward-time" to 20.

```
Admin(config)#stp timer forward-delay 20
```

2. Set the bridge parameter "hello-time" to 5.

```
Admin(config)#stp timer hello 5
```

3. Set the bridge parameter "max-age" to 20.

```
Admin(config)#stp timer max-age 20
```

4. Set the bridge parameter "time-factor" to 25.

```
Admin(config)#stp time-factor 25
Admin(config)#
```

19.1.6 Configuring the Bridge Priority (Optional)

Command Format

```
stp priority <priority-value>
```

Planning Data

Parameter	Description	Attribute	Example
priority <priority-value>	The bridge priority value. It is a multiple of 4096, ranging from 0 to 61440.	Mandatory	8192

Example

Set the bridge priority to 8192.

```
Admin(config)#stp priority 8192
Admin(config)#
```

19.1.7 Configuring Port Parameters (Optional)

Command Format

Configure the edge port of the current port.

```
stp port <frameid/slotid/portid> edged-port [enable|disable]
```

Configure the edge port of the Trunk group.

```
stp link-aggregation <group-id> edged-port [enable|disable]
```

Configure the link type of the port.

```
stp port <frameid/slotid/portid> point-to-point [enable|disable]
```

Configure the link type of the Trunk group.

```
stp link-aggregation <group-id> point-to-point [enable|disable]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the edge port of the current port	port <frameid/slo-tid/portid>	Subrack No. / slot No. / port No.	Mandatory	1/19/1
	edged-port [enable| disable]	◆ enable: auto-negotiation ◆ disable: edge port The default setting is "enable" (auto-negotiation).	Mandatory	enable
Configuring the edge port of the Trunk group	link-aggregation <group-id>	The Trunk group ID. The value ranges from 1 to 16.	Mandatory	1
	edged-port [enable| disable]	◆ enable: auto-negotiation ◆ disable: edge port The default setting is "enable" (auto-negotiation).	Mandatory	enable
Configuring the link type of the port	port <frameid/slo-tid/portid>	Subrack No. / slot No. / port No.	Mandatory	1/19/1
	point-to-point [enable| disable]	◆ enable: point-to-point ◆ disable: shared The default setting is "disable" (shared).	Mandatory	enable
Configuring the link type of the Trunk group	link-aggregation <group-id>	The Trunk group ID. The value ranges from 1 to 16.	Mandatory	1
	point-to-point [enable| disable]	◆ enable: point-to-point ◆ disable: shared The default setting is "disable" (shared).	Mandatory	enable

Example

1. Configure the edge port of the current port.

```
Admin(config)#stp port 1/19/1 edged-port enable
```

2. Configure the edge port of the Trunk group.

```
Admin(config)#stp link-aggregation 1 edged-port enable
```

3. Configure the link type of the port.

```
Admin(config)#stp port 1/19/1 point-to-point enable
```

4. Configure the link type of the Trunk group.

```
Admin(config)#stp link-aggregation 1 point-to-point enable
Admin(config)#
```

19.1.8 Configuring the MST Region

Command Format

Configure the revision level of the MSTP.

```
stp revision-level <level>
```

Planning Data

Parameter	Description	Attribute	Example
revision-level <level>	The revision level of the MSTP. The value ranges from 0 to 65535.	Mandatory	100

Example

Set the revision level of the MSTP to 100.

```
Admin(config)#stp revision-level 100
Admin(config)#
```

19.1.9 Configuring Basic Properties of the Instance (Optional)

Command Format

```
stp instance <instanceid> vlan <vlanlist>
```

Data Planning

Parameter	Description	Attribute	Example
instance <instanceid>	The instance ID, ranging from 1 to 64.	Mandatory	1
vlan <vlanlist>	The VLAN ID added to the instance.	Mandatory	100

Example

Add the VLAN ID 100 to Instance 1.

```
Admin(config)#stp instance 1 vlan 100
Admin(config)#
```

19.1.10 Configuring Parameters of the Bridge Instance

Command Format

```
stp instance <instanceid> priority <priority-value>
```

Planning Data

Parameter	Description	Attribute	Example
instance <instanceid>	The instance ID, ranging from 0 to 64.	Mandatory	1
priority <priority-value>	The priority of the instance. It is an integral multiple of 4096, ranging from 0 to 61440, and the default value is 32768.	Mandatory	4096

Example

Set the priority of Instance1 to 4096.

```
Admin(config)#stp instance 1 priority 4096
Admin(config)#
```

19.1.11 Configuring Instance Tree Parameters for the Port (Optional)

Command Format

Configure the path cost of the port.

```
stp port <frameid/slotid/portid> instance <instanceid> cost <cost>
```

Configure the path cost of the Trunk group.

```
stp link-aggregation <group-id> instance <instanceid> cost <cost>
```

Configure the priority of the port.

```
stp port <frameid/slotid/portid> instance <instanceid> priority <priority>
```

Configure the priority of the Trunk group.

```
stp link-aggregation <group-id> instance <instanceid> priority <priority>
```

Data Planning

Procedure	Parameter	Description	Attribute	Example
Configuring the path cost of the port	`port <frameid/slotid/portid>`	The subrack number / slot number / port number.	Mandatory	1/19/1
	`instance <instanceid>`	The instance ID, ranging from 0 to 64.	Mandatory	1
	`cost <cost>`	The path cost of the port. The value ranges from 1 to 200000000, and the default value is 0.	Mandatory	2000
Configuring the path cost of the Trunk group	`link-aggregation <group-id>`	The Trunk group ID. The value ranges from 1 to 16.	Mandatory	1
	`instance <instanceid>`	The instance ID, ranging from 0 to 64.	Mandatory	1
	`cost <cost>`	The path cost of the port. The value ranges from 1 to 200000000, and the default value is 0.	Mandatory	2000
Configuring the priority of the port	`port <frameid/slotid/portid>`	The subrack number / slot number / port number.	Mandatory	1/19/1
	`instance <instanceid>`	The instance ID, ranging from 0 to 64.	Mandatory	1
	`priority <priority>`	The priority of the port. It is an integral multiple of 16, ranging from 0 to 240, and the default value is 128.	Mandatory	160
Configuring the priority of the Trunk group	`link-aggregation <group-id>`	The Trunk group ID. The value ranges from 1 to 16.	Mandatory	1
	`instance <instanceid>`	The instance ID, ranging from 0 to 64.	Mandatory	1

Procedure	Parameter	Description	Attribute	Example
	priority <priority>	The priority of the port. It is an integral multiple of 16, ranging from 0 to 240, and the default value is 128.	Mandatory	160

Example

1. Configure the path cost of the port.

```
Admin(config)#stp port 1/19/1 instance 1 cost 2000
```

2. Configure the path cost of the Trunk group.

```
Admin(config)#stp link-aggregation 1 instance 1 cost 2000
```

3. Configure the priority of the port.

```
Admin(config)#stp port 1/19/1 instance 1 priority 160
```

4. Configure the priority of the Trunk group.

```
Admin(config)#stp link-aggregation 1 instance 1 priority 160
Admin(config)#
```

19.2 Configuring the LACP

19.2.1 Background Information

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 is inconsistent with those of other ports. In this case, the member port leaves the aggregation group. When conditions are met, the port rejoins the aggregation group. To delete a member from an aggregation group, manual operation of the user is required.

19.2.2 Configuration Rules

- 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 port 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.

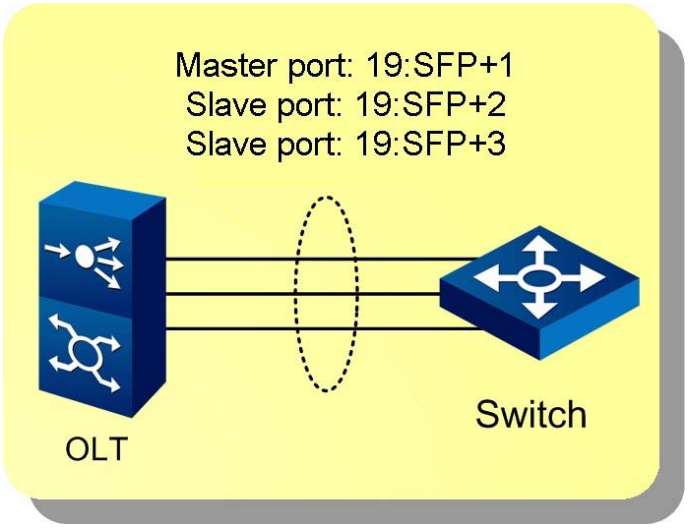
19.2.3 Network Scenario

Service Planning

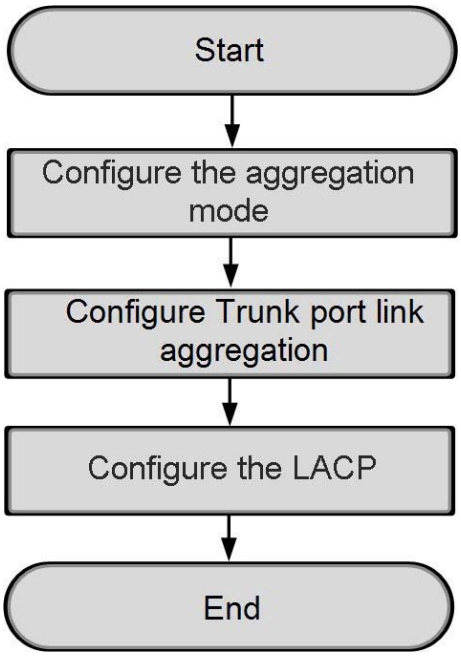
Set the three uplink ports of the OLT equipment to the member ports of the LACP protection group to enable link backup. Port 1 serves as the master port, and the other two the slave ones.

Network Diagram

The figure below shows the network for the LACP function.



19.2.4 Configuration Flow



19.2.5 Configuring the Aggregation Mode

Command Format

```
link-aggregation <frameid/slotid/portid> {[mode] [smac|dmac|sdmac|sip|dip|sdip]}*1 {[workmode] [lacp-static]}*1
```

Planning Data

Parameter	Description	Attribute	Example
<frameid/slotid/-portid>	Subrack No. / slot No. / port No.	Mandatory	1/19/1
{[mode] [smac|dmac|sdmac|sip|dip|sdip]}*1	The load balancing mode of the aggregation group ◆ smac: the source MAC address ◆ dmac: the destination MAC address ◆ sdmac: the source and destination MAC addresses ◆ sip: the source IP address ◆ dip: the destination IP address ◆ sdip: the source and destination IP addresses	Optional	smac
{[workmode] [lacp-static]}*1	Static Lacp	Optional	lacp-static

Example

Configure the static LACP aggregation mode based on the source MAC address for Port 1 in Slot 19 of Subrack 1.

```
Admin(config)#link-aggregation 1/19/1 mode smac workmode lacp-static
Admin(config)#
```

19.2.6 Configuring Trunk Port Link Aggregation

Command Format

```
link-aggregation add-member <frameid/slotid/portid> <frameid/slotid/
portid> {<frameid/slotid/portid>}*6
link-aggregation delete-member <frameid/slotid/portid> {<frameid/slotid/
portid>}*7
```

Data Planning

Parameter	Description	Attribute	Example
<frameid/slotid/-portid>	The master port. The subrack number / slot number / port number.	Mandatory	1/19/1
<frameid/slotid/-portid>	The member port. The subrack number / slot number / port number.	Mandatory	1/19/2
{<frameid/slotid/-portid>}*6	The member port. The subrack number / slot number / port number.	Optional	-

Example

1. Configure the Trunk port link aggregation, adding the master port 1/19/1 and the member port 1/19/2 to the Trunk group.

```
Admin(config)#link-aggregation add-member 1/19/1 1/19/2
```

2. Delete the Trunk group member 1/19/1. (Use this command format to delete a port)

```
Admin(config)#link-aggregation delete-member 1/19/1
Admin(config)#
```

19.2.7 Configuring the LACP

Command Format

Enable the LACP function.

```
lacp [enable|disable]
```

Configure the priority of the LACP system.

```
lacp priority <value> system
```

Configure the priority of the LACP port.

```
lacp priority <value> port <frameid/slotid/portid>
```

Configure the timer of the LACP port.

```
lacp timeout [fast|slow] port <frameid/slotid/portid>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Enabling / disabling the LACP function	`lacp [enable|disable]`	Enabling or disabling the LACP function globally.	Mandatory	enable
Configuring the priority of the LACP system	`priority <value>`	The LACP system priority. The value ranges from 0 to 65534, and the default value is 32768. The smaller is the value, the higher is the priority.	Mandatory	120
Configuring the priority of the LACP port	`priority <value>`	The LACP port priority. The value ranges from 0 to 65534, and the default value is 32768. The smaller is the value, the higher is the priority.	Mandatory	120
	`port <frameid/slo-tid/portid>`	Subrack No. / slot No. / port No.	Mandatory	1/19/1
Configuring the timer of the LACP port	`timeout [fast|slow]`	◆ fast: specifies the short-period timeout mode for packet receiving of the LACP port. ◆ slow: specifies the long-period timeout mode for packet receiving of the LACP port.	Mandatory	fast

Procedure	Parameter	Description	Attribute	Example
	port <frameid/slo-tid/portid>	Subrack No. / slot No. / port No.	Mandatory	1/19/1

Example

1. Enable the LACP function.

```
Admin(config)#lacp enable
```

2. Set the priority of the LACP system to 120.

```
Admin(config)#lacp priority 120 system
```

3. Set the priority of Port 1 in Slot 19 of Subrack 1 to 120.

```
Admin(config)#lacp priority 120 port 1/19/1
```

4. Set the timer type of Port 1 in Slot 19 of Subrack 1 to short timer.

```
Admin(config)#lacp timeout fast port 1/19/1
Admin(config)#
```

19.3 Configuring the ERPS

19.3.1 Background Information

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 OLT) 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)	When 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)	When 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 when a port misjudges 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 is not detected by the ERPS protocol. If the fault persists at the expiration of the hold-off time, link protection is implemented based on the ERPS protocol.

19.3.2 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.

19.3.3 Configuring Single-Ring Single-Instance Protection

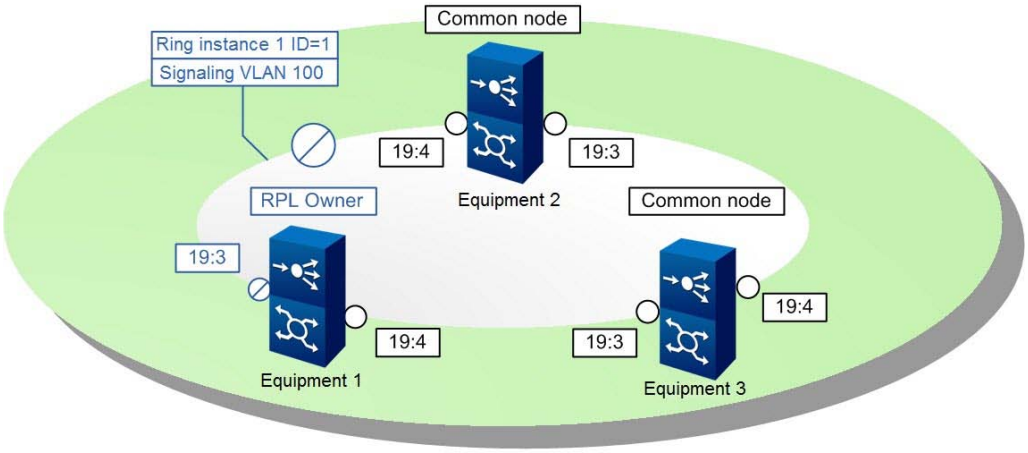
19.3.3.1 Network Scenario

Service Planning

Three OLT devices 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 the figure below.



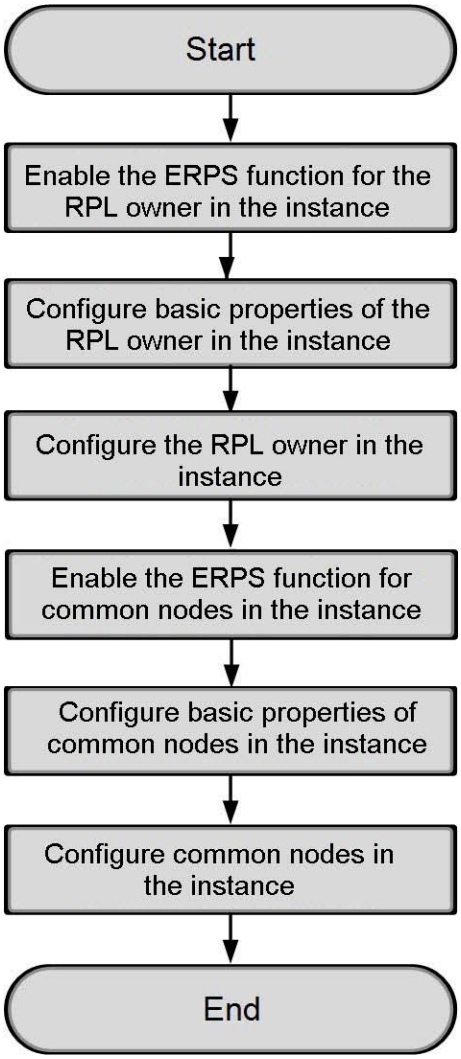
Equipment 1 serves as the RPL Owner of the ERPS ring. Port 19:3 of Equipment 1 serves as the RPL Port and is blocked.

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 is 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 is blocked again, and the service flow is switched back to the original direction.

19.3.3.2 Configuration Flow

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



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

Command Format

```
erps mode [enable|disable]
```

Planning Data

Parameter	Description	Attribute	Example
erps mode [enable|disable]	Enables or disables the ERPS function.	Mandatory	enable

Example

Enable the ERPS function.

```
Admin(config)#erps mode enable
Admin(config)#
```

19.3.3.4 Configuring Basic Properties of the RPL Owner in the Instance

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the mappings between the VLANs and the ERPS instance	`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	1
	`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	100
	`{to <vlanid-end>}*1`	The ending value of the VLAN ID range.	Optional	200
Creating an ERPS ring	`ring <ring-id>`	The ring ID, ranging from 1 to 239.	Mandatory	1
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common|rpl-owner]`	A node can act as the common node or RPL owner.	Mandatory	rpl-owner

Example

1. Map VLANs 100 to 200 to ERPS Instance 1.

```
Admin(config)#erps instance 1 vlan-id 100 to 200
```

2. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

3. Set Equipment 1 in Ring Instance 1 to RPL owner.

```
Admin(config)#erps ring 1 erps-role rpl-owner
Admin(config)#
```

19.3.3.5 Configuring the RPL Owner in the Instance

Note:

Default values are recommended for the optional configuration items.

Command Format

Configure the signaling VLAN for the ERPS ring instance.

`erps ring <ringid> control-vlan <vlanid>`

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the signaling VLAN for the ERPS ring instance	`ring <ringid>`	The ring ID.	Mandatory	1
	`control-vlan <vlanid>`	The signaling VLAN ID.	Mandatory	100

Procedure	Parameter	Description	Attribute	Example
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance ID. The value ranges from 1 to 64.	Mandatory	1
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrevertive]`	The switching mode ◆ revertive ◆ nonrevertive	Mandatory	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19
	`primary-port <value>`	The first uplink port.	Mandatory	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	rpl-port

Procedure	Parameter	Description	Attribute	Example
Configuring properties of the second port in the ERPS ring instance	second-slot <value>	The number of the second slot.	Mandatory	19
	second-port <value>	The second uplink port.	Mandatory	4
	role [common| rpl-port]	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring the virtual channel VLAN for the ERPS ring instance	virtual-vlan <value>	The virtual channel VLAN.	Mandatory	-

Example

1. Set the signaling VLAN ID of the ERPS ring instance to 100.

```
Admin(config)#erps ring 1 control-vlan 100
```

2. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

3. Associate the ERPS ring instance with the VLAN Instance 1.

```
Admin(config)#erps ring 1 protect-inst 1
```

4. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

5. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

6. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

7. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

8. Set the first port of the RPL owner device in the ERPS ring instance to RPL port.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role rpl-port
```

9. Set the second port of the RPL owner device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
Admin(config)#
```

19.3.3.6 Enabling the ERPS Function for Common Nodes in the Instance

Command Format

```
erps mode [enable|disable]
```

Data Planning

Parameter	Description	Attribute	Example
erps mode [enable|disable]	Enabling or disabling the ERPS function.	Mandatory	enable

Example

Enable the ERPS function.

```
Admin(config)#erps mode enable
Admin(config)#
```

19.3.3.7 Configuring Basic Properties of Common Nodes in the Instance

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the mappings between the VLANs and the ERPS instance	`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	1
	`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	100
	`{to <vlanid-end>} *1`	The ending value of the VLAN ID range.	Optional	200
Creating an ERPS ring	`ring <ring-id>`	The ring ID, ranging from 1 to 239.	Mandatory	1
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common| rpl-owner]`	A node can act as the common node or RPL owner.	Mandatory	common

Example

1. Map VLANs 100 to 200 to ERPS Instance 1.

```
Admin(config)#erps instance 1 vlan-id 100 to 200
```

2. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

3. Set Equipment 2 and Equipment 3 in Ring Instance 1 to common nodes.

```
Admin(config)#erps ring 1 erps-role common
Admin(config)#
```

19.3.3.8 Configuring Common Nodes in the Instance

Note:

Default values are recommended for the optional configuration items.

Command Format

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the signaling VLAN for the ERPS ring instance	`ring <ringid>`	The ring ID.	Mandatory	1
	`control-vlan <vlanid>`	The signaling VLAN ID.	Mandatory	100

Procedure	Parameter	Description	Attribute	Example
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance ID. The value ranges from 1 to 64.	Mandatory	1
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrevertive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19
	`primary-port <value>`	The first uplink port.	Mandatory	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common

Procedure	Parameter	Description	Attribute	Example
Configuring properties of the second port in the ERPS ring instance	second-slot <value>	The number of the second slot.	Mandatory	19
	second-port <value>	The second uplink port.	Mandatory	4
	role [common| rpl-port]	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring the virtual channel VLAN for the ERPS ring instance	virtual-vlan <value>	The virtual channel VLAN.	Mandatory	-

Example

1. Set the signaling VLAN ID of the ERPS ring instance to 100.

```
Admin(config)#erps ring 1 control-vlan 100
```

2. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

3. Associate the ERPS ring instance with the VLAN Instance 1.

```
Admin(config)#erps ring 1 protect-inst 1
```

4. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

5. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

6. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

7. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

8. Set the first port of the common device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role common
```

9. Set the second port of the common device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
Admin(config)#
```

19.3.4 Configuring Single-Ring Multi-Instance Protection

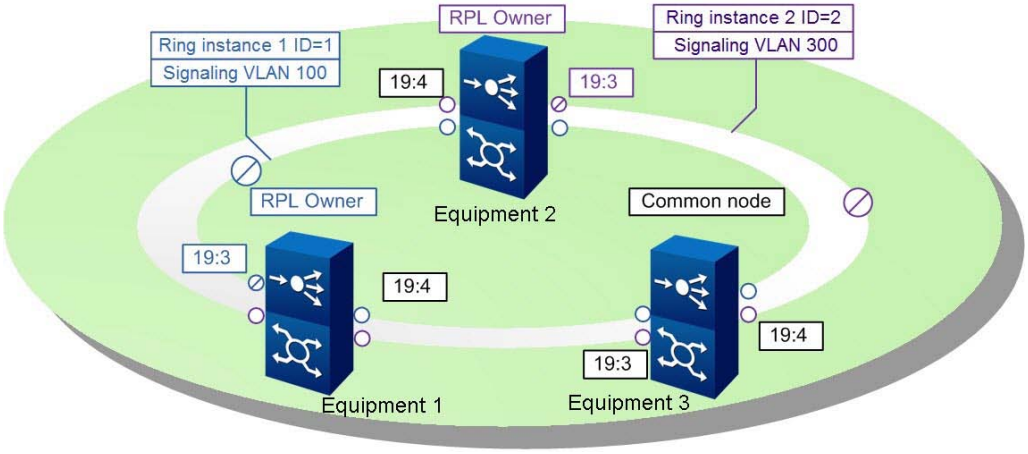
19.3.4.1 Network Scenario

Service Planning

Three OLT devices make up an ERPS protection ring. Two ERPS ring instances are created for the ring to protect different services.

Network Diagram

The network for the single-ring multi-instance ERPS is shown in the figure below.



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

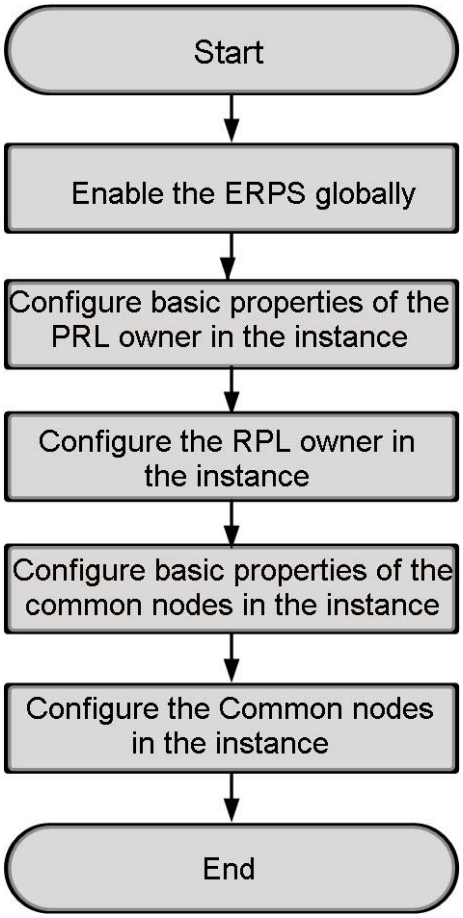
- Ring Instance 1 here is configured in the same way as that in the single-ring single-instance application. Equipment 1 serves as the RPL owner in Ring Instance 1; Port 19:3 servers as the RPL port and is blocked. With the signaling VLAN ID 100, Ring Instance 1 protects the service with the VLAN ID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

19.3.4.2 Configuration Flow

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

The figure below illustrates the flow of configuring an instance in the single-ring multi-instance application.



19.3.4.3 Enabling the ERPS Globally

Command Format

```
erps mode [enable|disable]
```

Planning Data

Parameter	Description	Attribute	Example
erps mode [enable|disable]	Enables or disables the ERPS function.	Mandatory	enable

Example

Enable the ERPS function.

```
Admin(config)#erps mode enable
Admin(config)#
```

19.3.4.4 Configuring Basic Properties of the RPL Owner in Instance One

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the mappings between the VLANs and the ERPS instance	erps instance <instance-id>	The ERPS instance ID, ranging from 1 to 64.	Mandatory	1
	vlan-id <vlanid>	The starting value of the VLAN ID range to be mapped.	Mandatory	100
	{to <vlanid-end>}*1	The ending value of the VLAN ID range.	Optional	-

Procedure	Parameter	Description	Attribute	Example
Creating an ERPS ring	`ring <ring-id>`	The ring ID, ranging from 1 to 239.	Mandatory	1
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common|rpl-owner]`	A node can act as the common node or RPL owner.	Mandatory	rpl-owner

Example

1. Map the VLAN 100 to ERPS Instance 1.

```
Admin(config)#erps instance 1 vlan-id 100
```

2. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

3. Set Equipment 1 in Ring Instance 1 to RPL owner.

```
Admin(config)#erps ring 1 erps-role rpl-owner
Admin(config)#
```

19.3.4.5 Configuring the RPL Owner in Instance One

Note:

Default values are recommended for the optional configuration items.

Command Format

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the signaling VLAN for the ERPS ring instance	`ring <ringid>`	The ring ID.	Mandatory	1
	`control-vlan <vlanid>`	The signaling VLAN ID.	Mandatory	100
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance. The value ranges from 1 to 64.	Mandatory	1

Procedure	Parameter	Description	Attribute	Example
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrevertive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19
	`primary-port <value>`	The first uplink port.	Mandatory	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	rpl-port
Configuring properties of the second port in the ERPS ring instance	`second-slot <value>`	The number of the second slot.	Mandatory	19
	`second-port <value>`	The second uplink port.	Mandatory	4
	`role [common| rpl-port]`	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring the virtual channel VLAN for the ERPS ring instance	`virtual-vlan <value>`	The virtual channel VLAN.	Mandatory	-

Example

1. Set the signaling VLAN ID of the ERPS ring instance to 100.

```
Admin(config)#erps ring 1 control-vlan 100
```

2. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

3. Associate the ERPS ring instance with the VLAN Instance 1.

```
Admin(config)#erps ring 1 protect-inst 1
```

4. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

5. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

6. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

7. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

8. Set the first port of the RPL owner device in the ERPS ring instance to RPL port.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role rpl-port
```

9. Set the second port of the RPL owner device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
```

19.3.4.6 Configuring Basic Properties of Common Nodes in Instance One

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the mappings between the VLANs and the ERPS instance	`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	1
	`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	100
	`{to <vlanid-end>}*1`	The ending value of the VLAN ID range.	Optional	-
Creating an ERPS ring	`ring <ring-id>`	The ring ID, ranging from 1 to 239.	Mandatory	1
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common|rpl-owner]`	The node can act as a common node or RPL owner.	Mandatory	common

Example

1. Map the VLAN 100 to ERPS Instance 1.

```
Admin(config)#erps instance 1 vlan-id 100
```

2. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

3. Set Equipment 2 and Equipment 3 in Ring Instance 1 to common nodes.

```
Admin(config)#erps ring 1 erps-role common
Admin(config)#
```

19.3.4.7 Configuring Common Nodes in Instance One

Note:

Default values are recommended for the optional configuration items.

Command Format

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the signaling VLAN for the ERPS ring instance	ring <ringid>	The ring ID.	Mandatory	1
	control-vlan <vlanid>	The signaling VLAN ID.	Mandatory	100

Procedure	Parameter	Description	Attribute	Example
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance. The value ranges from 1 to 64.	Mandatory	1
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrevertive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19
	`primary-port <value>`	The first uplink port.	Mandatory	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring properties of the second port in the ERPS ring instance	`second-slot <value>`	The number of the second slot.	Mandatory	19
	`second-port <value>`	The second uplink port.	Mandatory	4
	`role [common| rpl-port]`	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring the virtual channel VLAN for the ERPS ring instance	`virtual-vlan <value>`	The virtual channel VLAN.	Mandatory	-

Example

1. Set the signaling VLAN ID of the ERPS ring instance to 100.

```
Admin(config)#erps ring 1 control-vlan 100
```

2. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

3. Associate the ERPS ring instance with the VLAN Instance 1.

```
Admin(config)#erps ring 1 protect-inst 1
```

4. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

5. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

6. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

7. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

8. Set the first port of the common device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role common
```

9. Set the second port of the common device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
```

19.3.4.8 Configuring Basic Properties of the RPL Owner in Instance Two

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the mappings between the VLANs and the ERPS instance	`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	2
	`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	300
	`{to <vlanid-end>}*1`	The ending value of the VLAN ID range.	Optional	-
Creating an ERPS ring	`ring <ring-id>`	The ring ID, ranging from 1 to 239.	Mandatory	1
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common|rpl-owner]`	A node can act as the common node or RPL owner.	Mandatory	rpl-owner

Example

1. Map the VLAN 300 to ERPS Instance 2.

```
Admin(config)#erps instance 2 vlan-id 300
```

2. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

3. Set Equipment 2 in Ring Instance 2 to RPL owner.

```
Admin(config)#erps ring 1 erps-role rpl-owner
Admin(config)#
```

19.3.4.9 Configuring the RPL Owner in Instance Two

Note:

Default values are recommended for the optional configuration items.

Command Format

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the signaling VLAN for the ERPS ring instance	ring <ringid>	The ring ID.	Mandatory	1
	control-vlan <vlanid>	The signaling VLAN ID.	Mandatory	300

Procedure	Parameter	Description	Attribute	Example
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance. The value ranges from 1 to 64.	Mandatory	2
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrevertive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19
	`primary-port <value>`	The first uplink port.	Mandatory	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	rpl-port
Configuring properties of the second port in the ERPS ring instance	`second-slot <value>`	The number of the second slot.	Mandatory	19
	`second-port <value>`	The second uplink port.	Mandatory	4
	`role [common| rpl-port]`	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring the virtual channel VLAN for the ERPS ring instance	`virtual-vlan <value>`	The virtual channel VLAN	Mandatory	-

Example

1. Set the signaling VLAN ID of the ERPS ring instance to 300.

```
Admin(config)#erps ring 1 control-vlan 300
```

2. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

3. Associate the ERPS ring instance with the VLAN Instance 2.

```
Admin(config)#erps ring 1 protect-inst 2
```

4. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

5. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

6. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

7. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

8. Set the first port of the RPL owner device in the ERPS ring instance to RPL port.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role rpl-port
```

9. Set the second port of the RPL owner device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
```

19.3.4.10 Configuring Basic Properties of Common Nodes in Instance Two

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the mappings between the VLANs and the ERPS instance	`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	2
	`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	300
	`{to <vlanid-end>}*1`	The ending value of the VLAN ID range	Optional	-
Creating an ERPS ring	`ring <ring-id>`	The ring ID, ranging from 1 to 239.	Mandatory	1
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common|rpl-owner]`	A node can act as the common node or RPL owner.	Mandatory	common

Example

1. Map the VLAN 300 to ERPS Instance 2.

```
Admin(config)#erps instance 2 vlan-id 300
```

2. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

3. Set Equipment 1 and Equipment 3 in Ring Instance 2 to common nodes.

```
Admin(config)#erps ring 1 erps-role common
Admin(config)#
```

19.3.4.11 Configuring Common Nodes in Instance Two

Note:

Default values are recommended for the optional configuration items.

Command Format

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the signaling VLAN for the ERPS ring instance	ring <ringid>	The ring ID.	Mandatory	1
	control-vlan <vlanid>	The signaling VLAN ID.	Mandatory	300

Procedure	Parameter	Description	Attribute	Example
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance. The value ranges from 1 to 64.	Mandatory	2
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrevertive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19
	`primary-port <value>`	The first uplink port.	Mandatory	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring properties of the second port in the ERPS ring instance	`second-slot <value>`	The number of the second slot.	Mandatory	19
	`second-port <value>`	The second uplink port.	Mandatory	4
	`role [common| rpl-port]`	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common
Configuring the virtual channel VLAN for the ERPS ring instance	`virtual-vlan <value>`	The virtual channel VLAN.	Mandatory	-

Example

1. Set the signaling VLAN ID of the ERPS ring instance to 300.

```
Admin(config)#erps ring 1 control-vlan 300
```

2. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

3. Associate the ERPS ring instance with the VLAN Instance 2.

```
Admin(config)#erps ring 1 protect-inst 2
```

4. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

5. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

6. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

7. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

8. Set the first port of the common device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role common
```

9. Set the second port of the common device in the ERPS ring instance to common port.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
```

19.3.5 Configuring Tangent Ring Protection

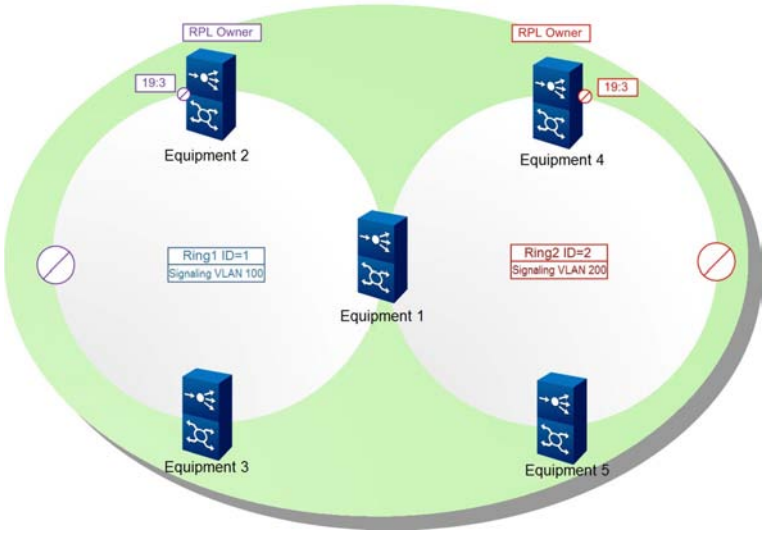
19.3.5.1 Network Scenario

Service Planning

Five OLT devices constitute two tangent ERPS protection rings, and each ring corresponds to an ERPS instance. The two instances protect different services.

Network Diagram

The figure below shows the network for the tangent-ring ERPS.



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 and 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 and 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.

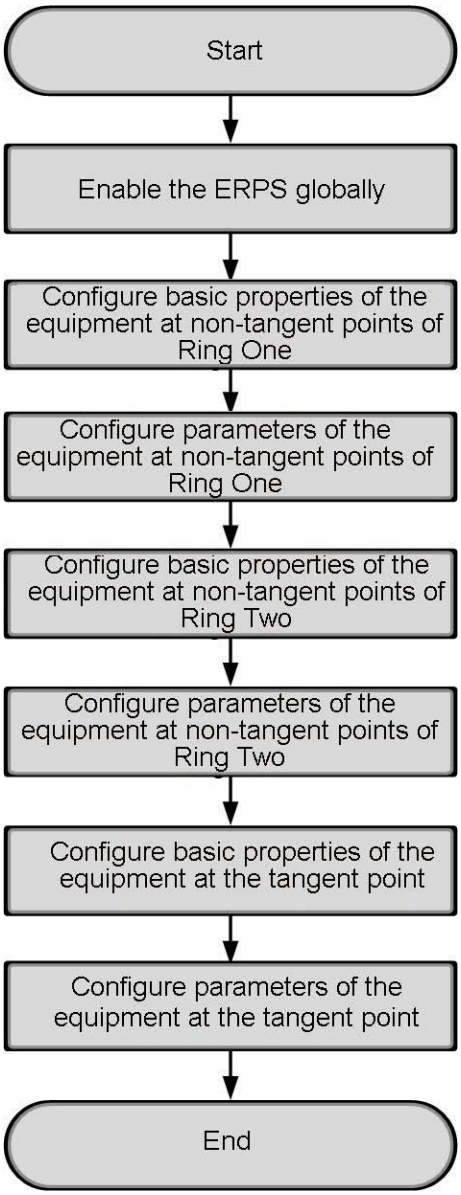
The table below describes the mappings between the ERPS instances created for the equipment and the rings in the example.

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 Name	Equipment Role	Ring Corresponding to Instance 1	Ring Corresponding to Instance 2
Equipment 4	RPL owner of Ring 2	N/A	Ring 2
Equipment 5	Common node of Ring 2	N/A	Ring 2

19.3.5.2 Configuration Flow

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



19.3.5.3 Enabling the ERPS Globally

Command Format

```
erps mode [enable|disable]
```

Planning Data

Parameter	Description	Attribute	Example
erps mode [enable|disable]	Enables or disables the ERPS function.	Mandatory	enable

Example

Enable the ERPS function.

```
Admin(config)#erps mode enable
Admin(config)#
```

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

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Planning Data

Parameter	Description	Attribute	Example
erps instance <instance-id>	The ERPS instance ID, ranging from 1 to 64.	Mandatory	1
vlan-id <vlanid>	The starting value of the VLAN ID range to be mapped.	Mandatory	100, 1000
{to <vlanid-end>}*1	The ending value of the VLAN ID range.	Optional	-

Example

Map VLANs 100 and 1000 to ERPS Instance 1.

```
Admin(config)#erps instance 1 vlan-id 100
```

```
Admin(config)#erps instance 1 vlan-id 1000
Admin(config)#
```

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

Note:

Default values are recommended for the optional configuration items.

Command Format

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example	
				Equipment 2	Equipment 3
Creating an ERPS ring	ring <ring-id>	The ring ID.	Mandatory	1	1
Configuring roles of the nodes in the ERPS ring instance	erps-role [common|rpl-owner]	A node can act as the common node or RPL owner.	Mandatory	rpl-owner	common
Configuring the signaling VLAN for the ERPS ring instance	ring <ringid>	The ring ID.	Mandatory	1	1
	control-vlan <vlanid>	The signaling VLAN ID.	Mandatory	100	100
Configuring the management domain level	mel <mel>	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7	7
Associating the ERPS ring instance with the VLAN instance	protect-inst <value>	The protection instance. The value ranges from 1 to 64.	Mandatory	1	1

Procedure	Parameter	Description	Attribute	Example	
				Equipment 2	Equipment 3
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrever-tive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19	19
	`primary-port <value>`	The first uplink port.	Mandatory	3	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	rpl-port	common

Procedure	Parameter	Description	Attribute	Example	
				Equipment 2	Equipment 3
Configuring properties of the second port in the ERPS ring instance	second-slot <value>	The number of the second slot.	Mandatory	19	19
	second-port <value>	The second uplink port.	Mandatory	4	4
	role [common| rpl-port]	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common	common
Configuring the virtual channel VLAN for the ERPS ring instance	virtual-vlan <value>	The virtual channel VLAN.	Mandatory	-	-

Example

1. Create an ERPS ring.

```
Admin(config)#erps ring 1
```

2. Set Equipment 2 to RPL owner and Equipment 3 to common node in the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-role rpl-owner
Admin(config)#erps ring 1 erps-role common
Admin(config)#
```

3. Set the signaling VLAN ID of the ERPS ring instance to 100.

```
Admin(config)#erps ring 1 control-vlan 100
```

4. Set the management domain level to 7.

```
Admin(config)#erps ring 1 mel 7
```

5. Associate the ERPS ring instance with the VLAN Instance 1.

```
Admin(config)#erps ring 1 protect-inst 1
```

6. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 1 erps-mode revertive
```

7. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 1 wrt-time 5
```

8. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 1 holdoff-time 1000
```

9. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 1 guard-time 500
```

10. Set the first port of Equipment 2 to RPL port and the first port of Equipment 3 to common port in the ERPS ring instance.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role rpl-port
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role common
```

11. Set the second port of Equipment 2 and Equipment 3 to common port in the ERPS ring instance.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
Admin(config)#
```

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

Command Format

Configure the mappings between VLANs and ERPS instances.

```
erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1
```

Planning Data

Parameter	Description	Attribute	Example
`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	2
`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	200, 2000
`{to <vlanid-end>}*1`	The ending value of the VLAN ID range.	Optional	-

Example

Map VLANs 200 and 2000 to ERPS Instance 2.

```
Admin(config)#erps instance 2 vlan-id 200
Admin(config)#erps instance 2 vlan-id 2000
Admin(config)#
```

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

Note:

Default values are recommended for the optional configuration items.

Command Format

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

```
erps ring <ring-id> second-slot <value> second-port <value> role [common|
rpl-port]
```

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

```
erps ring <ring-id> virtual-vlan <value>
```

Planning Data

Procedure	Parameter	Description	Attribute	Example	
				Equipment 4	Equipment 5
Creating an ERPS ring	`ring <ring-id>`	The ring ID.	Mandatory	2	2
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common| rpl-owner]`	The node can act as a common node or RPL owner.	Mandatory	rpl-owner	common
Configuring the signaling VLAN for the ERPS ring instance	`ring <ringid>`	The ring ID.	Mandatory	2	2
	`control-vlan <vlanid>`	The signaling VLAN ID.	Mandatory	200	200
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance. The value ranges from 1 to 64.	Mandatory	2	2
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive| nonrever-tive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive	revertive

Procedure	Parameter	Description	Attribute	Example	
				Equipment 4	Equipment 5
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000	1000
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	The number of the first slot.	Mandatory	19	19
	`primary-port <value>`	The first uplink port.	Mandatory	3	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	rpl-port	common
Configuring properties of the second port in the ERPS ring instance	`second-slot <value>`	The number of the second slot.	Mandatory	19	19
	`second-port <value>`	The second uplink port.	Mandatory	4	4
	`role [common| rpl-port]`	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common	common
Configuring the virtual channel VLAN for the ERPS ring instance	`virtual-vlan <value>`	The virtual channel VLAN.	Mandatory	-	-

Example

1. Create an ERPS ring.

```
Admin(config)#erps ring 2
```

2. Set Equipment 4 to RPL owner and Equipment 5 to common node in the ERPS ring instance.

```
Admin(config)#erps ring 2 erps-role rpl-owner
Admin(config)#erps ring 2 erps-role common
Admin(config)#
```

3. Set the signaling VLAN ID of the ERPS ring instance to 200.

```
Admin(config)#erps ring 2 control-vlan 200
```

4. Set the management domain level to 7.

```
Admin(config)#erps ring 2 mel 7
```

5. Associate the ERPS ring instance with the VLAN Instance 2.

```
Admin(config)#erps ring 2 protect-inst 2
```

6. Configure the switching mode for the ERPS ring instance.

```
Admin(config)#erps ring 2 erps-mode revertive
```

7. Set the wait-to-restore time for the ERPS ring instance to 5 minutes.

```
Admin(config)#erps ring 2 wrt-time 5
```

8. Set the hold-off time for the ERPS ring instance to 1000 ms.

```
Admin(config)#erps ring 2 holdoff-time 1000
```

9. Set the guard time for the ERPS ring instance to 500 ms.

```
Admin(config)#erps ring 2 guard-time 500
```

10. Set the first port of Equipment 4 to RPL port and the first port of Equipment 5 to common port in the ERPS ring instance.

```
Admin(config)#erps ring 2 primary-slot 19 primary-port 3 role rpl-port
Admin(config)#erps ring 2 primary-slot 19 primary-port 3 role common
```

11. Set the second port of Equipment 4 and Equipment 5 to common port in the ERPS ring instance.

```
Admin(config)#erps ring 2 second-slot 19 second-port 4 role common
Admin(config)#
```

19.3.5.8 Configuring Basic Properties of the Equipment at the Tangent Point

Command Format

Configure the mappings between VLANs and ERPS instances.

`erps instance <instance-id> vlan-id <vlanid> {to <vlanid-end>}*1`

Planning Data

Parameter	Description	Attribute	Example	
			Ring 1	Ring 2
`erps instance <instance-id>`	The ERPS instance ID, ranging from 1 to 64.	Mandatory	1	2
`vlan-id <vlanid>`	The starting value of the VLAN ID range to be mapped.	Mandatory	100, 1000	200, 2000
`{to <vlanid-end>}*1`	The ending value of the VLAN ID range.	Optional	-	-

Example

1. Map VLANs 100 and 1000 to ERPS Instance 1.

```
Admin(config)#erps instance 1 vlan-id 100
Admin(config)#erps instance 1 vlan-id 1000
```

2. Map VLANs 200 and 2000 to ERPS Instance 2.

```
Admin(config)#erps instance 2 vlan-id 200
Admin(config)#erps instance 2 vlan-id 2000
Admin(config)#
```

19.3.5.9 Configuring Parameters of the Equipment at the Tangent Point

Note:

Default values are recommended for the optional configuration items.

Command Format

Create an ERPS ring.

```
erps ring <ring-id>
```

Configure the roles of the nodes in the ERPS ring instance.

```
erps ring <ring-id> erps-role [common|rpl-owner]
```

Configure the signaling VLAN for the ERPS ring instance.

```
erps ring <ringid> control-vlan <vlanid>
```

Configure the management domain level. (Optional)

```
erps ring <ring-id> mel <mel>
```

Associate the ERPS ring instance with the VLAN instance.

```
erps ring <ring-id> protect-inst <value>
```

Configure the switching mode for the ERPS ring instance. (Optional)

```
erps ring <ring-id> erps-mode [revertive|nonrevertive]
```

Configure the wait-to-restore time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> wrt-time <value>
```

Configure the hold-off time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> holdoff-time <value>
```

Configure the guard time for the ERPS ring instance. (Optional)

```
erps ring <ring-id> guard-time <value>
```

Configure properties of the first port in the ERPS ring instance.

```
erps ring <ring-id> primary-slot <value> primary-port <value> role [common|
rpl-port]
```

Configure properties of the second port in the ERPS ring instance.

`erps ring <ring-id> second-slot <value> second-port <value> role [common|rpl-port]`

Configure the virtual channel VLAN for the ERPS ring instance. (Reserved function, configuration not required currently)

`erps ring <ring-id> virtual-vlan <value>`

Planning Data

Procedure	Parameter	Description	Attribute	Example	
				Ring 1	Ring 2
Creating an ERPS ring	`ring <ring-id>`	The ring ID.	Mandatory	1	2
Configuring roles of the nodes in the ERPS ring instance	`erps-role [common|rpl-owner]`	The node can act as a common node or RPL owner.	Mandatory	common	common
Configuring the signaling VLAN for the ERPS ring instance	`ring <ringid>`	The ring ID.	Mandatory	1	2
	`control-vlan <vlanid>`	The signaling VLAN ID.	Mandatory	100	200
Configuring the management domain level	`mel <mel>`	The maintenance entity level. The value ranges from 0 to 7.	Mandatory	7	7
Associating the ERPS ring instance with the VLAN instance	`protect-inst <value>`	The protection instance. The value ranges from 1 to 64.	Mandatory	1	2
Configuring the switching mode for the ERPS ring instance	`erps-mode [revertive|nonrevertive]`	The switching mode. ◆ revertive ◆ nonrevertive	Mandatory	revertive	revertive
Configuring the wait-to-restore time for the ERPS ring instance	`wrt-time <value>`	The wait-to-restore timer. The value ranges from 5 to 12 (unit: minute).	Mandatory	5	5
Configuring the hold-off time for the ERPS ring instance	`holdoff-time <value>`	The hold-off timer. The value ranges from 0 to 10000 (unit: millisecond).	Mandatory	1000	1000

Procedure	Parameter	Description	Attribute	Example	
				Ring 1	Ring 2
Configuring the guard time for the ERPS ring instance	`guard-time <value>`	The guard timer. The value ranges from 10 to 2000 (unit: millisecond).	Mandatory	500	500
Configuring properties of the first port in the ERPS ring instance	`primary-slot <value>`	No. of the first slot.	Mandatory	19	19
	`primary-port <value>`	The first uplink port.	Mandatory	3	3
	`role [common| rpl-port]`	The role of the first port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common	common
Configuring properties of the second port in the ERPS ring instance	`second-slot <value>`	The number of the second slot.	Mandatory	19	19
	`second-port <value>`	The second uplink port.	Mandatory	4	4
	`role [common| rpl-port]`	The role of the second port. It can be set to common port or RPL port. A ring instance can be configured with only one RPL port.	Mandatory	common	common
Configuring the virtual channel VLAN for the ERPS ring instance	`virtual-vlan <value>`	The virtual channel VLAN.	Mandatory	-	-

Example

1. Create the ERPS ring for Equipment 1.

```
Admin(config)#erps ring 1
Admin(config)#erps ring 2
```

2. Set Equipment 1 to common node in the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 erps-role common
Admin(config)#erps ring 2 erps-role common
```

3. Set the signaling VLAN ID to 100 for the ERPS ring instance 1, and 200 for the ERPS ring instance 2.

```
Admin(config)#erps ring 1 control-vlan 100
Admin(config)#erps ring 2 control-vlan 200
```

4. Set the management domain level to 7 for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 mel 7
Admin(config)#erps ring 2 mel 7
```

5. Associate the ERPS ring instance 1 with the VLAN instance 1, and associate the ERPS ring instance 2 with the VLAN instance 2.

```
Admin(config)#erps ring 1 protect-inst 1
Admin(config)#erps ring 2 protect-inst 2
```

6. Configure the switching mode for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 erps-mode revertive
Admin(config)#erps ring 2 erps-mode revertive
```

7. Set the wait-to-restore time to 5 minutes for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 wrt-time 5
Admin(config)#erps ring 2 wrt-time 5
```

8. Set the hold-off time to 1000 ms for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 holdoff-time 1000
Admin(config)#erps ring 2 holdoff-time 1000
```

9. Set the guard time to 500 ms for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 guard-time 500
Admin(config)#erps ring 2 guard-time 500
```

10. Set the first port of Equipment 1 to common port for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 primary-slot 19 primary-port 3 role common
Admin(config)#erps ring 2 primary-slot 19 primary-port 3 role common
```

11. Set the second port of Equipment 1 to common port for the ERPS ring instances 1 and 2.

```
Admin(config)#erps ring 1 second-slot 19 second-port 4 role common
Admin(config)#erps ring 2 second-slot 19 second-port 4 role common
Admin(config)#
```

19.4 Configuring the PON Protection

This section introduces how to configure the PON protection for the AN6001-G16 with examples.

19.4.1 Example of Configuring the PON Port Protection

This section gives an example to introduce how to configure the PON port protection.

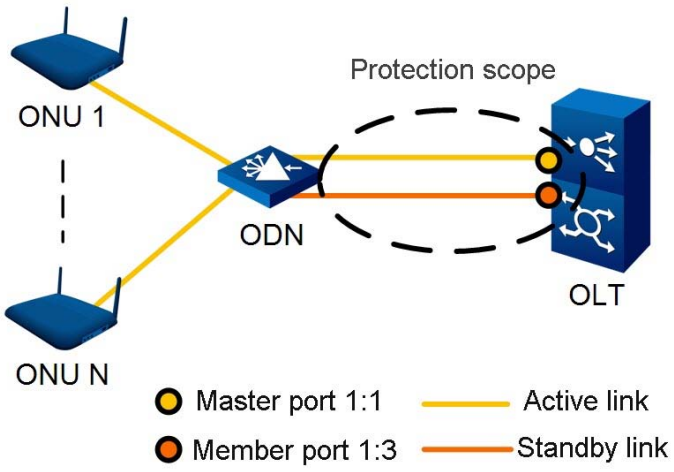
19.4.1.1 Network Scenario

Service Planning

Here we use type B single-homing protection as an example. Two PON ports (port 1:1 and port 1:3) on the same card in an OLT are configured as a PON port protection group, with port 1:1 as the master port and port 1:3 as the member port.

Network Diagram

The figure below shows the network for the PON port protection.



19.4.1.2 Configuring a PON Port Protection Group

Command Format

Configure a PON port protection group.

```
protect-group <group-no> master <frameid/slotid/portid> member <frameid/slotid/portid> {mode [type-b|type-c|type-d] auto-resume [enable|disable] <auto-resume-time>}*1
```

View a PON port protection group.

```
show protect-group <group-no>
```

Delete a PON port protection group.

```
no protect-group <group-no>
```

Planning Data

Parameter	Description	Attribute	Example
protect-group <group-no>	The PON port protection group number, ranging from 1 to 64.	Mandatory	1
master <frameid/slotid/-portid>	Master port, in the format of subrack No. / slot No. / PON port No.	Mandatory	1/1/1
member <frameid/slotid/-portid>	Member port, in the format of subrack No. / slot No. / PON port No.	Mandatory	1/1/3
mode [type-b|type-c|type-d]	Mode ◆ type-b: type B ◆ type-c: type C ◆ type-d: type D	Optional	type-b
auto-resume [enable|disable]	Enables or disables automatic return for the master port. This parameter can be configured only when type B is selected for the protection group mode.	Optional	enable
<auto-resume-time>	The WTR time (s), ranging from 180 to 3600. This parameter can be configured only when type B is selected for the protection group mode and automatic return is enabled for the master port.	Optional	300

Example

1. Configure a PON port protection group, setting port 1/1/1 as the master member and port 1/1/3 as the member port. Set the protection group mode to type B, enable automatic return for the master port and set the WTR time to 300s.

```
Admin(config)#protect-group 1 master 1/1/1 member 1/1/3 mode type-b auto-resume enable 300
Admin(config)#
```

2. View the configuration of a PON port protection group.

```
Admin(config)#show protect-group 1
----------Group [1] info----------
```

```
Group state: GEPON_PP_GROUP_WAITING_LINECARD_RESPONSE
Group mode: GEPON_PP_MODE_TYPEB
Group auto resume: enable
Group auto resume interval: 300

Master pon: slot 1 pon 1
Master pon use state: GEPON_PON_USE_STATE_DETECTING

Member pon: slot 1 pon 3
Member pon use state: GEPON_PON_USE_STATE_DETECTING
Admin(config)#
```

3. Delete a PON port protection group.

```
Admin(config)#no protect-group 1
Admin(config)#
```

19.4.2 Example of Forced Switching

When OLTs and ONUs are working normally, you can perform forced switching as needed.

- Type B protection supports the forced switching of a PON port protection group.
- Type C protection supports the forced switching of an ONU.

19.4.2.1 Forced Switching of the PON Port Protection Group

Command Format

```
protect-group force-switch <group-no>
```

Planning Data

Parameter	Description	Attribute	Example
<group-no>	The serial number of the PON port protection group	Mandatory	1

Example

Configure forced switching for the PON port protection group 1.

```
Admin(config)#protect-group force-switch 1
Admin(config)#
```

19.4.2.2 Forced Switching of the ONU

Command Format

```
onu force-switch <onuid>
```

Planning Data

Parameter	Description	Attribute	Example
<onuid>	ONU authorization No.	Mandatory	1

Example

Configure forced switching for the services over ONU 1 under PON port 3 in slot 1 of subrack 1.

```
Admin(config-if-pon-1/3/1)#onu force-switch 1
set ok!
Admin(config-if-pon-1/3/1)#
```

20 Configuring Traffic Classification

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

20.1 Background Information

Traffic classification refers to classification of packets according to their features and certain rules to differentiate the services, process the services in different ways, and provide different quality of services. For example, to provide Internet, voice and IPTV services for the same user, you need to classify the service packets into three service flows.

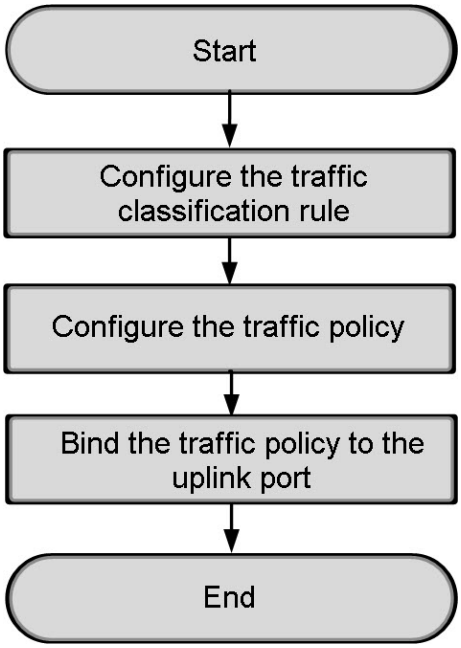
20.2 Configuration Rules

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

- 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.

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

20.3.1 Configuration Flow



20.3.2 Configuring the Traffic Classification Rules

Command Format

```
flow-rule-profile add <name> {[id] <id>}*1 {[src-mac|dst-mac|src-ipv4-addr|dst-ipv4-addr|svlan|eth-type|ip-protocol-type|cos|tos-dscp|l4-src-port|l4-dst-port|ttl|cvlan|ip-ver|traff-class|traff-label|ipv6-next-header] [range|value_mask|equal|not_equal|exist_match|not_exist_match] <value1> [<value2>|null]}*8
```

Data Planning

Parameter	Description	Attribute	Example
`flow-rule-profile add <name>`	The rule name.	Mandatory	rule0
`{[id] <id>}*1`	The rule ID. Specify the ID of the rule profile to be added. If this parameter is not configured, the system will assign a profile ID automatically. The value ranges from 1 to 256.	Optional	8

Parameter	Description	Attribute	Example
[src-mac|dst-mac|src-ipv4-addr|dst-ipv4-addr|svlan|eth-type|ip-protocol-type|cos|tos-dscp|l4-src-port|l4-dst-port|ttl|cvlan|ip-ver|traff-class|traff-label|ipv6-next-header]	The rule domain type. This parameter is used to set the rule type. You can select one from the following list of rule types: ◆ src-mac: based on the source MAC address ◆ dst-mac: based on the destination MAC address ◆ src-ipv4-addr: based on the source IPv4 address ◆ dst-ipv4-addr: based on the destination IPv4 address ◆ svlan: based on the SVLAN ◆ eth-type: based on the Ethernet type ◆ ip-protocol-type: based on the IP protocol type ◆ cos: based on the Ethernet priority ◆ tos-dscp: based on TOS/DSCP ◆ l4-src-port: based on the L4 source port number ◆ l4-dst-port: based on the L4 destination port number ◆ ttl: based on the TTL ◆ cvlan: based on the CVLAN ◆ ip-ver: based on the IP version number ◆ traff-class: based on the IPv6 traffic classification ◆ traff-label: based on the IPv6 traffic label ◆ ipv6-next-header: based on the IPv6 next header	Optional	l4-src-port
[range|value_mask|equal|not_equal|exist_match|not_exist_match]	The matching type. This parameter is used to set the logical conditions for rule matching. You can select one from the following list of matching types: ◆ equal: equal to ◆ not_equal: not equal to ◆ exist_match: existing means matching ◆ not_exist_match: not existing means matching ◆ value_mask: value plus mask ◆ range: range	Optional	equal

Parameter	Description	Attribute	Example
<value1>	The rule domain value for rule matching.	Optional	3
[<value2>|null]	The rule domain value 2 for rule matching. When the matching type is set to "range" or "value_ mask", this parameter cannot be set to "null". For other matching types, this parameter should be set to "null".	Optional	null

Example

Configure a traffic rule profile with the profile ID 8. Configure one rule (at most eight rules can be configured) for the profile, setting the rule name to rule0, the rule type to "l4-src-port" (based on the L4 source port number), the matching type to "equal", the rule domain value to "3", and the rule domain value 2 to "null".

```
Admin(config)#flow-rule-profile add rule0 id 8 l4-src-port equal 3 null
```

20.3.3 Configuring the Traffic Policy

Command Format

```
flow-policy-profile add <name> {[id] <id>}*1 {[pri] <1-12>}*1 {[acl]
[enable|disable]}*1 {[forward] [enable|disable]}*1 {[re-cos] [enable|
disable]}*1 {[cos] <0-7>}*1 {[re-dscp] [enable|disable]}*1 {[dscp] <0-63>}
*1 {[re-traff] [enable|disable]}*1 {[traff] <traff>}*1 {[re-queue] [enable|
disable]}*1 {[queue] <0-7>}*1 {[re-port] [enable|disable]}*1 {[rdport]
<port>}*1 {[flow-mirr] [enable|disable]}*1 {[mirrport] <port>}*1 {[rate-
limit] [enable|disable]}*1 {[cir] <cir>}*1 {[cbs] <cbs>}*1 {[ebs] <ebs>}*1
{[pir] <pir>}*1 {[re-vlan] [enable|disable]}*1 {[vlanact] [add|tras]}*1
{[vid] <1-4095>}*1
```

Data Planning

Parameter	Description	Attribute	Example
flow-policy-profile add <name>	The name of the policy profile.	Mandatory	policy5
{[id] <id>}*1	The ID of the policy profile.	Optional	8
{[pri] <1-12>}*1	The policy priority level, ranging from 1 to 12. The value "1" stands for the lowest priority level, and "12" the highest one.	Optional	3

Parameter	Description	Attribute	Example
{[acl] [enable| disable]}*1	The ACL function switch.	Optional	enable
{[forward] [enable| disable]}*1	The forwarding flag. Configure this item according to the network planning of the operator. It cannot be configured when the ACL function is disabled. ◆ enable: Only the traffic matching the set rule is forwarded, while other traffics are discarded. ◆ disable: The traffic matching the rule is discarded, while other traffics are forwarded.	Optional	enable
{[re-cos] [enable| disable]}*1	The CoS remarking flag. It is used to enable or disable the remarking function. The default setting is "disable".	Optional	-
{[cos] <0-7>}*1	The priority label. The value ranges from 0 to 7. This parameter cannot be configured when the CoS remarking flag is set to "disable".	Optional	-
{[re-dscp] [enable| disable]}*1	The DSCP remarking flag. The default setting is "disable".	Optional	-
{[dscp] <0-63>}*1	The DSCP. The value ranges from 0 to 63, and the default value is 0. This parameter cannot be configured when DSCP remarking is disabled.	Optional	-
{[re-traff] [enable| disable]}*1	The re-marking traffic class switch. The default setting is "disable".	Optional	-
{[traff] <traff>}*1	The communication classification. The value ranges from 0 to 255, and the default value is 0. This parameter cannot be configured when re-marking traffic class is disabled.	Optional	-
{[re-queue] [enable| disable]}*1	The queue mapping function switch. The default setting is "disable".	Optional	-
{[queue] <0-7>}*1	The queues mapped. The value ranges from 0 to 7, and the default value is 0. This parameter cannot be configured when queue mapping is disabled.	Optional	-
{[re-port] [enable| disable]}*1	The port re-direction function switch. The ID of the policy profile should be configured before this parameter is set. Otherwise, this function is disabled.	Optional	-
{[rdport] <port>}*1	The R port number. The value ranges from 13 to 18, corresponding to uplink ports 19:1 to 19:6 respectively.	Optional	-

Parameter	Description	Attribute	Example
{[flow-mirr] [enable|disable]}*1	The port mirroring function switch. The ID of the policy profile should be configured before this parameter is set. Otherwise, this function is disabled.	Optional	-
{[mirrport] <port>}*1	The M port number. The value ranges from 13 to 18, corresponding to uplink ports 19:1 to 19:6 respectively.	Optional	-
{[rate-limit] [enable|disable]}*1	The rate limit switch. The default setting is "disable".	Optional	-
{[cir] <cir>}*1	The committed information rate (unit: kbit/s). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[cbs] <cbs>}*1	The committed burst size (unit: Byte). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[ebs] <ebs>}*1	The excess burst size (unit: Byte). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[pir] <pir>}*1	The peak information rate (unit: kbit/s). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[re-vlan] [enable|disable]}*1	The VLAN remarking function switch.	Optional	-
{[vlanact] [add|tras]}*1	The VLAN action. ◆ add: adding ◆ tras: translation	Optional	-
{[vid] <1-4095>}*1	The VLAN value.	Optional	-

Example

Configure a traffic policy profile with the name policy5, the ID 8, and the priority 3. Enable the ACL, set the forwarding flag to "enable" (forward the traffics matching the rules and discard those that do not match), and use default settings for all the other policy items.

```
Admin(config)#flow-policy-profile add policy5 id 8 pri 3 acl enable forward enable
```

```
Admin(config)#
```

20.3.4 Binding the Traffic Policy to an Uplink Port

Command Format

```
flow-policy <frameid/slotid/portid> {policy-profile <policy-profile-id>
rule-profile <rule-profile-id>}*8
```

Planning Data

Parameter	Description	Attribute	Example
<frameid/slotid/-portid>	The subrack No. / slot No. / port No.	Mandatory	1/19/1
policy-profile <policy-profile-id>	The ID of the traffic policy profile	Optional	8
rule-profile <rule-profile-id>	The ID of the traffic rule profile	Optional	8

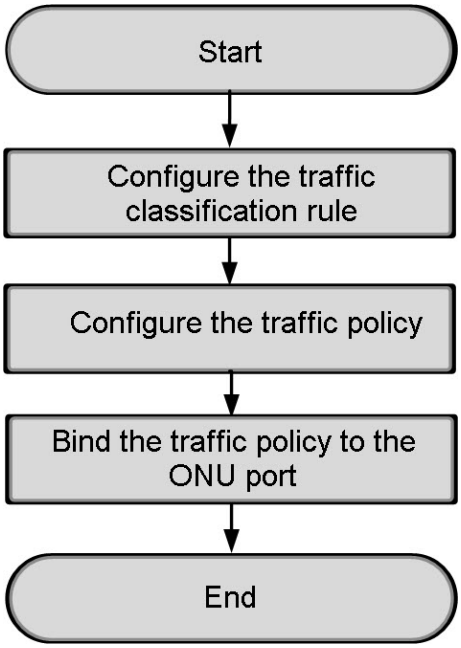
Example

Bind the traffic policy to Port 1 in Slot 19 of Subrack 1, setting the traffic policy profile ID to 8 and the traffic rule profile ID to 8.

```
Admin(config)#flow-policy 1/19/1 policy-profile 8 rule-profile 8
Admin(config)#
```

20.4 Configuration Example for Traffic Classification Based on the SVLAN

20.4.1 Configuration Flow



20.4.2 Configuring Traffic Classification Rules

Command Format

```
flow-rule-profile add <name> {[id] <id>}*1 {[src-mac|dst-mac|src-ipv4-
addr|dst-ipv4-addr|svlan|eth-type|ip-protocol-type|cos|tos-dscp|l4-src-
port|l4-dst-port|ttl|cvlan|ip-ver|traff-class|traff-label|ipv6-next-
header] [range|value_mask|equal|not_equal|exist_match|not_exist_match]
<value1> [<value2>|null]}*8
```

Planning Data

Parameter	Description	Attribute	Example
`flow-rule-profile add <name>`	Rule name	Mandatory	rule1
`{[id] <id>}*1`	Rule ID. Specify the ID of the rule profile to be added. If this parameter is not configured, the system assigns a profile ID automatically. The value ranges from 1 to 256.	Optional	8
`[src-mac|dst-mac|src-ipv4-addr|dst-ipv4-addr|svlan|eth-type|ip-protocol-type|cos|tos-dscp|l4-src-port|l4-dst-port|ttl|cvlan|ip-ver|traff-class|traff-label|ipv6-next-header]`	Rule domain type. Set the rule type. You can select a rule from the following list: ◆ src-mac: based on the source MAC address ◆ dst-mac: based on the destination MAC address ◆ src-ipv4-addr: based on the source IPv4 address ◆ dst-ipv4-addr: based on the destination IPv4 address ◆ svlan: based on the SVLAN ◆ eth-type: based on the Ethernet type ◆ ip-protocol-type: based on the IP protocol type ◆ cos: based on the Ethernet priority ◆ tos-dscp: based on the TOS/DSCP ◆ l4-src-port: based on the L4 source port number ◆ l4-dst-port: based on the L4 destination port number ◆ ttl: based on the TTL ◆ cvlan: based on the CVLAN ◆ ip-ver: based on the IP version number ◆ traff-class: based on the IPv6 traffic class ◆ traff-label: based on the IPv6 traffic label ◆ ipv6-next-header: based on the IPv6 next header	Optional	svlan

Parameter	Description	Attribute	Example
[range|value_mask|equal|not_equal|exist_match|not_exist_match]	Matching type. Set the logical condition for rule matching. You can select a matching type from the following list: ◆ equal ◆ not_equal: not equal to ◆ exist_match: existing means matching ◆ not_exist_match: not existing means matching ◆ value_mask: value plus mask ◆ range	Optional	equal
<value1>	Rule domain value for rule matching	Optional	300
[<value2>|null]	Rule domain value 2 for rule matching. Set it to "null" for matching types other than "range" and "value_mask".	Optional	null

Example

Configure a traffic rule profile with the ID 8. Configure a rule (up to eight rules can be configured) for the profile, setting the rule name to rule1, the rule type to be based on SVLAN, the matching type to equal, the rule domain value to 300, and the rule domain value 2 to null.

```
Admin(config)#flow-rule-profile add rule1 id 8 svlan equal 300 null
```

20.4.3 Configuring the Traffic Policy

Command Format

```
flow-policy-profile add <name> {[id] <id>}*1 {[pri] <1-12>}*1 {[acl] [enable|disable]}*1 {[forward] [enable|disable]}*1 {[re-cos] [enable|disable]}*1 {[cos] <0-7>}*1 {[re-dscp] [enable|disable]}*1 {[dscp] <0-63>}*1 {[re-traff] [enable|disable]}*1 {[traff] <traff>}*1 {[re-queue] [enable|disable]}*1 {[queue] <0-7>}*1 {[re-port] [enable|disable]}*1 {[rdport] <port>}*1 {[flow-mirr] [enable|disable]}*1 {[mirrport] <port>}*1 {[rate-limit] [enable|disable]}*1 {[cir] <cir>}*1 {[cbs] <cbs>}*1 {[ebs] <ebs>}*1 {[pir] <pir>}*1 {[re-vlan] [enable|disable]}*1 {[vlanact] [add|tras]}*1 {[vid] <1-4095>}*1
```

Data Planning

Parameter	Description	Attribute	Example
`flow-policy-profile add <name>`	The name of the policy profile.	Mandatory	policy5
`{[id] <id>}*1`	The ID of the policy profile.	Optional	8
`{[pri] <1-12>}*1`	The policy priority level, ranging from 1 to 12. The value "1" stands for the lowest priority level, and "12" the highest one.	Optional	3
`{[acl] [enable| disable]}*1`	The ACL function switch.	Optional	enable
`{[forward] [enable| disable]}*1`	The forwarding flag. Configure this item according to the network planning of the operator. It cannot be configured when the ACL function is disabled. ◆ enable: Only the traffic matching the set rule is forwarded, while other traffics are discarded. ◆ disable: The traffic matching the rule is discarded, while other traffics are forwarded.	Optional	enable
`{[re-cos] [enable| disable]}*1`	The CoS remarking flag. It is used to enable or disable the remarking function. The default setting is "disable".	Optional	-
`{[cos] <0-7>}*1`	The priority label. The value ranges from 0 to 7. This parameter cannot be configured when the CoS remarking flag is set to "disable".	Optional	-
`{[re-dscp] [enable| disable]}*1`	The DSCP remarking flag. The default setting is "disable".	Optional	-
`{[dscp] <0-63>}*1`	The DSCP. The value ranges from 0 to 63, and the default value is 0. This parameter cannot be configured when DSCP remarking is disabled.	Optional	-
`{[re-traff] [enable| disable]}*1`	The re-marking traffic class switch. The default setting is "disable".	Optional	-
`{[traff] <traff>}*1`	The communication classification. The value ranges from 0 to 255, and the default value is 0. This parameter cannot be configured when re-marking traffic class is disabled.	Optional	-
`{[re-queue] [enable| disable]}*1`	The queue mapping function switch. The default setting is "disable".	Optional	-
`{[queue] <0-7>}*1`	The queues mapped. The value ranges from 0 to 7, and the default value is 0. This parameter cannot be configured when queue mapping is disabled.	Optional	-

Parameter	Description	Attribute	Example
{[re-port] [enable|disable]}*1	The port re-direction function switch. The ID of the policy profile should be configured before this parameter is set. Otherwise, this function is disabled.	Optional	-
{[rdport] <port>}*1	The R port number. The value ranges from 13 to 18, corresponding to uplink ports 19:1 to 19:6 respectively.	Optional	-
{[flow-mirr] [enable|disable]}*1	The port mirroring function switch. The ID of the policy profile should be configured before this parameter is set. Otherwise, this function is disabled.	Optional	-
{[mirrport] <port>}*1	The M port number. The value ranges from 13 to 18, corresponding to uplink ports 19:1 to 19:6 respectively.	Optional	-
{[rate-limit] [enable|disable]}*1	The rate limit switch. The default setting is "disable".	Optional	-
{[cir] <cir>}*1	The committed information rate (unit: kbit/s). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[cbs] <cbs>}*1	The committed burst size (unit: Byte). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[ebs] <ebs>}*1	The excess burst size (unit: Byte). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[pir] <pir>}*1	The peak information rate (unit: kbit/s). The value ranges from 0 to 2147483647, and the default value is 0. This parameter cannot be configured when the rate limit is disabled.	Optional	-
{[re-vlan] [enable|disable]}*1	The VLAN remarking function switch.	Optional	-
{[vlanact] [add|tras]}*1	The VLAN action. ◆ add: adding ◆ tras: translation	Optional	-
{[vid] <1-4095>}*1	The VLAN value.	Optional	-

Example

Configure a traffic policy profile with the name policy5, the ID 8, and the priority 3. Enable the ACL, set the forwarding flag to "enable" (forward the traffics matching the rules and discard those that do not match), and use default settings for all the other policy items.

```
Admin(config)#flow-policy-profile add policy5 id 8 pri 3 acl enable forward enable
Admin(config)#
```

20.4.4 Binding a Traffic Policy to an ONU Port

Command Format

```
onu flow-policy-profile <onuid> port <portno> {upstream-profile
<uppolicyprf> downstream-profile <downpolicyprf> upstream-rule-profile
<upruleprf> downstream-rule-profile <downruleprf>}*8
```

Planning Data

Parameter	Description	Attribute	Example
<onuid>	ONU authorization number, ranging from 1 to 128	Mandatory	1
port <portno>	Port number, ranging from 1 to 32	Mandatory	1
upstream-profile <uppolicyprf>	ID of the uplink traffic policy profile	Optional	8
downstream-profile <downpolicyprf>	ID of the downlink traffic policy profile	Optional	8
upstream-rule-profile <upruleprf>	ID of the uplink traffic rule profile	Optional	8
downstream-rule-profile <downruleprf>	ID of the downlink traffic rule profile	Optional	8

Example

Bind a traffic policy to port 1 of ONU 1 connected to port 1 in slot 1 of subrack 1. Set uplink and downlink traffic policy profile IDs and uplink and downlink traffic rule profile IDs to 8.

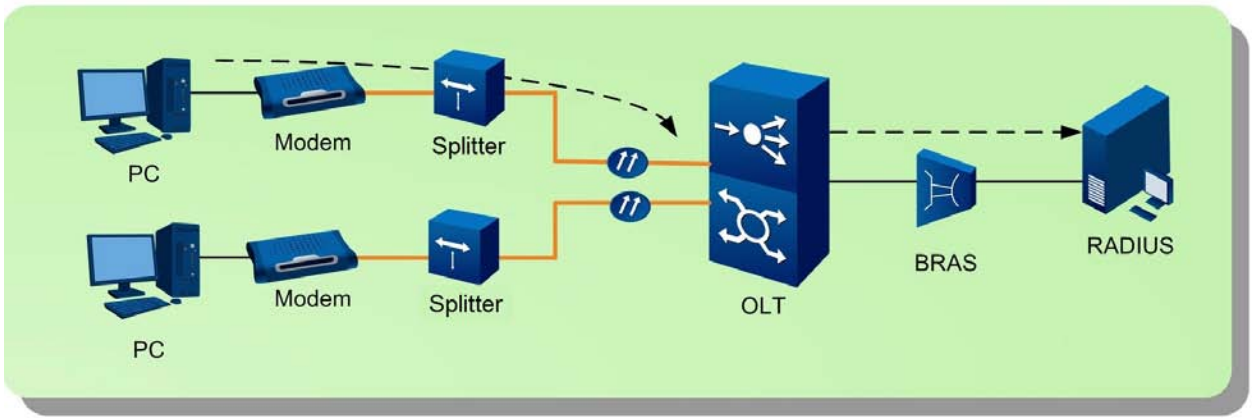
```
Admin(config-if-pon-1/1/1)#onu flow-policy-profile 1 port 1 upstream-profile 8
downstream-profile 8 upstream-rule-profile 8 downstream-rule-profile 8
Admin(config-if-pon-1/1/1)#
```

21 Configuring Subscriber Line Identifiers

- Background Information
- Configuration Rules
- Example of Configuring Subscriber Line Identifiers

21.1 Background Information

The figure below illustrates the signal flow of subscriber line identifiers.



1. The OLT 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 OLT equipment 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 forward them to the remote authorization dial-in user service (RADIUS) server.
3. The RADIUS server performs the authentication, authorization and accounting (AAA) function based on the identifier information.

21.2 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 21-1 lists the custom identifier variables defined by the system.

Table 21-1 Custom Identifier Variables

Identifier	Meaning	Identifier	Meaning
%s	User outer VLAN	%o	ONU authorization No.
%c	User inner VLAN	%n	ONU type
%a	Access node identifier	%T	MDU ONU slot No.
%r	Rack No. of the access node	%M	MDU ONU sub-slot No.
%f	Subrack No. of the access node	%P	MDU ONU UNI port No.
%S	Slot No. of the access node	%t	ONU user port type
%p	PON port No. of the access node	%X	Port VPI or SVLAN
%m	ONU identifier (MAC) of the access node	%x	Port VCI or CVLAN
%u	Uplink port type	%I	IAD IP address
%L	Service card type	%A	IAD MAC address
%O	IP address of the OLT management VLAN	%B	Access 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 21-2.

Table 21-2 List of Delimiters

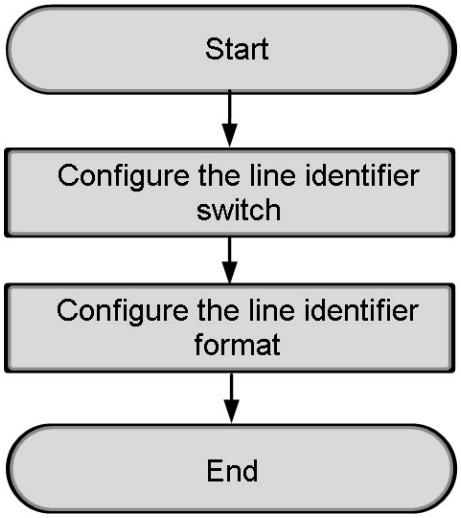
Delimiter	Meaning
	Space
.	Decimal point
/	Slash
;	Semicolon
:	Colon
{	Open curly bracket
}	Close curly bracket
<	Open angle bracket
>	Close angle bracket
[	Open square bracket
]	Close square bracket

  - 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.

21.3 Example of Configuring Subscriber Line Identifiers

21.3.1 Configuration Flow



21.3.2 Configuring the Line Identifier Switch

Command Format

Enable or disable the DHCP Option 82 function.

```
dhcp option82 [enable|disable]
```

Enable or disable the PPPoE Plus function.

```
pppoe-plus [enable|disable]
```

Enable or disable the DHCP Option18 / Option37 function.

```
dhcp [option18|option37] [enable|disable]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Enabling or disabling the DHCP Option 82 function	`dhcp option82 [enable|disable]`	◆ enable: Enable the function. ◆ disable: Disable the function.	Mandatory	enable
Enabling or disabling the PPPoE Plus function	`pppoe-plus [enable|disable]`	◆ enable: Enable the function. ◆ disable: Disable the function.	Mandatory	disable
Enabling or disabling the DHCP Option18 / Option37 function	`[option18|option37]`	◆ option18: the Option18 service ◆ option37: the Option37 service	Mandatory	option18
	`[enable|disable]`	◆ enable ◆ disable	Mandatory	enable

Example

1. Enable the DHCP Option 82 function.

```
Admin(config)#dhcp option82 enable
```

2. Disable the PPPoE Plus function.

```
Admin(config)#pppoe-plus disable
```

3. Enable the DHCP Option 18 function.

```
Admin(config)#dhcp option18 enable
Admin(config)#
```

21.3.3 Configuring the Line Identifier Format

Command Format

```
line [circuit-id|remote-id] format [<format-str>|ctc|cnc]
```

Planning Data

Parameter	Description	Attribute	Example		
[circuit-id|remote-id]	◆ circuit-id: the line identifier format ◆ remote-id: the remote end identifier format	Mandatory	circuit-id	circuit-id	remote-id
format [<format-str>|ctc|cnc]	◆ <format-str>: the custom format ◆ ctc: the CTC format, which means the standard of China Telecom Corporation ◆ cnc: the CNC format, which means the standard of China Netcom Corporation	Mandatory	ctc	/%a.%b.%L/%_fiberhome	/%a.%b.%L/%_fiberhome

Example

1. Set the line identifier format to "ctc".

```
Admin(config)#line circuit-id format ctc
```

2. Set the line identifier to the custom format "/%a.%b.%L/%_fiberhome".

```
Admin(config)#line circuit-id format /%a.%b.%L/%_fiberhome
Format accepted.
Admin(config)#
```

3. Set the remote end identifier format to "/%a.%b.%L/%_fiberhome".

```
Admin(config)#line remote-id format /%a.%b.%L/%_fiberhome
Admin(config)#
```

22 Configuring TACACS+

- Background Information
- Configuration Flow
- Configuring Information about the TACACS+ Server
- Configuring the Authentication Mode
- Configuring the Authorization Mode
- Configuring the Accounting Mode

22.1 Background Information

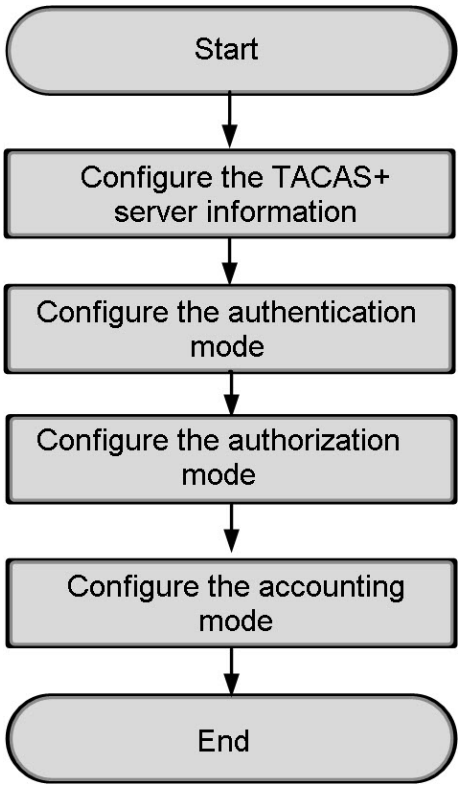
The TACACS+ (Terminal Access Controller Access-Control System Plus) protocol is a user access control protocol based on the C-S mode. The protocol is mainly used for user authentication, authorization and accounting (i.e., the AAA function). The protocol is based on TCP for service transmission and uses 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 OLT serves as the access equipment to allow the communication between the user and the TACACS+ server. It authenticates, authorizes and accounts the user access according to the user information on the TACACS+ server to enable user access control based on the TACACS+ protocol.

22.2 Configuration Flow



22.3 Configuring Information about the TACACS+ Server

Command Format

```
tacacs-server host <A.B.C.D> [key|port|timeout] <value>
```

Planning Data

Parameter	Description	Attribute	Example		
`host <A.B.C.D>`	The destination IP address of IP messages.	Mandatory	10.10.10.10	10.10.10.10	10.10.10.10
`[key|port|timeout]`	◆ key: the encrypted key for interaction with the server. The key contains 0 to 255 characters. ◆ port: the port for interaction with the server. The value ranges from 1 to 65535. ◆ timeout: the timeout period for establishing connection with the server. The value ranges from 3 to 10 seconds.	Mandatory	port	key	timeout
`<value>`	Value	Mandatory	49	123	10

Example

1. Configure the TACACS+ sever, setting its IP address to 10.10.10.10 and the interaction port to 49.

```
Admin(config-aaa)#tacacs-server host 10.10.10.10 port 49
server_ip:10.10.10.10
Admin(config-aaa)#
```

2. Configure the TACACS+ sever, setting its IP address to 10.10.10.10 and the key to 123.

```
Admin(config-aaa)#tacacs-server host 10.10.10.10 key 123
server_ip:10.10.10.10
Admin(config-aaa)#
```

3. Configure the TACACS+ sever, setting its IP address to 10.10.10.10 and the timeout period to 10 seconds.

```
Admin(config-aaa)#tacacs-server host 10.10.10.10 timeout 10
server_ip:10.10.10.10
Admin(config-aaa)#
```

22.4 Configuring the Authentication Mode

Command Format

```
aaa authentication-mode [local|radius|tacacs]
```

Planning Data

Parameter	Description	Attribute	Example
[local|radius|tacacs]	◆ local: the local authentication mode ◆ radius: the RADIUS authentication mode ◆ tacacs: the TACACS authentication mode	Mandatory	tacacs

Example

Set the authentication mode to TACACS.

```
Admin(config-aaa)#aaa authentication-mode tacacs
Admin(config-aaa)#
```

22.5 Configuring the Authorization Mode

Command Format

Configure the user authorization mode.

```
aaa authorization-mode [none|tacacs]
```

Configure the command line authorization mode.

```
aaa authorization-mode command [none|tacacs]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the user authorization mode	[none|tacacs]	◆ none: the non-authorization mode ◆ tacas: the TACACS authorization mode	Mandatory	tacacs
Configuring the command line authorization mode	command [none|tacacs]	◆ none: the non-authorization mode ◆ tacas: the TACACS authorization mode	Mandatory	tacacs

Example

1. Set the user authorization mode to TACACS.

```
Admin(config-aaa)#aaa authorization-mode tacacs
```

2. Set the command line authorization mode to TACACS.

```
Admin(config-aaa)#aaa authorization-mode command tacacs
```

```
Admin(config-aaa)#
```

22.6 Configuring the Accounting Mode

Command Format

Configure the user accounting mode.

```
aaa accounting-mode [none|radius|tacacs]
```

Configure the command line accounting mode.

```
aaa accounting-mode command [none|tacacs]
```

Planning Data

Procedure	Parameter	Description	Attribute	Example
Configuring the user accounting mode	`[none|radius|tacacs]`	◆ none: the non-accounting mode ◆ radius: the RADIUS accounting mode ◆ tacacs: the TACACS accounting mode	Mandatory	tacacs
Configuring the command line accounting mode	`command [none|tacacs]`	◆ none: the non-accounting mode ◆ tacacs: the TACACS accounting mode	Mandatory	tacacs

Example

1. Set the user accounting mode to TACACS.

```
Admin(config-aaa)#aaa accounting-mode tacacs
```

2. Set the command line accounting mode to TACACS.

```
Admin(config-aaa)#aaa accounting-mode command tacacs
Admin(config-aaa)#
```

23 Configuring RADIUS

- Background Information
- Configuration Flow
- Configuring the RADIUS Authentication Mode
- Configuring the RADIUS Authentication Information

23.1 Background Information

The OLT equipment 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 are 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 sends the user's authority information to the RADIUS client end via the access-accept packets. If the authentication fails, the RADIUS server returns 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.

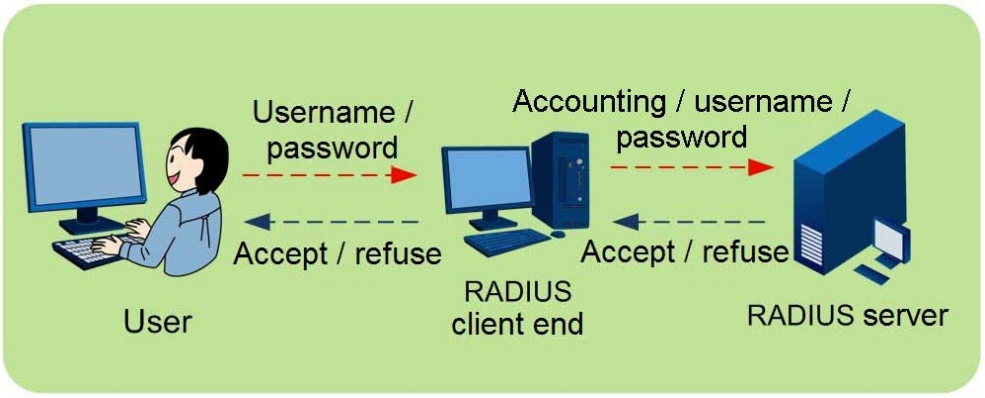
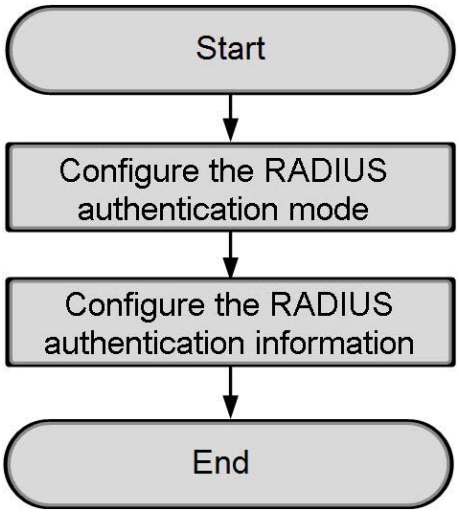


Figure 23-1 Principle of RADIUS Protocol Interaction

23.2 Configuration Flow



23.3 Configuring the RADIUS Authentication Mode

Command Format

```
aaa authentication-mode [local|radius|tacacs]
```

Planning Data

Parameter	Description	Attribute	Example
[local|radius|tacacs]	◆ local: the local authentication mode ◆ radius: the RADIUS authentication mode ◆ tacacs: the TACACS authentication mode	Mandatory	radius

Example

Set the authentication mode to RADIUS.

```
Admin(config-aaa)#aaa authentication-mode radius
Admin(config-aaa)#
```

23.4 Configuring the RADIUS Authentication Information

Command Format

```
radius server ip-address <ipaddr> [key|auth-port|acct-port|timeout|
retransmit] <value>
```

Data Planning

Parameter	Description	Attribute	Example
ip-address <ipaddr>	The IP address of the RADIUS authentication server.	Mandatory	10.1.1.1
key	The key.	Mandatory	123456
auth-port	The port number of the authentication server, ranging from 1 to 65535.	Optional	1812
acct-port	The port number of the accounting server, ranging from 1 to 65535.	Optional	1813
timeout	The timeout period (second), ranging from 3 to 10.	Optional	10
retransmit	The retransmission times, ranging from 1 to 5.	Optional	1

Example

1. Configure the IP address of the RADIUS authentication server to 10.1.1.1 and the key to 123456.

```
Admin(config)#radius server ip-address 10.1.1.1 key 123456
```

2. Configure the IP address of the RADIUS authentication server to 10.1.1.1 and the authentication server port to 1812.

```
Admin(config)#radius server ip-address 10.1.1.1 auth-port 1812
```

3. Configure the IP address of the RADIUS authentication server to 10.1.1.1 and the port of the accounting server to 1813.

```
Admin(config)#radius server ip-address 10.1.1.1 acct-port 1813
```

4. Configure the IP address of the RADIUS authentication server to 10.1.1.1 and the timeout period to 10 seconds.

```
Admin(config)#radius server ip-address 10.1.1.1 timeout 10
```

5. Configure the IP address of the RADIUS authentication server to 10.1.1.1 and the retransmission times to 1.

```
Admin(config)#radius server ip-address 10.1.1.1 retransmit 1
Admin(config)#
```

24 Configuring Environment Monitoring and Discharge Test

- ☑ Configuring Environment Monitoring
- ☑ Configuring the Discharge Test

24.1 Configuring Environment Monitoring

24.1.1 Configuring Environment Monitoring Parameters

Command Format

Configure the environment monitoring parameters.

```
hcu bat-cap <batcap> sound-sw [enable|disable] bat-coef <batcoef> bat-fill <batfill> bat-limit <batlimit> bat-cir <batcir> bat-time <battime> bat-stop <batstop> temp-coef <tempcoef> bat-bas <batbas> bat-adjust <batadjust> bat-temp <battemp> com-float <comfloat> com-equal <comqueal> com-num <comnum> bat-vol <batvol> load-vol <loadvol> rect-cur <rectcur> batdis2vol <batdisvol> batdis2time <batdistime> batdis2cap <batdiscap>
```

View the environment monitoring parameters.

```
show hcu config
```

Planning Data

Parameter	Description	Attribute	Example
bat-cap <batcap>	Battery capacity (AH). The value ranges from 0 to 100.	Mandatory	100
sound-sw [enable|disable]	Alarm sound switch. ◆ enable ◆ disable	Mandatory	disable
bat-coef <batcoef>	Battery recharge coefficient (× 0.1). The value ranges from 0 to 9999.	Mandatory	10
bat-fill <batfill>	Battery charge threshold value (× 0.1). The value ranges from 0 to 9999.	Mandatory	20
bat-limit <batlimit>	Battery charge limiting current (× 0.1 A). The value ranges from 0 to 9999.	Mandatory	30
bat-cir <batcir>	Battery charge circle (× 0.1 H). The value ranges from 0 to 9999.	Mandatory	30
bat-time <battime>	Battery charge time (× 0.1 H). The value ranges from 0 to 9999.	Mandatory	10
bat-stop <batstop>	Battery stop-charge time (× 0.1 H). The value ranges from 0 to 9999.	Mandatory	20
temp-coef <tempcoef>	Battery temperature compensation coefficient (× 0. 1). The value ranges from 0 to 9999.	Mandatory	100

Parameter	Description	Attribute	Example
bat-bas <batbas>	Battery charge reference temperature (× 0.1℃). The value ranges from 0 to 390.	Mandatory	200
bat-adjust <batadjust>	Charge voltage adjustment rate (× 0.1). The value ranges from 0 to 9999.	Mandatory	200
bat-temp <battemp>	Charge temperature adjustment rate (× 0.1). The value ranges from 0 to 9999.	Mandatory	3000
com-float <comfloat>	Floating charge voltage for the rectifier module (× 0.1 V). The value ranges from 430 to 560.	Mandatory	560
com-equal <comqueal>	Equalized charge voltage for the rectifier module (× 0.1 V). The value ranges from 430 to 570.	Mandatory	570
com-num <comnum>	Number of the rectifier modules. The value ranges from 0 to 4.	Mandatory	2
bat-vol <batvol>	Battery cut-off voltage (× 0.1 V). The value ranges from 400 to 520.	Mandatory	470
load-vol <loadvol>	Load cut-off voltage (× 0.1 V). The value ranges from 400 to 560.	Mandatory	500
rect-cur <rectcur>	Limiting current for the rectifier module (× 0.1 A). The value ranges from 20 to 550.	Mandatory	400
batdis2vol <batdisvol>	Voltage for the battery switching from discharge to equalized charge (× 0.1 V). The value ranges from 430 to 510.	Mandatory	430
batdis2time <batdistime>	Time for the battery switching from discharge to equalized charge (min). The value ranges from 300 to 600.	Mandatory	320
batdis2cap <batdiscap>	Capacity for the battery switching from discharge to equalized charge (× 0.1%). The value ranges from 100 to 900.	Mandatory	600

Example

1. Configure the environment monitoring parameters.

```
Admin(config)#hcu bat-cap 100 sound-sw disable bat-coef 10 bat-fill 20 bat-limit 30 bat-cir 30 bat-time 10 bat-stop 20 temp-coef 100 bat-bas 200 bat-adjust 200 bat-temp 3000 com-float 560 com-equal 570 com-num 2 bat-vol 470 load-vol 500 rect-cur 400 batdis2vol 430 batdis2time 320 batdis2cap 600
Set hcu config para success!
Admin(config)#
```

2. View the environment monitoring parameters.

```
Admin(config)#show hcu config
```

```
Show hcu parameter config begin:
 battery capacity = 100.0 %
 sound alarm switch = disable
 batteryfill back coefficient value = 1.0
 batteryfill value = 2.0
 batteryfill limit current value = 3.0
 batteryfill circle value = 3.0
 batteryfill time value = 1.0
 batteryfill stop time = 2.0
 temperature compensate coefficient = 10.0
 batteryfill basic temperature = 20.0
 batteryfill voltage adjust rate = 20.0
 batteryfill temperature adjust rate = 300.0
 commonte float charge voltage = 56.0
 commonte equal charge voltage = 57.0
 commonte number = 2
 battery switch voltage = 47.0
 load switch voltage = 50.0
 rect limit current = 40.0
 battery discharge 2 equal charge voltage = 43.0
 battery discharge 2 equal charge time = 32.0
 battery discharge 2 equal charge capacity = 60.0
finished
Admin(config)#
```

24.1.2 Configuring the Charging Mode

Command Format

```
hcu charging-mode [float|equal]
```

Planning Data

Parameter	Description	Attribute	Example
`charging-mode [float|equal]`	Charging mode ◆ float: floating charge ◆ equal: equalized charge	Mandatory	float

Example

Set the charging mode to floating charge.

```
Admin(config)#hcu charging-mode float
Set hcu charging mode float success!
Admin(config)#
```

24.1.3 Enabling the Rectifier Module

Command Format

```
hcu rectifier <rectno> [enable|disable]
```

Planning Data

Parameter	Description	Attribute	Example
rectifier <rectno>	Number of the rectifier modules. The value ranges from 1 to 4.	Mandatory	1
[enable|disable]	State of being enabled / disabled. ◆ enable ◆ disable	Mandatory	enable

Example

Enable the No. 1 rectifier module.

```
Admin(config)#hcu rectifier 1 enable
Set rect 1 switch enable success!
Admin(config)#
```

24.1.4 Checking the HCU Device Status

Command Format

```
show hcu power-supply-status
```

Example

```
Admin(config)#show hcu power-supply-status
show HCU power supply status begin!
 Power Supply Status = Rectifier module supply
 charging mode = float
 HCU format = AN4802
 SN number = 201408290001
 Contactor status: none
```

```
 Software version: 0.1
 Hardware version: 2.0
 ModuleNO 1  Rectifier format EPA30  enable
 ModuleNO 2  not exist
 ModuleNO 3  not exist
 ModuleNO 4  not exist
finished!
Admin(config)#
```

Result Description

Parameter	Description
Power Supply Status	Power supply status
charging mode	Charging mode
HCU format	HCU model number
SN number	Sequence number
Contactor status	Current status of the contactor
Software version	Software version
Hardware version	Hardware version

24.1.5 Checking the Instant Performance of the HCU Card

Command Format

```
show hcu card
```

Example

```
Admin(config)#show hcu card
DC_voltage = 56.0 V
total_load_current = 0.0 A
total_battery_current = 0.0 A
system_temp = 25.0 Celsius
system_humidity = 30.0 %rh
AC_voltage_S = 0.0 V
AC_voltage_T = 0.0 V
AC_current = 0.0 A
AC_frequency = 0.0 Hz
total_output_current = 0.1 A
battery_temp = 25.0 Celsius
battery_voltage = 0.0 V
```

```
battery_humidity = 0.0 %rh
AC_voltage_R = 218.8 V
battery_capacity = 0.0 %
storage battery status: Float charge
show HCU card enviromental parameter finished!
Admin(config)#
```

Result Description

Parameter	Description
DC_voltage	DC voltage (V)
total_load_current	Total load current (A)
total_battery_current	Total battery current (A)
system_temp	System temperature (℃)
system_humidity	Relative humidity (%RH)
AC_voltage_R	R-phase AC voltage (V)
AC_voltage_S	S-phase AC voltage (V)
AC_voltage_T	T-phase AC voltage (V)
AC_current	AC current (A)
AC_frequency	AC frequency (HZ)
total_output_current	Total system output current (A)
battery_temp	Battery temperature (℃)
battery_voltage	Battery voltage (V)
battery_humidity	Battery humidity (%RH)
battery_capacity	Battery capacity (%)
storage battery status	Storage battery status

24.1.6 Checking the Instant Performance of the Rectifier Module

Command Format

```
show hcu rectifier <rectno>
```

Planning Data

Parameter	Description	Attribute	Example
rectifier <rectno>	Number of the rectifier module. The value ranges from 1 to 4.	Mandatory	1

Example

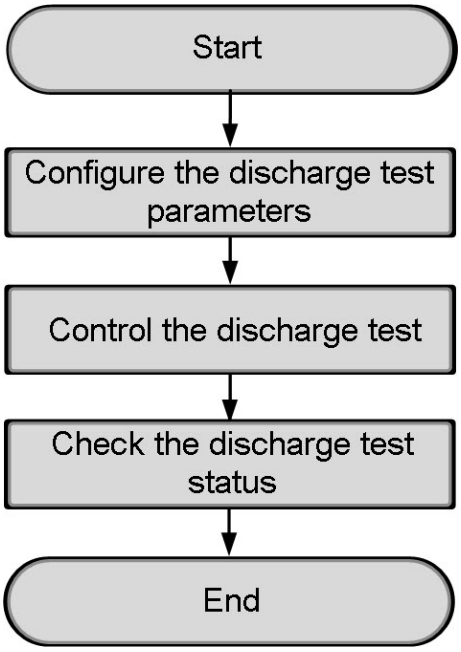
```
Admin(config)#show hcu rectifier 1
show HCU rectifier 1 enviromental parameter begin!
rect_voltage = 55.7 V
rect_current = 0.1 A
rect_temp = 39.0 Celsius
show HCU rectifier 1 enviromental parameter finished!
Admin(config)#
```

Result Description

Parameter	Description
rect_voltage	Voltage of the rectifier module (V)
rect_current	Current of the rectifier module (A)
rect_temp	Temperature of the rectifier module (℃)

24.2 Configuring the Discharge Test

24.2.1 Configuration Flow



24.2.2 Configuring the Discharge Test Parameters

Command Format

```
hcu discharge vol <voltage> time <timing>
```

Planning Data

Parameter	Description	Attribute	Example
vol <voltage>	Voltage at the end of discharge (× 0.1 V). The value ranges from 450 to 520.	Mandatory	482
time <timing>	Discharge time (in minutes). The value ranges from 1 to 300.	Mandatory	10

Example

Set the voltage at the end of discharge to 48.2 V and the discharge time to 10 minutes.

```
Admin(config)#hcu discharge vol 482 time 10
Set discharging test para voltage 48.2 V time 10 minute success!
Admin(config)#
```

24.2.3 Controlling the Discharge Test

Command Format

```
hcu discharge [start|end]
```

Planning Data

Parameter	Description	Attribute	Example
discharge [start|end]	Discharge control ◆ start ◆ end	Mandatory	start

Example

Start the discharge test.

```
Admin(config)#hcu discharge start
Set discharging test status Start success!
```

```
Admin(config)#
```

24.2.4 Checking the Discharge Test Status

Command Format

```
show hcu discharge-test-control
```

Example

```
Admin(config)#show hcu discharge-test-control
show HCU Discharge test control!
Discharge end voltage : 48.2 V
Discharge time : 10 minute
status : End
finished!
Admin(config)#
```

Result Description

Parameter	Description
Discharge end voltage	Voltage at the end of discharge (V)
Discharge time	Discharge time (in minutes)
status	Discharge test status

25 Detecting the Optical Power

- Background Information
- Viewing the Information about the Optical Module at the PON Port
- Viewing Optical Module Parameters of the ONU

25.1 Background Information

GPON Optical Module

Item	Specification	
Module code	2.5/1.25G-20km-GPON OLT-SFP (CLASS C+)	2.5/1.25G-20km-GPON OLT-SFP (CLASS C++)
Optical module type	CLASS C+	CLASS C++
Output optical power	4 dBm to 7 dBm (room temperature)	5.5 dBm to 10 dBm (room temperature)

25.2 Viewing the Information about the Optical Module at the PON Port

Command Format

```
show optical info
```

Example

View the information about the optical module at PON Port 15 in Slot 1 of Subrack 1.

```
Admin(config-if-pon-1/1/15)#show optical info
----- PON OPTIC MODULE PAR INFO -----
NAME VALUE UNIT
----------------------------------------
TYPE : 20 (KM)
TEMPERATURE : 31.37 ('C)
VOLTAGE : 3.28 (V)
BIAS CURRENT : 29.71 (mA)
SEND POWER : 6.68 (Dbm)

ONU_NO RECV_POWER , ITEM=3
1 -16.19 (Dbm)
2 -14.63 (Dbm)
3 -16.45 (Dbm)
Admin(config-if-pon-1/1/15)#
```

Result Description

Parameter	Description
TYPE	The type of the optical module
TEMPERATURE	The temperature of the optical module
VOLTAGE	The voltage of the optical module
BIAS CURRENT	The bias current of the optical module
SEND POWER	The Tx optical power of the optical module
ONU_NO	The authorization number of the ONU under the PON port
RECV_POWER	The Rx optical power of the optical module

25.3 Viewing Optical Module Parameters of the ONU

Command Format

```
show onu optical-info <onuid>
```

Planning Data

Parameter	Description	Attribute	Example
<onuid>	ONU authorization No.	Mandatory	1

Example

```
Admin(config-if-pon-1/1/15)#show onu optical-info 1
----- ONU OPTIC MODULE PAR INFO 1.15.1-----
NAME VALUE UNIT
----------------------------------------
TYPE : 20 (KM)
TEMPERATURE : 40.91 ('C)
VOLTAGE : 3.32 (V)
BIAS CURRENT : 12.64 (mA)
SEND POWER : 2.06 (Dbm)
RECV POWER : -20.21 (Dbm)
OLT RECV POWER : -16.19 (Dbm)
Admin(config-if-pon-1/1/15)#
```

Result Description

Parameter	Description
TYPE	The type of the optical module
TEMPERATURE	The temperature of the optical module
VOLTAGE	The voltage of the optical module
BIAS CURRENT	The bias current of the optical module
SEND POWER	The Tx optical power of the optical module
RECV POWER	The Rx optical power of the optical module
OLT RECV POWER	The Rx optical power of the OLT

26 Commands for Upgrading the Equipment

- Commands for Upgrading Cards
- Commands for Upgrading ONUs
- Uploading the Configuration Data

26.1 Commands for Upgrading Cards

Command Format

```
load program [system|config|script|ver-file|boot|patch|cpld] <filename>
[tftp|ftp|sftp] <ipaddr> {<username> <password>}*1
```

Planning Data

Parameter	Description	Attribute	Example
[system|config|script|ver-file|boot|patch|cpld]	The file type ◆ system: the system image file ◆ config: the configuration file ◆ script: the batch command line file ◆ ver_file: the version file ◆ boot: the system boot file ◆ patch: the system patch file ◆ cpld: the system cpld file	Mandatory	system
<filename>	The file name	Mandatory	hb_hsoa_1000_tst.bin
[tftp|ftp|sftp]	The FTP protocol type	Mandatory	ftp
<ipaddr>	The IP address of the FTP server	Mandatory	3.3.3.100
{<username> <password>}*1	The username and password of the FTP server	Optional	1, 1

Example

Upgrade the system image file for the main control service card. The IP address of the FTP server is 3.3.3.100, the user name is 1, the password is 1, and the file name is hb_hsoa_1000_tst.bin.

```
Admin(config)#load program system hb_hsoa_1000_tst.bin ftp 3.3.3.100 1 1
```

26.2 Commands for Upgrading ONUs

Command Format

```
load onu-program <frameid/slotid/portid> <onulist> <filename> [tftp|ftp|
sftp] <ipaddr> {<username> <password>}*1
```

Planning Data

Parameter	Description	Attribute	Example
<frameid/slotid/-portid>	The subrack No. / slot No. / port No.	Mandatory	1/1/1
<onulist>	The ONU authorization No.	Mandatory	1
<filename>	The file name	Mandatory	gpop.gz
[tftp|ftp|sftp]	The FTP protocol type	Mandatory	ftp
<ipaddr>	The IP address of the FTP server	Mandatory	3.3.3.100
{<username> <password>}*1	The username and password of the FTP server	Optional	1, 1

Example

Upgrade the file for ONU 1 under PON Port 1 in Slot 1 of Subrack 1. The IP address of the FTP server is 3.3.3.100, the user name is 1, the password is 1, and the FTP file name is gpop.gz.

```
Admin(config)#load onu-program 1/1/1 1 gpop.gz ftp 3.3.3.100 1 1
Admin(config)#
```

26.3 Uploading the Configuration Data

Command Format

```
upload program [system|config|showrun|igmplog|syslog|ver_file|patch]
<filename> [ftp|sftp|tftp] <server_ipaddr> {<username> <password>}*1
```

Planning Data

Parameter	Description	Attribute	Example
[system|config|showrun|igmplog|syslog|ver_file|patch]	The file type. ◆ system: the system image file ◆ config: the configuration file ◆ showrun: the running configuration file ◆ igmplog: the multicast log file ◆ syslog: the system log file ◆ ver_file: the version file ◆ patch: the system patch file	Mandatory	config
<filename>	The file name.	Mandatory	hb_hsoa_1000_tst.bin

Parameter	Description	Attribute	Example
[ftp|sftp|tftp]	The FTP protocol type.	Mandatory	ftp
<server_ipaddr>	The IP address of the FTP server.	Mandatory	3.3.3.100
{<username> <password>}*1	The username and password of the FTP server.	Optional	1, 1

Example

Export the configuration file in the Flash to the FTP server with the IP address 3.3.3.100. Set the server user name to 1, password to 1, and system file name to "hb_hsoa_1000_tst.bin".

```
Admin(config)#upload program config hb_hsoa_1000_tst.bin ftp 3.3.3.100 1 1
Admin(config)#
```

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