Airlive

XGSPON OLT-2XGS

XGSPON OLT-2XGS-WDM

CLI UserGuide

Command line format conventions

Format	Meaning
Bold type	The command line keywords (the portion of the command excluding parameters and optional parameters replaced by actual values) are written in bold.
italic type	The command line parameter (the part of the command that must be replaced by actual values) is represented in italics.
[ ]	It means that the section enclosed with "[ ]" is optional when the command is configured.
(x - y)	Represents a numerical value in the selected range.
< x | y | ... >	Indicates selecting one from two or more options.
[x | y | ...]	Indicates one or out of two or more options.
< x | y | ... > *1	Select multiple options from two or more options, one less, and all more options.

Example:

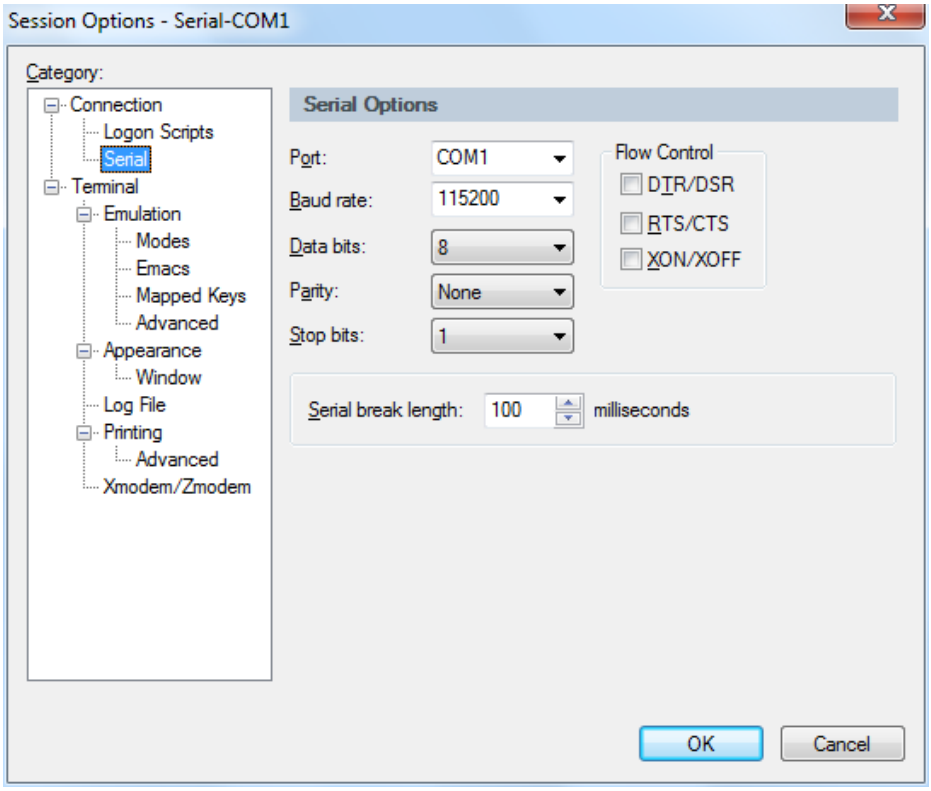
Bold type: gpon-olt(config)# **show running-config**
italic type: gpon-olt(config-aux)# **ip address** *A.B.C.D net-mask*
[ ]: gpon-olt(config)#**show pon statistics** [brief]
(x - y): gpon-olt(config)#**show vlan** (1-4094)
< x | y | ... >:
gpon-olt(config)#**erase** <web-logo|web-logo1|web-logo2|web-logo3>
[x | y | ...]:
gpon-olt(config)#**show idprom interface xgpon** <*S/P*> [<vendor|manufacture>]
< x | y | ... > *1:
gpon-olt(config)#**clear syslog** <[level]
[debug|info|notice|warning|major|critical|alert|emerg]>

CONTENTS

1. Access OLT

You can access OLT by CLI (Command Line Interface) via console cable or telnet. This chapter introduces how to access OLT CLI via console cable.

1. Connect PC serial port or USB-to-Serial port to OLT console port by console cable.
2. Run secureCRT or other simulation tools such as Putty in the PC, and set parameters as follows.
   - Baudrate: 115200
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Follow control: none



COM port properties

After truned on the power, there is boot information printing. After startup, press enter and input username and password to login.

Notice: *The default account is admin/Xpon@Olt9417#. For example,*

Login: **admin**
Password: **Xpon@Olt9417#**
gpon-olt> **enable**
Password: **Xpon@Olt9417**
gpon-olt#

Input commands to configure or check device's status. Input "?" any time you need help.

This document will introduce each command begin at next chapter.

2. Command Line Interface

2.1 Abstract

The OLT provides command line interface for configuration and management. The following is its specialties.

- Configure from console port.
- Input "?" any time you need help.
- Provide network test command, such as ping, for diagnosing connection.
- Provide FTP service for uploading and downloading files.
- Provide Doskey analogous function, you can execute a history command.
- Support ambiguous keywords searching, you just need to input unconflict keywords and press "tab" or "?".

2.2 CLI Configuration Mode

GPON OLT provides three configuration modes.

- Privileged mode
- Global configuration mode
- Interface configuration mode

The following table shows specialties, commands to enter and prompts.

CLI mode	Specialty	Prompt	Command to enter	Command to exit
Privileged mode	Show configurations and execute system commands	gpon-olt#	/	**exit**
Global configuration mode	Configure system parameters	gpon-olt (config)#	**configure terminal**	**exit**
Interface configuration mode	Configure interface parameters	gpon-olt (config-if)#	**interface** *interface_type slot/port*	**exit**

2.3 CLI Characteristic

2.3.1 Online Help

The OLT CLI provides the following online help:

- Completely help
- Partly help

You can get some help information of CLI with the help above.

(1) Input "?" to get all commands and illustrations at any configuration mode.

gpon-olt (config)#

access-list	Add an access list entry.
alarm	Specify alarm.
banner	Set banner string
channel-group	Etherchannel/port bundling configuration.
clean	Specify clean operation.
clear	Specific save syslog to flash.
copy	Copy configuration
debug	System debugging functions.
enable	Modify enable password parameters
enable-password	Set your enable password.
end	Exit current mode and down to previous mode
erase	Erase info from flash.
event	Specify event.
exec	exec system cmd
exit	Exit current mode and down to previous mode
fan	Specify olt fan management.
gateway	system manage gateway.
help	Description of the interactive help system
hostname	Set system's network name
igmp	Global IP configuration subcommands
interface	Select an interface to configure.
ip	IP information
ipmc	Global IP configuration subcommands
isolate	the isolate configuration information.Set switchport characteristics.
l3	set ecmp dip reg
line	Configure a terminal line
list	Print command list
log	Logging control
login-password	Reset your login password.
mac	Configure the MAC address table.
mc	pim add ipmc group
monitor	Configure SPAN monitoring.
no	Negate a command or set its default.
password	Assign the terminal connection password
pim	pim add ipmc group
ping	ping command
profile	Select profile to configure.
queue-scheduler	Configure egress queueing policy.

```
  quit                Exit current mode and down to previous mode
  reboot              Reboot the switch.
  save                Specific save syslog to flash.
  service             Set up miscellaneous service
  set                 Specify set command.
  show                Show information
  snmp-server         Snmp server config
  spanning-tree       Config STPD information.
  storm-control       Specify the storm control.
  switch              switch to shell
  syslog              Specific system log save level,which syslog level not less
than level will save to flash.
  tftp                Specify tftp download.
  time                Specify system time configuration.
  upgrade             Specify upgrade system.
  upload              Upload file for software or user config.
  user                Manage System's users.
  vlan                Vlan commands.
  write               Write running configuration to memory, network, or
terminal
```

(2) Input "?" behind a command, it will display all key words and illustrations when this site should be a key word.

```
gpon-olt (config)# interface
  aux                 aux interface.
  gpon                Specify gpon interface
  gigabitethernet     GigabitEthernet IEEE 802.3z.
  vlan                Config vlan information.
  range               interface range command.
  loopback            config loopback information.
```

(3) Input "?" behind a command, it will display description of parameters when this site should be a parameter.

```
gpon-olt (config)# access-list
  <0-999>             IP standard access list.
  <1000-1999>         IP extended access list.
  <2000-2999>         L2 packet header access list.
  <3000-3999>         User define field access list.
  <4000-4999>         Vlan translation access list.
  <5000-5999>         Port business access list.
  ipv6                IPv6 access list.
```

(4) Input a character string end with "?", it will display all key words that begin with this character string.

```
gpon-olt (config)# e
  enable              Modify enable password parameters
```

```
enable-password      Set your enable password.
end                  End current mode and change to enable mode.
erase                Erase info from flash.
event                Specify event
exec                 Exec system cmd
exit                 Exit current mode and down to previous mode
```

(5) Input a command and a character string end with "?", it will display all key words begin with this character sring.

```
gpon-olt (config)# show ver
   version    show version command.
```

(6) Input a character string end with "Tab", it will display completely key words that begin with this character string when it is unique.

2.3.2 Display Characteristic

The OLT CLI provides the following display characteristic. There is a pause when the information displays a whole screen at a time. Users have two ways to choose.

Operation	function
Input <Ctrl+C>	Stop displaying and executing.
Input any key	Continue displaying next screen

2.3.3 History Commands

CLI provides Doskey analogous function. It can save history commands that executed before. Users can use direction key to invoke history command. The device can save at most ten commands.

Operation	Action	Result
Display history commands	**history**	Display all history commands.
Visit previous command	Up direction key "↑" or <Ctrl+P>	Display previous command if there is early history command.
Visit next command	Down direction key "↓" or <Ctrl+N>	Display next command if there is later history command.

2.3.4 Error Messages

Every command will be executed if it passes syntax check. Otherwise it will come out error message. The following table shows some frequent errors.

Error messages	Reasons
Unknown command	No this command

	No this key word
	Parameter type error
	Parameter out of range
Command incomplete	Command is not complete
Too many parameters	Too many parameters
Ambiguous command	Command is ambiguous

2.3.5 Edit Characteristic

CLI provides basic edit function. Every command supports maximum 256 characters. The following table shows how to edit.

Operation	Function
Generally input	Insert character at cursor position and move cursor to right if edit buffer has enough space.
Backspace key	Delete the character in front of cursor.
Left direction key ← or <Ctrl+B>	Cursor moves one character position towards the left.
Right direction key → or <Ctrl+F>	Cursor moves one character position towards the right.
Up direction key↑or <Ctrl+P> Down direction key↓or <Ctrl+N>	Display history command.
Tab key	Input incomplete key words end with Tab key, CLI will provide partly help. If it is unique, the key word which matches what you input will be used and display in another row. If it should be parameter, or the key word is mismatched or matched but not unique, CLI will use what you input and display in another row.

3. OLT Management Configuration

3.1 Configure Outband Management

Port AUX is outband management port. So its IP is outband management IP.

3.1.1 Enter AUX Port Configuration Mode

Start from privileged configuration mode, enter interface configuration mode as the

following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface aux**	Enter AUX interface.

3.1.2 Outband Management IP address

Start from privileged configuration mode, configure outband management IP address and mask as the following table shows.

	Command	Function
Step 1	**config terminal**	Enter global configuration mode.
Step 2	**interface aux**	Enter AUX interface.
Step 3a	**ip address <***A.B.C.D/M* | *A.B.C.D A.B.C.D***>**	Configure IP address and mask of AUX port.
Step 3b	**no aux ip address**	Reset outband management IP to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show aux ip address**	Show outband management IP.
Step 6	**write**	Save configurations.

3.1.3 Outband Management IPv6 Address

Start from privileged configuration mode, configure outband management IPv6 address and mask as the following table shows.

	Command	Function
Step 1	**config terminal**	Enter gobal configuration mode.
Step 2	**interface aux**	Enter AUX port configuration mode.
Step 3a	**ipv6 address** *X:X::X:X /M*	Configure IPv6 address and prefix length of AUX port.
Step 3b	**no aux ipv6 address**	Delete IPv6 address of AUX port.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show aux ipv6 address**	Display AUX port cofniguraiton.

Step 6	**write**	Save configuration.

3.1.4 Show AUX Port Information

Start from privileged configuration mode, show AUX port information as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show interface aux**	Show AUX port information.

3.2 Configure Inband Management

This device provides inband management which can be managed from uplink port. Start from privileged configuration mode, configure inband management IP address and mask as the following table shows.

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan_id*	Create VLAN.
Step 3	**exit**	Exit to global configuration mode.
Step 4	**interface vlan** *vlan_id*	Enter VLAN interface configuration mode. *vlan_id* range is 1－4094.
Step 5a	**ip address** <*A.B.C.D/M* | *A.B.C.D A.B.C.D*>	Configure IP address and mask.
Step 5b	**no ip address** <*A.B.C.D/M* | *A.B.C.D A.B.C.D*>	Delete IP address and mask.
Step 6	**exit**	Exit to global configuration mode.
Step 7	**show interface vlan** *vlan_id*	Show VLAN information.
Step 8	**write**	Save configurations.

3.3 Configure Manangement Gateway

3.3.1 Configure the Management IPv4 Gateway

When OLT management IP and management server are not in the same network

segment, it needs to configure a gateway.
Start from privileged configuration mode, configure management gateway as the following table shows.

	Command	Function
Step 1	**config terminal**	Enter global configuration mode.
Step 2	**ip route** <*A.B.C.D/M* | *A.B.C.D A.B.C.D*>	Configure management gateway.
Step 3	**no ip route** <*A.B.C.D/M* | *A.B.C.D A.B.C.D*>	Delete management gateway.
Step 4	**show ip route**	Show management gateway configuration.
Step 5	**write**	Save configurations.

3.3.2 Configure the Management IPv6 Gateway

When the OLT management IP and management servers are not in the same network segment, the gateway needs to be configured.
Start from the privileged configuration mode, press the configuration management gateway shown in the table.

	Command	Function
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**interface aux**	Enter the aux interface
Step 3	**ipv6 gateway** *X:X::X:X*	Configure the ipv 6 management gateway
Step 4	**no ipv6 gateway**	Delete the ipv 6 management gateway
Step 5	**show ipv6 gateway**	Displays the ipv 6 management gateway configuration
Step 6	**write**	Save configuration

3.4 Configure DNS

3.4.1 Configure the IPv4 DNS

You can configure two ipv4 DNS servers

	Command	Function
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**ip dns** *A.B.C.D* [*A.B.C.D*]	configure DNS
Step 3	**show ip dns**	Displays the DNS configuration
Step 4	**write**	Save configuration

3.4.2 Configure the IPv6 DNS

You can configure two ipv6 DNS servers

	Command	Function
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**Ipv6 dns** *X:X::X:X* [*X:X::X:X*]	Configure the IPv6 DNS
Step 2a	**no ipv6 dns**	Delete ipv6 dns
Step 3	**show ipv6 dns**	Displays the IPv6 DNS configuration
Step 4	**write**	Save configuration

4. Port Configuration

4.1 Port Configuration

4.1.1 Enter Port Configuration Mode

Start from privileged configuration mode, input the following commands to enter port configuration mode.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.

4.1.2 Enable /Disable Port

You can use these commands to enable or disable port. The ports are enabled by default. If you want a port not to transfer data, you can shutdown it.
Start from privileged configuration mode, enable or disable ports as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**no shutdown**	Enable port
Step 3b	**shutdown**	Disable port.
Step 4	**exit**	Exit to gloable configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.3 Configure Port Description

This command is used to configure port description. There is no description by default.
Start from privileged configuration mode, configure port description as the following

table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**description** *string*	Configure port description.
Step 3b	**no description**	Delete description.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.4 Configure Port Duplex Mode

Duplex includes full duplex and half duplex. When it works at full duplex, port can transmit and receive data at the same time; when it works at half duplex, port can only transmit or receive data at the same time. The duplex is auto by default.
Start from privileged configuration mode, configure port duplex mode as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**duplex** < auto | full | half >	Configure port duplex mode.
Step 3b	**no duplex**	Reset duplex mode to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step6	**write**	Save configurations.

4.1.5 Configure Port Speed

When port speed mode is auto, the actual speed of port is determined by the automated negotiation result with opposite port. The speed is auto by default.
Start from privileged configuration mode, configure port speed as the following table

shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**speed** < 10 | 100 | 1000 | 10000 | auto >	Configure port speed.
Step 3b	**no speed**	Reset port speed to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.6 Configure Port Rate Limitation

Start from privileged configuration mode, configure port rate limitation as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**line-rate** <ingress | egress> **kbps** *value*	Configure port rate limitation. Enter limit value,step is 64 kbps,maximum 100000 for fe,1000000 for ge,10000000 for xe, 100000000 for ce.it should be integral multiple of 64kbps.
Step 3b	**no line-rate** <ingress | egress>	Delete port rate limitation configurations.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step6	**write**	Save configurations.

4.1.7 Configure Port VLAN Mode

Each port has three VLAN mode, access, trunk and hybrid.
Access mode is usually used for port that connects with PC or other terminals, only one VLAN can be set up. Trunk mode is usually used for port that connects with switch; one or more VLAN can be set up. Hybrid mode can be used for port that connects with PC or switch. Default VLAN mode is hybrid.
Start from privileged configuration mode, configure port VLAN mode as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**switchport mode** < access | trunk | hybrid>	Configure port VLAN mode.
Step 3b	**no switchport mode**	Reset VLAN mode to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

Notice:
All VLAN configurations will lose when you change port VLAN mode.

4.1.8 Configure Hybrid Port VLAN

Hybrid port can belong to several VLAN. It can be used to connect with switch or router, and also terminal host.
Start from privileged configuration mode, configure hybrid port VLAN as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**switchport hybrid vlan** *vlan_id* <tagged | untagged>	Add specific VLAN to hybrid port.
Step 3b	**no switchport hybrid vlan** *vlan_id*	Remove VLAN from port.

Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

Notice:
You must configure PVID for the port that if it is configured untagged mode. PVID is the same as VLAN ID. Please refer to 3.1.10.

4.1.9 Configure Trunk Port VLAN

Trunk mode port can belong to several VLAN. It is usually used to connect with switches routers.
Start from privileged configuration mode, configure trunk port VLAN as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration
Step 2	**interface** *interface_type slot/port*	Enter interface configuration
Step 3a	**switchport trunk vlan** *vlan_id*	Add specific VLAN to trunk port. VLAN mode is tagged.
Step 3b	**no switchport trunk vlan** *vlan_id*	Remove VLAN from port.
Step 5	**exit**	Exit to global configuration mode.
Step 6	**show interface** *interface_type slot/port*	Show interface configurations.
Step 7	**write**	Save configurations.

Notice:
If PVID of trunk mode port is the same as VLAN ID, the VLAN will add to the port as untagged mode.

4.1.10 Configure Port PVID

Only under hybrid mode and trunk mode can set up PVID.
Start from privileged configuration mode. Configure port PVID as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration.

Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**switchport** <hybrid|trunk> **pvid vlan** *vlan_id*	Configure hybrid mode or trunk mode port PVID.
Step 3b	**no switchport** <hybrid|trunk>**pvid**	Reset hybrid or trunk port PVID to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.11 VLAN Configure Access Port VLAN

Only one untagged mode VLAN can be set to access port. Port's PVID is the same as VLAN ID.
Start from privileged configuration mode, configure access port VLAN as the thable shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**switchport access vlan** *vlan_id*	Configure access port VLAN.
Step 3b	**no switchport access vlan**	Reset access port VLAN to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.12 Configure Port Flow Control

Start from privileged configuration mode, configure port flow control as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.

Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**flowcontrol on**	Enable flow control function.
Step 3b	**no flowcontrol**	Disable flow control function.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.13 Configure Port Broadcast Suppression

Start from privileged configuration mode, configure port broadcast suppression as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**storm-control broadcast fps** *value*	Configure broadcast suppression. Value range: 64-1000000, it should be integral multiple of 64kbps.
Step 3b	**no storm-control broadcast**	Remove broadcast suppression.
Step 4	**exit**	Exit global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.14 Configure Port Multicast Suppression

Start from privileged configuration mode, configure port multicast suppression as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration

		mode.
Step 3a	**storm-control multicast fps** *value*	Configure multicast suppression. Value range: 64-1000000, it should be integral multiple of 64kbps.
Step 3b	**no storm-control multicast**	Remove multicast suppression.
Step 4	**exit**	Exit global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.15 Configure Port Unknown Unicast Suppression

Start from privileged configuration mode, configure port unknown unicast suppression as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**storm-control unknow fps** *value*	Configure unknown unicast suppression. Value range: 64-1000000, it should be integral multiple of 64kbps.
Step 3b	**no storm-control unknow**	Remove unknown unicast suppression.
Step 4	**exit**	Exit global configuration mode.
Step 5	**show interface** *interface_type slot/port*	Show interface configurations.
Step 6	**write**	Save configurations.

4.1.16 Configure Port Isolation

With this function, customers can add ports to a same isolation group so that these ports can be isolated among L2 and L3 steams. This will improve security of network and provide flexible networking scheme.

Start from privileged configuration mode, configure port isolation as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**switchport isolate**	Add port to isolation group.
Step 3b	**no switchport isolate**	Remove port from isolation group.
Step 4	**exit**	Exit to global configuration mode.
Step 5a	**show interface** *interface_type slot/port*	Show interface configurations.
Step 5b	**show isolate** <gigabitEthernet | gpon>	Show isolation group.
Step 6	**write**	Save configurations.

4.1.17 Configure Port Loopback

Start from privileged configuration mode, configure port loopback as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**loopback-detect enable**	Enable port loopback detection.
Step 2b	**loopback-detect disable**	Disable port loopback detection.
Step 3	**show loopback detect**	Show port loopback detection status.
Step 4	**exit**	Exit to global configuration mode.

4.1.18 Configure Port Jumboframe

Start from privileged configuration mode, configure jumboframe that the port can pass as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**jumboframe enable**	Enable jumboframe transmission. By default, switch chipset supports transmitting maximum 1536 bytes frame; PON chipset supports transmitting maximum 2047 bytes frame.
Step 3b	**no jumboframe**	Disable jumboframe transmission.
Step 4	**exit**	Exit to global configuration mode.

4.1.19 Show Port Statistics

Start from privileged configuration mode, show port statistics as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3	**show statistics**	Show port statistics.
Step 4	**exit**	Exit to global configuration mode.

4.1.20 Clean Port Statistics

Start from privileged configuration mode, clean port statistics as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.

Step 2	**show statistics**	Show port statistics.
Step 3	**clean statistics**	Clean port statistics.

4.1.21 Show Interface Configurations

Operation	Command
Show interface configurations.	**show interface** *interface_type slot/port*

In the system, interface gigabitethernet 0/1~0/x stands for uplink port 1~x. Interface gpon0/1~0/x stands for GPON port 1~x,interface xgpon0/1~0/x stands for XGPON port 1~x.
For example, display configurations of uplink port 1.

```
gpon(config)# show interface gigabitEthernet 0/1
   Interface gigabitEthernet 0/1 is up
      Description: no set
      The Maximum Transmit Unit is (MTU) 1536 bytes
      Inter Packet Gap 64 ns
      Full-duplex, 1000Mb/s, media type is 1000BASE-SX
      Input flow-control is off, Output flow-control is off
      Forward Error Correction : Disable
      Pre-Emphasis pre 0, main 100, post 0, post2 0, post3 0
      DFE       : Disable
      LP DFE : Disable
      BR DFE : Disable
      RX_PEAK_FILTER    : 10
      RX_LOW_FREQ_PEAK_FILTER : 0
      RX_VGA : 32
      RX TAP1 0, TAP2 0, TAP3 0, TAP4 0, TAP5 0, TAP6 0
      Interface : lr
      Broadcast storm control           : 512 fps
      Multicast storm control           : disable
      Unknow unicast storm control : 512 fps
      Ingress line rate control        : no limit
      Egress line rate control          : no limit
      MAC Address state : enable, no limit
      PVID : 1
      Isolate member      : No
      Port link-type      : hybrid
      Tagged VLAN ID      : 1000    3000    999
      Untagged VLAN ID : 1
      QinQ :
```

VLAN Translate :
Ingress access-list :
Egress access-list :
Ingress access-list ipv6 :
Egress access-list ipv6 :
Last 300 seconds input: 0 packets 0 bytes
Last 300 seconds output: 61489146912362300 packets/sec 2675.00 MB/sec
Input(total): 0 packets, 0 bytes
0 broadcasts, 0 multicasts
Input(normal): 0 packets, 0 bytes
0 broadcasts, 0 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, 0 throttles, 0 CRC
0 overruns, 0 aborts, 0 ignored, 0 parity errors
Output(total): 777 packets, 77746 bytes
214 broadcasts, 563 multicasts, 0 pauses
Output(normal): 777 packets, 77746 bytes
214 broadcasts, 563 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, 0 buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lost carrier, 0 no carrier

4.1.22 Show Optical Module Parameters

Optical module parameters include transmit optical power, receive optical power, temperature, voltage, and bias current. These 5 parameters determine whether the optical module can work normally. Any of these exceptions can result in lost packets. Start from the privileged configuration mode, the port optical module parameters are displayed, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show transceiver**	Show the information of the optical uplink port.

4.1.23 Show Information of the Optical Module

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show idprom interface** <gpon	Show information about the

|gigabitEthernet> *slot/port* [vendor | manufacture]	optical module manufacturer

4.2 Example

Configure VLAN and broadcast suppression of trunk mode port.

1.Requirement

Uplink port 1 of OLT connects to switch, port mode is trunk. It can pass through VLAN 20 and VLAN 100, add VLAN tag 123 to untagged streams. Rate of broadcast streams is 64bps.

2.Framework

3.Steps

(1)Enter interface configuration mode.

gpon-olt (config)# interface gigabitethernet 0/1

gpon-olt (config-if-ge0/1) #

(2)Configure port mode and add VLAN

gpon-olt (config-if-ge0/1) # switchport mode trunk

gpon-olt (config-if-ge0/1) # switchport trunk vlan 20

gpon-olt (config-if-ge0/1) # switchport trunk vlan 100

PS. The VLAN must be added first. Please refer to 6.1.1.

(3)Configure port PVID

gpon-olt (config-if-ge0/1) # switchport trunk pvid vlan 123

(4)Configure port broadcast suppression

gpon-olt (config-if-ge0/1) # storm-control broadcast fps 64

5. Port Aggregation Configuration

5.1 Introduction

Port aggregation is that several ports constitute an aggregation group so that it can share responsibility for traffic load in each port. When one link is broken down, the traffic will switch to another automatically to ensure traffic is unblocked. It seems that the aggregation group is the same as a port.

In an aggregation group, member ports must have the same speed, the same duplex mode and the same basic configurations. Basic configurations contain:

(1) STP configurations such as STP status, link properties (e.g. p2p port), priority, cost, message format, loopdetect status, edge port or not.
(2) QoS configurations such as rate limiting, priority mark, 802.1p priority, congestion avoidance.
(3) VLAN configurations such as VLAN ID, PVID.
(4) Port link type such as trunk mode, hybrid mode and access mode.
(5) GVRP configurations such as switch status, registration type, timer value.

5.2 Port Aggregation Configuration

5.2.1 Configure Load Balancing Policy of Group

Configuring load balancing policy includes source MAC, destination MAC, both source and destination MAC, source IP, destination IP, both source and destination IP. Default load balancing policy is based on source MAC.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**channel-group** <(1-2) | all >**load-balance <**dip | dmac | sdip | sdmac | sip | smac>	Specify which link is used to transmit traffic in aggregation group.
Step 3	**show channel-group summary**	Show aggregation configurations.

5.2.2 Configure Member Port of Group

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gigabitEthernet** *slot/port*	Enter interface configuration mode.
Step 3a	**channel-group** (1-2)	Add current port to specific channel group.
Step 3b	**no channel-group** (1-2)	Delete current port from specific channel group.

5.3 Configure Dynamic Port Aggregation

For details about how to configure load balancing policies, refer to chapter 5.2.1.

5.3.1 Configure Member Port

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gigabitEthernet** *slot/port*	Enter interface configuration mode.
Step 3	**channel-group** (1-2)	Add current port in the specified working mode.
Step 4	**lacp timeout** <long|short>	Specified the LACP timeout period for a port. long:90s short:3s
Step 5	**lacp port-priority** (0-65535)	Configure the port priority. A smaller priority indicates a higher priority. The default value is 32768.

If the LACP working mode of member ports in a dynamic aggregation group is PASSIVE and the LACP working mode of the peer end is PASSIVE, both ends cannot send LACPDUs. If the LACP working mode of either end is ACTIVE, both ends can send LACPDUs.

5.3.2 Show Aggregation Group Information

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gigabitEthernet**	Enter interface configuration mode.

	slot/port	
Step 3	**show channel-group** (1-4)	Show group information.
Step 4	**show channel-group information**	Show the LACP statistics of all uplink port.
Step 5	**show channel-group interface all**	Show the LACP negotiation status of all uplink port.
Step 6	**show channel-group ports**	Show the information about the ports added to the aggregation group.

6. VLAN Configuration

6.1 VLAN Configuration

VLAN configuration mainly contains:

- Create/delete VLAN
- Configure/delete VLAN description
- Configure/delete IP address and mask of VLAN

6.1.1 Create/Delete VLAN

Start from privileged configuration mode, create or delete VLAN as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**vlan** *vlan_id*	Create VLAN or enter VLAN interface configuration mode. VLAN ID range is from 1 to 4094.
Step 2b	**no vlan** *vlan_id*	Delete specific VLAN.
Step 3	**exit**	Exit to global configuration mode.
Step 4	**show vlan** <*vlan_id* | all>	Show VLAN configurations. Choosing all means display all existed VLAN. And choosing *vlan_id* means display information of specific VLAN.
Step 5	**write**	Save configurations.

6.1.2 Configure/Delete VLAN Description

Start from privileged configuration mode, configure or delete VLAN description as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan_id*	Create VLAN or enter VLAN infterface configuration mode. VLAN ID range is from 1 to 4094.
Step 3a	**description** *string*	Configure VLAN description.
Step 3b	**no description**	Delete VLAN description.

Step 4	**exit**	Exit to bloble configuration mode.
Step 5	**show interface vlan** *vlan_id*	Show VLAN interface information.
Step 6	**write**	Save configurations.

Notice:
By default, VLAN description is VLAN ID, such as " vlan 1".

6.1.3 Configure/Delete IP Address and Mask of VLAN

Start from privileged configuration mode, configure or delete IP address and mask of VLAN as the following table shows.

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode.
Step 2	**interface vlan** *vlan_id*	Enter VLAN interface configuration mode. VLAN ID range is from 1 to 4094.
Step 3a	**ip address <***A.B.C.D A.B.C.D* | *A.B.C.D/M* >	Configure IP address and mask of VLAN.
Step 3b	**no ip address**	Delete IP address and mask of VLAN.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface vlan** *vlan_id*	Show VLAN information.
Step 6	**write**	Save configurations.

6.2 Show VLAN Information

Input the following commands to Show VLAN information and port members.

Operation	Command
Show VLAN information	**show interface vlan**
Show VLAN port members	**show interface vlan** *vlan-id*

Example:
Show VLAN 100 port members
gpon-olt(config)# show interface vlan 100
VLAN ID : 100
Name : vlan100
IP Address :
IPv6 Address :
Tagged Ports : GE 0/1 GE 0/2

Untagged Ports : GE 0/6 GE 0/7
MAC Address : 00:4F:5B:F4:18:D5
MAC Address Learn : enable
MAC VLAN :
Subnet VLAN :
IPv6 Subnet VLAN :

Notice:
By default, It have one vlan on system ,do not delete and edit.

VLAN ID : 1
Name : default
IP Address :
IPv6 Address :
Tagged Ports :
Untagged Ports : GE 0/1 GE 0/2 GE 0/3 GE 0/4 GE 0/5 GE 0/6 GE 0/7
MAC Address : 00:4F:5B:F4:18:D5
MAC Address Learn : enable
MAC VLAN :
Subnet VLAN :
IPv6 Subnet VLAN :

7. VLAN Translation/QinQ

7.1 Configure VLAN Translation/QinQ

Start from privileged configuration mode, configure VLAN translation/QinQ as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3a	**dot1q-tunnel vlan-mapping** (1-4094) < any | (0-7) | vport (0-15)> (1-4094) < any | (0-7) > < db-tagged | one-tagged >	Configure VLAN translation/QinQ. db-tag means QinQ. one-tag means translation.
Step 3b	**no dot1q-tunnel vlan-mapping** (1-4094) < (1-4094) | vport (0-15)>	Delete VLAN translation/QinQ.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show vlan dot1q-tunnel vlan-mapping**	Show VLAN translation/QinQ configurations.
Step 6	**write**	Save configurations.

7.2 Example

(1)VLAN Translation

Configure GE1 VLAN translation function, CVLAN is 100, priority is 1, and translated VLAN is 200, priority is 2.

```
gpon-olt (config)# interface gigabitethernet 0/1
gpon-olt (config-if)#switchport hybrid vlan 100 tagged
gpon-olt (config-if)#switchport hybrid vlan 200 tagged
gpon-olt(config-if)#dot1q-tunnel vlan-mapping 100 1 200 2 one-tagged
gpon-olt (config)#show vlan dot1q-tunnel vlan-mapping
```

(2)QinQ function

Configure GE2 QinQ function, CVLAN is 300, priority is 3, and SVLAN is 400, priority is 4.

```
gpon-olt (config)# interface gigabitethernet 0/2
gpon-olt (config-if)#switchport hybrid vlan 300 tagged
gpon-olt (config-if)#switchport hybrid vlan 400 tagged
```

gpon-olt (config-if)#dot1q-tunnel vlan-mapping 300 3 400 4 db-tagged
gpon-olt (config)#show vlan dot1q-tunnel vlan-mapping

8. MAC Address Configuration

8.1 Overview

In order to forward messages rapidly, a device need to maintain its MAC address table. MAC address table contains MAC addresses that connect with the device, ports, VLAN, type and aging status. Dynamic MAC addresses in the table are learnt by device. The proccess of learning is that: if port A receives a message, device will analyze the source MAC address (SrcMAC), and think of messages whose destination MAC address is SrcMAC can be forwarded to port A. If SrcMAC has been in the table, device will update it; if not, device will add this new address to the table.
For the messages whose destination MAC address can be found in MAC address table, they are forwarded by hardware. Otherwise, they flood to all ports. When flooded messages arrive to its destination, the destination device will respond. The device will add new MAC to the table. Then, messages with this destination MAC will be forwarded via the new table. However, when messages still can't find its destination by flood, device will discard them and tell sender destination is unreachable.

8.2 Configure MAC Address

MAC address management includes:
- Configure MAC address table
- Configure MAC address aging time

8.2.1 Configure MAC Address Table

You can add static MAC address entries, delete MAC address entries or clean MAC address table.
Start from privileged configuration mode, configure MAC address table as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**mac address-table static vlan** *vlan_id xxxx:xxxx:xxxx* **interface gigabitethernet** *slot/port*	Add static MAC address entry.
Step 2b	**no mac address-table vlan** *vlan_id xxxx:xxxx:xxxx*	Delete MAC address entry.

Step 3	**show mac address-table**	Show MAC address table.
Step 4	**write**	Save configurations.

8.2.2 Configure MAC Address Aging Time

There is aging time in device. If device doesn't receive any message from other devices in aging time, it will delete the MAC address from MAC table. But for static MAC in the table, aging time is not effective.
Start from privileged configuration mode, configure MAC address aging time as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac address-table aging-time** <(10-1000000) | default>	Configure MAC address aging time, range is 10-1000000s. 0s means don't aging. Default is 300s.
Step 3	**show mac address-table aging-time**	Show aging time.
Step 4	**write**	Save configurations.

8.2.3 Configure Maximum Learnt MAC Enties of Port

Start from privileged configuration mode, configure maximum learnt MAC entries of port as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type slot/port*	Enter interface configuration mode.
Step 3	**mac-address mac-limit** (0-16384)	0 means no limitation.
Step 4	**exit**	Exit to global configuration mode.

8.3 Show MAC Address Table

8.3.1 Show MAC Address Table

Start from privileged configuration mode, show MAC address table as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**show mac address-table interface** *interface_type slot/port*	Show MAC address table based on Ethernet port.
Step 2b	**show mac address-table vlan** *vlan_id*	Show MAC address table based on VLAN ID.
Step 2c	**show mac address-table**	Show whole MAC address table.

8.3.2 Show MAC Address Aging Time

Start from privileged configuration mode, show MAC address aging time as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show mac address-table aging-time**	Show MAC address aging time.

9. Configure Port Mirroring

Port mirroring is to copy one or more ports' traffic to specific port. It is usually used for network traffic analysis and diagnosis.
The device supports 4 mirroring sessions.

9.1 Configure Mirroring Destination Port

Start from privileged configuration mode, configure mirroring destination port as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**monitor session** *session_number* **destination interface gigabitethernet** *slot/port*	Confire mirroring destination port. Session number is 1~4.
Step 3	**show monitor session** <(1-4) | all>	Show mirroring configurations.
Step 4	**write**	Save configurations.

9.2 Configure Mirroring Source Port

Mirroring source port is the port we want to monitor. Data that pass through the port will be copied to mirroring destination port.
Start from privileged configuration mode, configure mirroring source port as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**monitor session** (1-4) **source interface** *interface_type slot/port* [**-** *port*] <rx | tx>	Configure mirroring source port. session_number is 1-4. **rx** means received data. **tx** means transmitted data.
Step 3	**show monitor session**	Show mirroring configurations.

Step 4	**write**	Save configurations

9.3 Delete Port Mirroring

Start from privileged configuration mode, delete port mirroring as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** (1-4) [destination | source]	Delete port mirroring. session_number is 1-4
Step 3	**show monitor session**	Show mirroring configurations.

Example:

Mirror data from gpon 0/1 to uplink port 1.

gpon-olt(config)# monitor session 1 destination interface gigabitethernet 0/1

gpon-olt (config)# monitor session 1 source interface gpon 0/1 both

10. IGMP Configuration

10.1 IGMP Snooping

10.1.1 Enable/Disable IGMP Snooping

IGMP snooping is disabled by default. You should enable by the following command. Start from privileged configuration mode, enable/disable IGMP snooping as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ip igmp snooping enable**	Enable IGMP Snooping.
Step 2b	**no ip igmp snooping**	Disable IGMP snooping.
Step 3	**show ip igmp snooping configuration**	Show IGMP snooping configurations.
Step 4	**write**	Save configurations.

10.1.2 Configure Multicast Data Forwarding Mode

Start from privileged configuration mode, configure multicast data forwarding mode as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp snooping forward vlan** (1-4094) **mode** [flood | forward | strict-forward]	Configure multicast data forwarding mode.
Step 3	**write**	Save configurations.

10.1.3 Configure Port Multicast VLAN

After add VLAN to the port, you should also configure multicast VLAN for multicast service. Start from privileged configuration mode, configure port multicast VLAN as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet |gpon] *slot/port*	Enter interface configuration mode;slot:<0>,port:<1-x>
Step 3a	**ip igmp snooping user-vlan** (1-4094) **group-vlan** (1-4094) [tagged | untagged]	Configure port multicast VLAN. VLAN range is 1-4094.。
Step 3b	**no ip igmp snooping group-vlan** (1-4094)	Delete port multicast VLAN.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show ip igmp snooping user-vlan**	Show multicast VLAN.
Step 6	**write**	Save configurations.

10.1.4 Configure Multicast Router Port

Multicast router port is used to forward IGMP messages. Usually, uplink port is configured as multicast router port.

Start from privileged configuration mode, configure multicast router port as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ip igmp snooping mrouter vlan** (1-4094) **interface gigabitEthernet** *slot/port*	Configure multicast router .port.slot:<0>/port:<1-x>
Step 2b	**no ip igmp snooping mrouter vlan** (1-4094) **interface gigabitEthernet** *slot/port*	Delete multicast router port.port.slot:<0>/port:<1-x>
Step 3	**show ip igmp snooping mrouter vlan** <(1-4094) | all>	Show multicast router mode configuration.
Step 4	**write**	Save configurations.

10.1.5 Configure Static Multicast

Start from privileged configuration mode, configure static multicast as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.

Step 2a	**ip igmp snooping static vlan** (1-4094) *A.B.C.D* **interface gpon** *slot/port*	Configure static multicast.
Step 2b	**no ip igmp snooping static vlan** (1-4094) *A.B.C.D* **interface gpon** *slot/port*	Delete static multicast.
Step 3	**show ip igmp snooping configuration**	Show IGMP configurations.
Step 4	**write**	Save configurations.

10.1.6 Configure Fast Leave

Start from privileged configuration mode, configure fast leave as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet | gpon] *slot/port*	Enter interface configuration mode.
Step 3a	**ip igmp snooping immediate-leave**	Enable fast leave.
Step 3b	**no ip igmp snooping immediate-leave**	Disable fast leave.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show ip igmp snooping port information**	Show port IGMP information.
Step 6	**write**	Save configurations.

10.1.7 Configure Multicast Group Limit

Start from privileged configuration mode, configure multicast group limitation as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet | gpon] *slot/port*	Enter interface configuration mode.
Step 3a	**ip igmp snooping limit** (0-1024)	Configure port multicast group limitation.
Step 3b	**no ip igmp snooping limit**	Reset multicast group limitation to default.
Step 4	**exit**	Exit to global configuration mode.

Step 5	**show ip igmp snooping port information**	Show port multicast information.
Step 6	**write**	Save configurations.

10.1.8 Configure Parameters of Special Query

Start from privileged configuration mode, configure parameters of specific query as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ip igmp snooping lastmember-querycount** (1-255)	Configure specific query count. Default is 2.
Step 2b	**ip igmp snooping lastmember-queryinterval** (1-255)	Configure specific query interval. Default is 1s.
Step 2c	**ip igmp snooping lastmember-queryresponse** (1-25)	Configure specific query response time. Default is 1s.
Step 3	**show ip igmp snooping configuration**	Show IGMP configurations.
Step 4	**write**	Save configurations.

10.1.9 Configure Parameters of General Query

Start from privileged configuration mode, configure parameters of general query as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ip igmp snooping general-query-packet** [enable|disable]	Enable or disable general query function. Default is disable.
Step 2b	**ip igmp snooping general-query-time** (10-255)	Configure general query interval. Default is 126s.
Step 3	**show ip igmp snooping configuration**	Show IGMP configurations.
Step 4	**write**	Save configurations.

10.1.10 Configure Source IP of Query

Start from privileged configuration mode, configure source IP of query message as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp snooping member-query source-ip** *A.B.C.D*	Configure source IP of query message. Default is 1.1.1.1.
Step 3	**show ip igmp snooping configuration**	Show IGMP configurations.
Step 4	**write**	Save configurations.

10.1.11 Configure Multicast Member Aging Time

If the port doesn't receive any report message from member in aging time, device will delete this port from group members.
Start from privileged configuration mode, configure muticast member aging time as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp snooping routeer-aging-time** (10-3600)	Configure multicast port member aging time. Value range is 10-3600s, defaultis260s.
Step 3	**show ip igmp snooping configuration**	Show IGMP configurations.
Step 4	**write**	Save configurations.

10.1.12 Show Multicast Gourp Information

If there is member join a group, you can use the following commands to show multicast group information.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**show ip igmp snooping vlan** [(1-4094) | all]	Show multicast group information.
Step 2b	**show ip igmp snooping statistic**	Show multicast statistic.

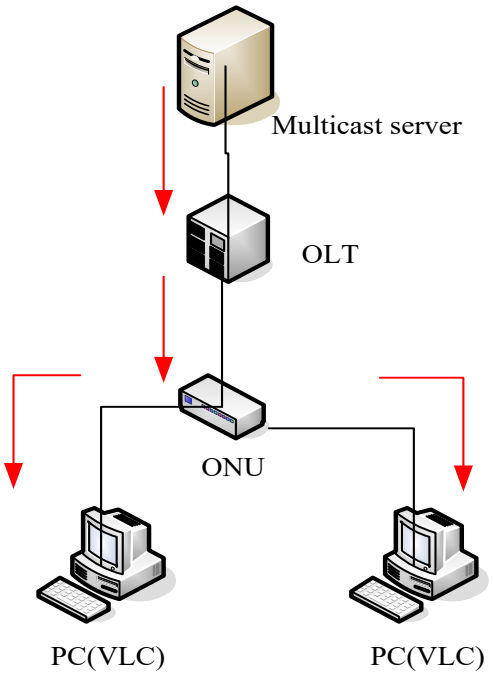
10.2 Example

This example introduces how to configure IGMP snooping function, including multicast VLAN, multicast router port and ONU LAN port, etc.

1. Requirement

In order to achieve multicast function, you should enable IGMP Snooping, configure multicast VLAN, multicast router port, and so on. The requirement contains:
multicast is VLAN 100.
Multicast server connects to uplink port 1.
ONU connects to PON 1.
Client, such as a PC, connects to ONU LAN 1.

2. Framework



3. Steps

(1)Create VLAN

```
gpon-olt (config)# vlan 100
gpon-olt (config-vlan-100)# exit
```

(2)Configure multcast VLAN100

```
gpon-olt (config)# interface gigabitethernet 0/1
gpon-olt (config-if-ge0/1)# switchport hybrid vlan 100 tagged
gpon-olt (config-if-ge0/1)# exit
gpon-olt (config)# interface gpon 0/1
gpon-olt(config-pon-0/1)# ip igmp snooping user-vlan 100 group-vlan 100 tagged
gpon-olt(config-pon-0/1)# exit
```

(3)Enable IGMP Snooping

```
gpon-olt(config)# ip igmp snooping enable
```

(4)Configure the G0/1 to multcast router port

gpon-olt(config)# ip igmp snooping mrouter vlan 100 interface gigabitethernet 0/1

(5)Configure the onu

gpon-olt(config)# interface gpon 0/1

gpon-olt(config-pon-0/1)#onu add 1 profile default sn MONU002b5791 us-rate 1g

gpon-olt(config-pon-0/1)# onu 1 tcont 1 dba default1

gpon-olt(config-pon-0/1)# onu 1 gemport 1 tcont 1 gemport_name gem_1

gpon-olt(config-pon-0/1)#onu 1 service ser_1 gemport 1 vlan 100

gpon-olt(config-pon-0/1)# onu 1 service-port 1 gemport 1 uservlan 100 vlan 100

gpon-olt(config-pon-0/1)#onu 1 portvlan eth 1 mode tag vlan 100

gpon-olt(config-pon-0/1)# onu 1 mvlan 100

11. IPv6 MLD Configuration

11.1 MLD Snooping

11.1.1 Enable/Disable MLD Snooping

MLD Snooping is disabled by default. You should enable by the following command. Start from privileged configuration mode, enable/disable mld snooping as the following table shows.

。

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ipv6 mld snooping**	Enable MLD Snooping.
Step 2b	**no ipv6 mld snooping**	Disable MLD snooping.
Step 3	**show ipv6 mld snooping running-config**	Show MLD snooping configurations.
Step 4	**write**	Save configurations.

11.1.2 Configure Port Multicast VLAN

After add VLAN to the port, you should also configure multicast VLAN for multicast service. Start from privileged configuration mode, configure port multicast VLAN as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet |gpon] *slot/port*	Enter interface configuration mode.
Step 3a	**ipv6 mld snooping user-vlan** (1-4094) **group-vlan** (1-4094)	Configure port multicast VLAN. VLAN range is 1-4094.
Step 3b	**no ipv6 mld snooping user-vlan** (1-4094)	Delete port multicast VLAN.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show ipv6 mld snooping user-vlan**	Show multicast VLAN.
Step 6	**write**	Save configurations.

11.1.3 Configure Multicast Router Port

Multicast router port is used to forward MLD messages. Usually, uplink port is configured as multicast router port.
Start from privileged configuration mode, configure multicast router port as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet |gpon] *slot/port*	Enter interface configuration mode.
Step 2a	**ipv6 mld snooping mrouter vlan** (1-4094)	Configure multicast router port.
Step 2b	**no ipv6 mld snooping mrouter vlan** (1-4094)	Delete multicast router port.
Step 3	**exit**	Exit to global configuration mode.
Step 4	**show ipv6 mld snooping mrouter**	Show multicast router mode configuration.
Step 5	**write**	Save configurations.

11.1.4 Configure Static Multicast

Start from privileged configuration mode, configure static multicast as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet |gpon] *slot/port*	Enter interface configuration mode.
Step 2a	**ipv6 mld snooping static vlan** (1-4094) *X:X::X:X*	Configure static multicast.
Step 2b	**no Ipv6 mld snooping static vlan** (1-4094) *X:X::X:X*	Delete static multicast.
Step 3	**show ipv6 mld snooping static-group**	Show MLD configurations.
Step 4	**write**	Save configurations.

11.1.5 Configure Fast Leave

Start from privileged configuration mode, configure fast leave as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet |gpon] *slot:<0>/port:<1-x>*	Enter interface configuration mode.
Step 3a	**ipv6 mld snooping fast-leave**	Enable fast leave.
Step 3b	**no ipv6 mld snooping fast-leave**	Disable fast leave.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show ipv6 mld snooping interface**	Show port MLD information.
Step 6	**write**	Save configurations.

11.1.6 Configure Multicast Group Limit

Start from privileged configuration mode, configure multicast group limitation as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** [gigabitEthernet |gpon] *slot/port*	Enter interface configuration mode.
Step 3a	**ipv6 mld snooping group-limit** (0-256)	Configure port multicast group limitation.
Step 3b	**no ipv6 mld snooping group-limit**	Reset multicast group limitation to default.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show ipv6 mld snooping interface**	Show port multicast information.
Step 6	**write**	Save configurations.

11.1.7 Configure Parameters of Special Query

Start from privileged configuration mode, configure parameters of specific query as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ipv6 mld snooping last-listener-query-count** (1-7)	Configure specific query count. Default is 2.
Step 2b	**ipv6 mld snooping last-listener-query-interval** (1-255)	Configure specific query interval. Default is 1s.
Step 2c	**ipv6 mld snooping last-listener-query-response** (1-255)	Configure specific query response time. Default is 1s.
Step 3	**show ipv6 mld snooping**	Show MLD configurations.
Step 4	**write**	Save configurations.

11.1.8 Configure Parameters of General Query

Start from privileged configuration mode, configure parameters of general query as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ipv6 mld snooping general-query-packet**	Enable general query function. Default is disable.
Step 2b	**no Ipv6 mld snooping general-query-packet**	disable general query function. Default is disable.
Step 2b	**ipv6 mld snooping general-query-interval** (10-3600)	Configure general query interval. Default is 125s.
Step 3	**show ipv6 mld snooping**	Show MLD configurations.
Step 4	**write**	Save configurations.

11.1.9 Configure Source IP of Query

Start from privileged configuration mode, configure source IP of query message as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 mld snooping general-query-source-ip** *X:X::X:X*	Configure source IP of query message. Default is fe80::1.

Step 3	**show ipv6 mld snooping**	Show MLD configurations.
Step 4	**write**	Save configurations.

11.1.10 Configure Multicast Member Aging Time

If the port doesn't receive any report message from member in aging time, device will delete this port from group members.
Start from privileged configuration mode, configure muticast member aging time as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 mld snooping query-response-interval** (1-64)	Configure multicast port member aging time. Value range is 1-64s, defaultis10s.
Step 3	**show ipv6 mld snooping**	Show MLD configurations.
Step 4	**write**	Save configurations.

11.1.11 Show Multicast Gourp Information

If there is member join a group, you can use the following commands to show multicast group information.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show ipv6 mld snooping statistics**	Show multicast statistic.

11.2 Example

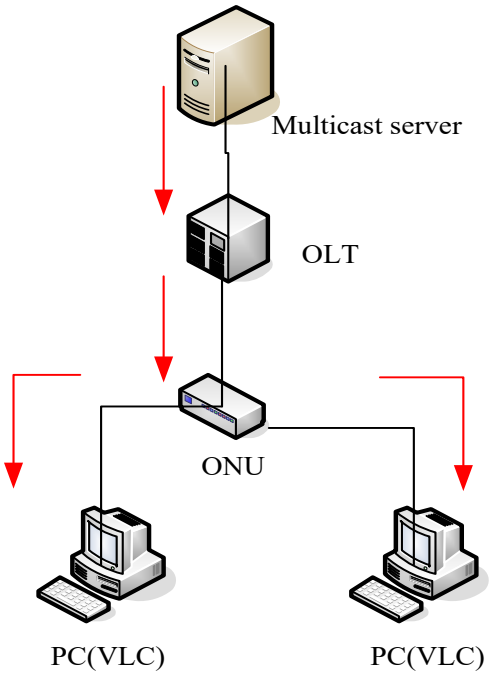
This example introduces how to configure MLD snooping function, including multicast VLAN, multicast router port and ONU LAN port, etc.

11.2.1 Requirement

In order to achieve multicast function, you should enable IGMP Snooping, configure multicast VLAN, multicast router port, and so on. The requirement contains:
multicast is VLAN 100.

Multicast server connects to uplink port 1.
ONU connects to PON 1.
Client, such as a PC, connects to ONU LAN 1.

11.2.2 Framework



11.2.3 Steps

(1)Create VLAN
gpon-olt (config)# vlan 100
gpon-olt (config-vlan-100)# exit
(2)Configure multcast VLAN100
gpon-olt (config)# interface gigabitethernet 0/1
gpon-olt (config-if-ge0/1)# switchport hybrid vlan 100 tagged
gpon-olt (config-if-ge0/1)# exit
gpon-olt (config)# interface gpon 0/1
gpon-olt(config-pon-0/1)# ipv6 mld snooping user-vlan 100 group-vlan 100 tagged
gpon-olt(config-pon-0/1)# exit
(3)Enable MLD Snooping
gpon-olt(config)# ipv6 mld snooping
Configure the G0/1 to multcast router portgpon-olt (config)# interface gigabitethernet 0/1
gpon-olt(config-if-ge0/1)# ipv6 mld snooping mrouter vlan 100
(5)Configure the onu

```
gpon-olt(config)# interface gpon 0/1
gpon-olt(config-pon-0/1)#onu add 1 profile default sn MONU002b5791 us-rate 1g
gpon-olt(config-pon-0/1)# onu 1 tcont 1 dba default1
gpon-olt(config-pon-0/1)# onu 1 gemport 1 tcont 1 gemport_name gem_1
gpon-olt(config-pon-0/1)#onu 1 service ser_1 gemport 1 vlan 100
gpon-olt(config-pon-0/1)# onu 1 service-port 1 gemport 1 uservlan 100 vlan 100
gpon-olt(config-pon-0/1)#onu 1 portvlan eth 1 mode tag vlan 100
gpon-olt(config-pon-0/1)# onu 1 mvlan 100
```

12. ACL Configuration

12.1 Overview

In order to filter data packages, network equipments need to setup a series of rules for identifying what need to be filtered. Only matched with the rules the data packages can be filtered. ACL can achieve this function. Matched conditions of ACL rules can be source address, destination address, Ethernet type, VLAN, protocol port, and so on. These ACL rules also can be used in other situations, such as classification of stream in QoS. An ACL rule may contain one or several sub-rules, which have different matched conditions.

This device supports the following types of ACL.

- IP Standard ACL.
- IP Extended ACL.
- ACL based on MAC address
- ACL based on port binding.
- ACL based on QoS.

Limitation of each ACL rule:

ACL type	ACL index	Maximum rules
IP Standard ACL	0-999	1000
IP Extended ACL	1000-1999	1000
ACL based on MAC address	2000-2999	1000
ACL based on port binding	5000-5999	1000

12.2 ACL Configuration

12.2.1 IP Standard ACL

Start from privileged configuration mode, configure IP standard ACL as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**access-list** *access-list-index*	Enter ACL configuration mode. *access-list-number* is ACL index. range:0-999.
Step 3a	**subset ip** [permit|deny] <*A.B.C.D A.B.C.D* | host *A.B.C.D* |any>	Configure ACL rule. A.B.C.D: define based on source IP address and mask ACL rule. **Host**: define based on single IP

		address ACL rule. **Any**: define based on any source IP address ACL rule.
Step 3b	**No access-list** *access-list-index*	Delete the ACL
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show access-list** [index *access-list-index*| all]	Show ACL configurations.
Step 6	**write**	Save configurations.

12.2.2 IP Extended ACL

Start from privileged configuration mode, configure IP extended ACL as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configration mode.
Step 2	**access-list** *access-list-index*	Enter ACL configuration mode. *access-list-number* is ACL index. range:1000-1999.
Step 3a	**subset protocol** <deny | permit> *protocol* <*A.B.C.D A.B.C.D* | **host** *A.B.C.D* | any > <*A.B.C.D A.B.C.D* | **host** *A.B.C.D* | any > [<match | set > <dscp *priority*| precedence *priority* | tos *priority*>]	Configure IP extended ACL rule. Parameter *protocol* should be icmp, igmp, igrp, ip, ospf, pim, tcp, or udp, etc. it also can be replaced by protocol code 0~255.
Step 3b	**exit**	Exit global configuration mode.
Step 4	**no access-list** *access-list-index*	Delete ACL
Step 5	**show access-list index** <*access-list-index* |all>	Show ACL configurations.
Step 6	**write**	Save configurations.

12.2.3 ACL Based on IP Address

Start from the privileged configuration mode, apply the ACL rules to the IP as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**access-list** (1000-1999)	Enter ACL configuration mode. *access-list-number* is ACL index.

		range:1000-1999.
Step 3a	**subset protocol** <deny|permit> [tcp|udp|igmp|ipinip|ospf|icmp|pim|egp|gre|rsvp|ip|(0-255)] <*A.B.C.D A.B.C.D* | host *A.B.C.D* | any > <*A.B.C.D A.B.C.D* | host *A.B.C.D* | any > [<match | set > <dscp *priority* | precedence *priority* | tos *priority*>]	Configure IP ACL rule.
Step 3b	**exit**	Exit global configuration mode.
Step 4	**no access-list** *access-list-index*	Delete ACL
Step 5	**show access-list index** <*access-list-index* | all>	Show ACL configurations.
Step 6	**write**	Save configurations.

12.2.4 ACL Based on MAC Address

Start from the privileged configuration mode, apply the ACL rules to the MAC as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**access-list** *access-list-number*	Enter ACL configuration mode. *access-list-number* is ACL index. range:2000-2999.
Step 3a	**subset ethernet** <permit|deny> **source** *xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx* {dest *xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx* | valn (1-4094) | cos (0-7) | ethernet-type *xxxx xxxx*}*1	Configure IP extended ACL rule.
Step 3b	**exit**	Exit to global configuration mode.
Step 4	**no access-list** *access-list-index*	Delete ACL
Step 5	**show access-list index** <*access-list-index* | all>	Show ACL configurations.
Step 6	**write**	Save configurations.

12.2.5 ACL Based on MAC and IP Address

Start from the privileged configuration mode, apply the ACL rules to the MAC and IP as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**access-list** (5000-5999)	Enter ACL configuration mode. *access-list-number* is ACL index. range:5000-5999.
Step 3a	**subset port-business** <deny|permit> <src-ip | dest-ip> *A.B.C.D A.B.C.D* [{[dest-ip *A.B.C.D A.B.C.D*] | protocol (0-255) (0-255) | tos-dscp (0-255) (0-255)}*1]	Permit:Permit data stream which match the rule passing through. Deny:Do not permit data stream which match the rule passing through. dest:destination MAC address source :source MAC address *X:X:X:X:X:X*：MAC address mask
Step 3b	**subset port-business** <deny|permit> <src-mac *xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx*|dest-mac *xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx*> [{[dest-mac *xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx*] | vlan (1-4096) (1-4096) | cos (0-7) |ethernet-type *xxxx*}*1]	Permit:Permit data stream which match the rule passing through. Deny:Do not permit data stream which match the rule passing through. dest:destination MAC address source :source MAC address A.B.C.D：IP address mask
Step 3c	**exit**	Exit to global configuration mode.
Step 4	**no access-list** *access-list-index*	Delete ACL
Step 5	**show access-list index** <*access-list-index* | all>	Show ACL configurations.
Step 6	**write**	Save configurations.

12.2.6 ACL Based on Ports

This type of ACL includes other types.
Start from the privileged configuration mode and configure ACLs based on port binding, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration

		mode
Step 2	**access-list** *access-list-number*	Enter the ACL configuration mode. The ID of the access list is an ACL index. The value ranges from 5000-5999.
Step 3a	**subset port-business** <permit|deny> <src-port (0-65535) *xxxx* | dest-port (0-65535) *xxxx*>	Allow: Allows the flow of data that complies with the rules. Reject: Data matching the rule is not allowed to flow. src ip: indicates the source ip address dest ip: indicates the destination ip address Protocol: IP protocol type tos-dscp: indicates the IP priority src-mac: indicates the source mac address dest-mac: indicates the destination mac address vlan: indicates the VLAN ID cos: 802.1p priority Ethernet-type: indicates the ethernet type src-port: indicates the Layer 4 source port dest-port: indicates the Layer 4 destination port
Step 3b	**no access-list** *access-list-index*	Delete ACL
Step 4	**exit**	Exit the global configuration mode
Step 5	**show access-list** *access-list-number*	Show ACL configuration
Step 6	**write**	Save configuration

12.2.7 Apply ACL to the Port

Start from the privileged configuration mode, apply ACL rules to ports, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration

		mode
Step 2	**interface** *interface_type slot/port*	The port configuration mode is displayed
Step 3a	**ip access-group** *access-list-number* <in | out>	Apply ACL rules to ports
Step 3b	**no ip access-group** *access-list-number* <in | out>	Example Delete an ACL rule from a port
Step 4	**exit**	Exit the global configuration mode
Step 5	**show access-list** *access-list-number*	Show ACL configuration
Step 6	**write**	Save configuration

12.2.8 IPv6 standard ACL Configuration

Start from the privileged configuration mode, configure the IPV6 standard ACL according to the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**access-list ipv6** *access-list-index*	Enter the ACL configuration mode. An access list is an ACL index. The value ranges from 0 to 999.
Step 3a	**subset ipv6** <permit | deny> *X:X::X:X/M*	Configure ACL rules. <X:X: X:X> : indicates the ACL rule definition based on the source IP address and mask.
Step 3b	**exit**	Exit the global configuration mode
Step 4	**no access-list ipv6** *access-list-index*	Delete ACL
Step 5	**show access-list ipv6 index** <*access-list-index* | active | all>	Show ACL configuration
Step 6	**write**	Save configuration

12.2.9 IPv6 Extended ACL configuration

Start from the privileged configuration mode, configure the IPV6 extended ACL according to the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**access-list ipv6** *access-list-index*	Enter the ACL configuration mode. The ID of the access list is an ACL index. The value ranges from 1000 to 1999.
Step 3a	**subset protocol** <deny|permit> <(0-255)|igmpv6|ipv6|ospf|tcp|udp> [<src-ipv6 *X:X::X:X/M*|src-port (0-65535)| dest-ipv6 *X:X::X:X/M*|dest-port (0-65535)|dscp (0-63)>]	Configure an extended ACL rule. The parameter protocol can be icmp, igmp, igrp, IP, ospf, pim, tcp, or udp, or the protocol number can be 0 to 255.
Step 3b	**exit**	Exit the global configuration mode
Step 4	**no access-list ipv6** *access-list-index*	Delete ACL
Step 5	**show access-list ipv6 index <***access-list-index* | active | all>	Show ACL configuration
Step 6	**write**	Save configuration

12.2.10 ACL based on IPv6 addresses

Start from the privileged configuration mode, apply ACL rules to IP addresses, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**access-list ipv6** *access-list-index*	Enter the ACL configuration mode. The ID of the access list is an ACL index. The value ranges from 1000 to 1999.
Step 3a	**subset protocol** <deny|permit> <(0-255)|igmpv6|ipv6|ospf|tcp|udp> [<src-ipv6 *X:X::X:X/M*|src-port (0-65535)| dest-ipv6 *X:X::X:X/M*|dest-port (0-65535)|dscp (0-63)>]	Configure an extended ACL rule. The parameter protocol can be icmp, igmp, igrp, IP, ospf, pim, tcp, or udp, or the protocol number can be 0 to 255.
Step 3b	**exit**	Exit the global configuration

		mode
Step 4	**no access-list ipv6** *access-list-index*	Delete ACL
Step 5	**show access-list ipv6 index <***access-list-index* | active | all>	Show ACL configuration
Step 6	**write**	Save configuration

12.2.11 ACL based on IPv6 and MAC Addresses

Start from the privileged configuration mode, ACL rules are applied to both IP and MAC addresses, as shown in the following table

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**access-list ipv6** *access-list-number*	Enter the ACL configuration mode. The ID of the access list is an ACL index. The value ranges from 5000-5999.
Step 3a	**subset port-business** <deny|permit | traffic_classifier> {src-mac *X:X:X:X:X:X X:X:X:X:X:X*|dest-mac *X:X:X:X:X:X X:X:X:X:X:X*> < vlan (1-4094) (0 -4095)|cos (0-7)|ethernet-type *xxxx*}*1	Allow: Allows the flow of data that complies with the rules. Reject: Data matching the rule is not allowed to flow. dest: indicates the destination MAC address source: indicates the source MAC address X:X:X:X:X:X: MAC address and mask
Step 3b	**subset port-business** <deny|permit | traffic_classifier> {src-ipv6 *X:X::X:X/M*|dest-ipv6 *X:X::X:X/M*|protocol (0-255) (0-255)|tos-dscp (0-255) (0-255)}*1	Allow: Allows the flow of data that complies with the rules. Reject: Data matching the rule is not allowed to flow. dest-ipv6: indicates the destination IP address src-ipv6: indicates the source IP address X:X::X:X/M: IP address and mask
Step 4	**exit**	Exit the global configuration mode
Step 5	**show access-list ipv6 index <***access-*	Show ACL configuration

	list-index | active | all>	
Step 6	**write**	Save configuration

12.2.12 IPv6 ACL applied to ports

Start from the privileged configuration mode, apply ACL rules to ports, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface** *interface_type slot/port*	The port configuration mode is displayed
Step 3a	**ipv6 access-group** *access-list-number* <in|out>	Apply ACL rules to ports
Step 3b	**no ipv6 access-group** *access-list-number* <in|out>	Example Delete an ACL rule from a port
Step 4	**exit**	Exit the global configuration mode
Step 5	**show access-list ipv6 index <***access-list-index* | active | all>	Show ACL configuration
Step 6	**write**	Save configuration

12.3 Examples

(1)Reject packets with specific IP addresses

PON1 denies the packet whose source IP address is 192.168.100.10.

```
gpon-olt(config)# access-list 5000
gpon-olt(config-bsn-acl-5000)# subset port-business deny src-ip 192.168.100.10 255.255.255.255
gpon-olt(config-bsn-acl-5000)# exit
gpon-olt(config)# interface gpon 0/1
gpon-olt(config-pon-0/1)# ip access-group 5000 in
```

(2)Allow packets with specific MAC addresses to pass through

PON1 allows IP packets whose source MAC address is B8:97:55:72:37:8D to pass.

```
gpon-olt(config)#access-list 2000
gpon-olt(config-eth-acl-2000)# subset ethernet deny ethernet-type 0800 ffff
gpon-olt(config-eth-acl-2000)#exit
gpon-olt(config)# access-list 2001
gpon-olt(config-eth-acl-2001)# subset ethernet permit source b8:97:5a:72:37:8d ff:ff:ff:ff:ff:ff
```

```
gpon-olt(config-eth-acl-2001) # exit
gpon-olt(config)# interface gpon 0/1
gpon-olt(config-pon-0/1)# ip access-group 2000 in
gpon-olt(config-pon-0/1)# ip access-group 2001 in
gpon-olt(config-pon-0/1)#exit
```

13. QoS Configure

13.1 Configure the queue scheduling mode

Queue scheduling modes include strict priority, weighted cyclic scheduling and mixed scheduling. The device supports a total of eight queues.
Start from the privileged configuration mode, configure the queue scheduling mode as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**queue-scheduler strict-priority**	Configure the strict priority scheduling mode
Step 2b	**queue-scheduler wrr** [*queue0 |queue1|queue2|queue3|queue4|queue5|queue6|queue7*]	Set the weighted cyclic scheduling mode. Queuex is the weight of queue x. The value ranges from 1 to 127. By default, the weights of queues 0 to 7 are 1, 1, 2, 2, 4, 4, 8, and 8.
Step 2c	**queue-scheduler sp-wrr** [*queue0 |queue1|queue2|queue3|queue4|queue5|queue6|queue7*]	Configure the mixed scheduling mode. Queuex is the weight of queue x and ranges from 0 to 127. If it is set to 0, the queue is listed as a strict priority queue. By default, the weights of queues 0 to 7 are 1, 1, 2, 2, 4, 4, 8, and 8.
Step 3	**show queue-scheduler**	Displays the queue scheduling configuration.
Step 4	**write**	Save configuration

14. Configure STP

14.1 STP Default Settings

STP Default Settings：

Speciality	Default value
Enable status	STP disabled
Bridge priority	32768
STP port priority	128
STP port cost	10-Gigabit Ethernet :2 Gigabit Ethernet :4 Fast Ethernet :19 Ethernet :100
Hello time	2s
Forward delay time	15s
Maxmum aging time	20s
Mode	RSTP

14.2 STP Configure

STP configuration includes:

- Enables the STP function of the device
- Enable the STP function on the port
- Configuring the STP Mode
- Configure the bridge priority of the device
- The forwarding delay of the device is configured
- The hello time of the device was set
- The maximum service life of a specified device is specified
- Configures the priority of a specified port
- The path cost of a specified port is specified

14.2.1 Enable the STP Function

Start from the privileged configuration mode, enable the STP function on the device, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**spanning-tree on**	Enable the STP function on the device. By default, STP is

		disabled.
Step 2b	**no spanning-tree**	The STP function of the device is disabled
Step 3	**show spanning-tree**	Show STP configuration
Step 4	**write**	Save configuration

14.2.2 Enable STP on a Port

In order to work flexibly, you can disable some specific ports' STP function.
Start from the privileged configuration mode, enable the STP function on the port, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface** *interface_type slot/port*	The port configuration mode is displayed
Step 3a	**spanning-tree on**	The STP function on the port is enabled
Step 3b	**no spanning-tree on**	The STP function on a port is disabled
Step 4	**exit**	Exit the global configuration mode
Step 5	**show spanning-tree interface** *interface_type slot/port*	The STP configuration of the port is displayed
Step 6	**write**	Save configuration

14.2.3 Configure the Bridge Priority

The bridge priority of the device determines whether it will be selected as the root of the tree.
Start from the privileged configuration mode, configure the bridge priority of the device as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**spanning-tree priority** *bridge-priority*	Configure the bridge priority of the device. The priority ranges from 0 to 61440. The default value is 32768.

Step 3	**show spanning-tree**	Show STP configuration
Step 4	**write**	Save configuration

14.2.4 Configure the Forwarding Latency

When a link failure occurs in the network, the network recalculates the spanning tree. The structure of the spanning tree will also change. However, the new STP PDUs cannot be recycled over the network. In this case, a temporary loop occurs if the new root port and the specified port immediately forward the data. Therefore, STP uses a state transition mechanism. The root port and the specified port are in an intermediate state before the data is re-forwarded. After the forwarding delay in the intermediate state times out, the new STP PDU circulates in the network, and then the root port and the specified port start to forward data.

Start from the privileged configuration mode, configure the forwarding delay of the device according to the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**spanning-tree forwardDelay** *seconds*	The forwarding delay of the device is configured. The bridging priority ranges from 4 to 30. The default value is 15.
Step 3	**show spanning-tree**	Show STP configuration
Step 4	**write**	Save configuration

The forwarding delay is related to the size of the network. Generally, the larger the network, the longer the forwarding delay to be configured. If the forwarding delay is too small, temporary redundant paths may exist. Although it is too big, the network will need more time to restore the connection. If you don't know this, we recommend that you use the default values.

Attention:

Hello Time, Forward Delay, and Max Age are the time parameters of the root device. These three parameters should meet the following formula, otherwise, the network will be unstable.

2 × (forward delay-1) >= maximum age

maximum age >= 2 × (hello + 1)

The unit of “1” in formula is second.

14.2.5 Configure Hello Time

The bridge will periodically send greeting messages to other nearby Bridges to verify

the link connection. An appropriate hello time ensures that the device detects link faults in time without occupying more network resources. If the hello time is too large, the device misidentifies the link as faulty when it loses data packets. The network device then recalculates the spanning tree. If it is too small, the network device will frequently send repeated STP PDUs. This will increase the load on the device and waste network resources.

Start from the privileged configuration mode, configure the hello time of the device, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**spanning-tree hellotime** *seconds*	Configure the greeting time of the device. The greeting time ranges from 1 to 10. The default value is 2.
Step 3	**show spanning-tree**	Show STP configuration
Step 4	**write**	Save Configure

14.2.6 Configure Maximum Aging Time

The maximum aging time is the maximum service life of the configuration message. When the message duration is greater than the maximum, the configuration message is discarded.

Start from the privileged configuration mode, set the maximum aging time according to the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**spanning-tree max-age** *seconds*	The maximum aging time of the device is specified. The maximum aging time ranges from 6 to 40, and the default value is 20
Step 3	**show spanning-tree**	Show STP configuration
Step 4	**write**	Save configure

14.2.7 Configure the Priority of a Specified Port

Port priority determines whether the port can be selected as the root port. Under the same conditions, the port with a higher priority is selected as the root port. Generally, the smaller the priority value, the higher the priority of the port. If all ports have the

same priority value, their priority is determined by their port number.
Start from privileged configuration mode, configure the priority of the specified port as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface** *interface_type slot/port*	The port configuration mode is displayed
Step 3	**spanning-tree port-priority** *priority*	Configures the priority of a specified port. The priority ranges from 0 to 255. The default value is 128.
Step 4	**exit**	Exit the global configuration mode
Step 5	**show spanning-tree interface** *interface_type slot/port*	The STP configuration of the port is displayed
Step 6	**write**	Save configure

14.2.8 Configure Maximum Aging Time

The maximum aging time is the maximum service life of the configuration message. When the message duration is greater than the maximum, the configuration message is discarded.
Start from the privileged configuration mode, set the maximum aging time according to the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**spanning-tree max-age** *seconds*	The maximum aging time of the device is specified. The maximum aging time ranges from 6 to 40, and the default value is 20
Step 3	**show spanning-tree**	Show STP configuration
Step 4	**write**	Save configure

14.2.9 Configure the Priority of a Specified Port

Port priority determines whether the port can be selected as the root port. Under the same conditions, the port with a higher priority is selected as the root port. Generally, the smaller the priority value, the higher the priority of the port. If all ports have the

same priority value, their priority is determined by their port number.
Start from privileged configuration mode, configure the priority of the specified port as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface** *interface_type slot/port*	The port configuration mode is displayed
Step 3	**spanning-tree port-priority** *priority*	Configures the priority of a specified port. The priority ranges from 0 to 255. The default value is 128.
Step 4	**exit**	Exit the global configuration mode
Step 5	**show spanning-tree interface** *interface_type slot/port*	The STP configuration of the port is displayed
Step 6	**write**	Save configure

14.2.10 Configure the Point-to-point Mode

Point-to-point mode is usually a link to a switch. A port connected by a point-to-point link can quickly transition to the forwarding state by sending synchronous packets when certain port role conditions are met, thus reducing unnecessary forwarding delay.
Start from the privileged configuration mode, configure the port point-to-point link, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface** *interface_type slot/port*	The port configuration mode is displayed
Step 3a	**spanning-tree link-type point-to-point enable**	Configure the port as a point-to-point port. By default, all ports are configured as point-to-point ports.
Step 3b	**spanning-tree link-type point-to-point disable**	Example Delete the configuration of a point-to-point port
Step 4	**exit**	Exit the global configuration mode
Step 5	**show spanning-tree interface** *interface_type slot/port*	The STP configuration of the port is displayed
Step 6	**write**	The STP configuration of the

	port is displayed

14.3 Display STP Information

After the configuration, run the following command to display STP information.

Command	Function
show spanning-tree	Displays the STP configuration and running status
show spanning-tree interface *interface_type slot/port*	Displays the STP configuration and port running status

15. Loop Detection Configuration

15.1 Configure Loop Detection

15.1.1 Enable Loop Detection Function

Loopback Detect is disabled by default. You can enable it with the following command. Start from the privileged configuration mode, enable/disable Loopback Detect listening, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**Loopback detect enable**	Enable loopback-detect Feature
Step 2b	**No loopback detect**	loopback-detect is disabled Feature
Step 3	**show loopback detect**	The loopback-detect configuration is displayed
Step 4	**write**	Save configuration

15.1.2 Configure the Loop Detection Range

After this function is configured, you can enable loop detection only for the upper link port, pon port, or all ports, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Loopback detect enable all**	Enable full-port loop detection
Step 3	**Loopback detect enable uplink**	Enable loop detection of the upper interface
Step 4	**Loopback detect enable pon**	Enable loop detection of the PON port
Step 5	**write**	Save configure

15.1.3 Configure the Loop Detection Mode

If different loop detection modes are configured, the device processes loops in different

ways after detecting loops. If the mode is Auto recovery, the device automatically turns down the port after detecting a loop and automatically turns up the port after a period of time. If the configuration mode is manual recovery, the device will down the port after detecting a loop, and you need to enable the port. If the configuration mode is alarm only, the device only sends an alarm message after detecting a loop and does not process the port. The following table describes the command configuration.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**loopback mode auto-recovery**	Set the loop detection mode to automatic recovery
Step 3	**loopback mode manual-recovery**	Set the loop detection mode to manual recovery
Step 4	**loopback mode only-alarm**	Set the loop detection mode to alarm only
Step 5	**Write**	Save configure

15.1.4 Configure the Aging Time

Aging time is the maximum service life of loop messages. Loop messages are discarded when the message duration is greater than the maximum. When a loop occurs on the network, the device displays the detected loop information. After the aging time is reached, the information is deleted and no longer displayed. The following table shows the specific configurations.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**loopback aging-time** (*10-3600)*	The aging time of loop detection ranges from 10 to 3600s
Step 3	**show loopback detect**	The loopback-detect configuration is displayed
Step 4	**write**	Save configure

15.1.5 Configure Loop Detection Packet Send Method

Loop detection packets can be sent by port or vlan, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode

Step 2	**Loopback packet-send port-base**	Set the packet sending mode to the port
Step 3	**loopback packet-send vlan-base**	Send to vlan
Step 4	**write**	Save configure

15.1.6 Configure the Time for Sending Data Packets

This parameter is used to determine the interval for sending loop data packets, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Loopback packet-send port-base** *(1-720)*	The packet sending time was set The range is 1-720s
Step 3	**show loopback detect**	Display loop information
Step 4	**write**	Save configure

15.2 Loop Detection Port Configuration

Access the port and enable loop detection for the port, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface** *interface_typeslot/port*	The port configuration mode is displayed
Step 3	**loopback enable**	Loop detection is enabled for the port
Step 4	**loopback disable**	The loop detection function is disabled on the port
Step 5	**Exit**	Exit the port configuration mode
Step 6	**Show loopback detect**	Displays loop detection configurations
Step 7	**write**	Save configure

15.3 Display Loop Detection Information

After the configuration, run the following command to display loopback-detect information.

Command	Function
show loopback detect	Displays loop detection information and port configuration status

16. DHCP management Configuration

16.1 DHCP Server Configuration

Now, more and more IP addresses need to be assigned. DHCP (Dynamic Host Configuration Protocol) was created to solve this problem. It includes a DHCP server and a DHCP client. The IP address is assigned by the server at the request of the client. Configure the DHCP server as shown in the following table:

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 2a	**interface vlan** (1-4094)	Enter a VLAN interface
Step 2b	**ip dhcp** *pool name*	The DHCP server function is enabled or disabled
Step 3	**exit**	Exit the global configuration mode
Step 4a	**ip dhcp** *pool name*	Enter the interface of the DHCP address pool
Step 4b	**dns-server** *A.B.C.D A.B.C.D A.B.C.D*	Configure the DHCP DNS server
Step 4c	**wins** *A.B.C.D*	The DHCP WINS server is configured
Step 4d	**address** *A.B.C.D E.F.G.H*	Configure the range of the DHCP IP address pool
Step 4e	**network** *A.B.C.D/M*	Configure the DHCP mask
Step 4f	**default-router** *A.B.C.D*	Configuring a DHCP Gateway
Step 4g	**Leasetime** (60-864000)	Configure the IP address lease
Step 5	**exit**	Exit the global configuration mode
Step 6	**show ip dhcp pool** *pool name*	The DHCP server configuration is displayed
Step 7	**write**	Save configure

16.2 Configure DHCP Relay

Because the DHCP receiving need to broadcast, so the server and the client should be in the same network.The DHCP relay can save this issue effective. Configure DHCP relay as the following table show:

1.Single DHCP relay configuration：

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode
Step 2	**interface vlan** (1-4094)	Add VLAN and enter VLAN interface configuration *vlan_id(*1－4094)
Step 3	**dhcp relay** *A.B.C.D*	Configure the DHP relay server IP address ,and enable the DHCP relay
Step 3b	**no dhcp relay** *A.B.C.D*	Delete DHCP relay
Step 4	**exit**	Exit to global configuration mode
Step 6	**write**	Save the configuration

16.3 Configure DHCP Snooping

To prevent the DHCP message attacking and protect you network to get a useful IP address.DHCP Snooping is used for do that.Configure DHCP Snooping as the following table show:

A.DHCP Snooping enable/disable

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode.
Step 2a	**Dhcp-snooping enable**	Enable DHCP Snooping.（DHCP Snooping enable，can not open dhcp server and dhcp relay）
Step 2b	**dhcp-snooping disable**	disable DHCP Snooping
Step 3a	**Dhcp-snooping vlan** (1-4094)	Configure DHCP Snooping vlan list
Step3b	**no dhcp-snooping vlan** (1-4094)	Delete DHCP Snooping vlan list
Step 4	**exit**	Exit to global configuration mode

Step 5	**show dhcp-snooping configuration**	Show DHCP Snooping configuration
Step 6	**write**	Save configuration

B.Configure DHCP Snooping option82

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode
Step 2	**Dhcp-snooping information option** <enable|disable>	Enable/disable DHCP Snooping option82
Step 3	**Dhcp-snooping information strategy** <drop|keep|replease>	Configure the message with option82，drop、keep and replace
Step 4	**exit**	Exit to global configuration mode
Step 5	**show dhcp-snooping configuration**	Show DHCP Snooping configuration
Step 6	**write**	Save configuration

C.Configure DHCP Snooping binding list

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode
Step 2	**Dhcp-snooping binding** *HHHH:HHHH:HHHH:HHHH* **vlan** (1-4094) *A.B.C.D* **interface** *interface_type slot/port* **lease** (60-1000000)	Add the static DHCP binding list
	no dhcp-snooping binding mac *HHHH:HHHH:HHHH:HHHH*	Delete MAC binding list
	no dhcp-snooping binding <all|static|dynamic>	Delete DHCP binding list.can delete all、static、dynamic
Step 3	**Dhcp-snooping binding delete-time** (1-3600)	Configure the biding list aging time and delete time
Step 4	**exit**	Exit to global configuration

		mode
Step 5	**show dhcp-snooping binding** <all|static|dynamic>	Show DHCP Snooping configuration
Step 6	**write**	Save configuration

D.Configure DHCP Snooping port

	Command	**Function**
Step 1	**config terminal**	Enter global configuration mode
Step 2	**interface** *interface_type slot/port*	Enter the interface configuration
Step 3a	**Dhcp-snooping trust**	Configure the trust port. All the port are untrust in default
Step 3b	**Dhcp-snooping untrust**	Delete trust port.
Step 3c	**Dhcp-snooping information circuit-id string** *string*	Configure the option82 circuit-id value
Step 3d	**no dhcp-snooping information circuit-id string**	Delete option82 circuit-id value,load default value
Step 3e	**Dhcp-snooping information remote-id string** *string*	Configure option82 remote-id value
Step 3f	**no dhcp-snooping information remote-id string**	Delete option82 remote-id value，load default value
Step 3g	**Dhcp-snooping limit rate** (0-4096)	Configure the port max speed of receiving the DHCP packet. It doesn't limit by default
Step 3h	**no dhcp-snooping limit rate**	No limit speed
Step 4	**exit**	Exit to the global configuration mode
Step 5a	**Dhcp-snooping errdisable recovery** <enable|disable>	CConfigure whether the port get down when the DHCP packetreceiving speed larger then the limit speed .The default is disable
Step 5b	**Dhcp-snooping errdisable recovery interval** (3-3600)	Configure the time when the port recovery after getting down
Step 6	**show dhcp-snooping configuration**	Show DHCP Snooping configuration

Step 7	**write**	Save configuration

16.4 Configure IP Source Guard

IP Source Guard (IPSG) is an IP/ MAC-based port traffic filtering technology that prevents IP address spoofing attacks on local area networks. IPSG ensures that the IP addresses of end devices in the Layer 2 network are not hijacked, but also ensures that unauthorized devices cannot access the network through their own IP address or attack the network to crash and crash the network.

	Command	**Function**
Step 1a	**ip source binding** {*A.B.C.D/M*|*X:X:X:X:X:X*} [{vlan (1-4094)|interface <gigabitEthernet S/P|gpon S/P }]	Configure static IP address binding for the interface gigabitEtherne or PON port
Step 1b	**no ip source binding** {*A.B.C.D/M*|*X:X:X:X:X:X*} [{vlan (1-4094)|interface <gigabitEthernet S/P |gpon S/P }]	Delete static IP address binding for the interface gigabitEtherne or PON port
Step 6	**show ip source binding**	Show the binding list

Enter the interface mode and configure the ip source Guard function.

	Command	**Function**
Step 1	**interface** <gigabitethernet S/P |gpon S/P >	Enter the interface configuration
Step 2a	**ip verify source** <ip-address|mac-address|ip-mac-address> **vlan** (1-4094)	Configure the ip source Guard function on a port
Step 2b	**no ip verify source vlan** (1-4094)	Delete ip source Guard
Step 3	**show ip verify source** [<gigabitEthernet S/P|gpon S/P|] [json]	Show ip source Guard configuration

17. L3 Route Configuration

17.1 L3 Route Configuration

17.1.1 Router Table

	Command	Function
Step 1	**debug mode**	Enter the debug configuration mode
Step 2a	**show l3 defip route**	Show defip route information
Step 2b	**show l3 hostroute**	Show host routing information
Step 2c	**show l3 interface**	Show interface information

17.1.2 Static Route

Static route is usually used in a simple network. This device supports maximum 512 static route rules.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**ip route** *<A.B.C.D A.B.C.D|A.B.C.D/M> A.B.C.D A.B.C.D*	Add static route rule
Step 3	**no ip route** *<A.B.C.D A.B.C.D|A.B.C.D/M> A.B.C.D A.B.C.D*	Delete static route rule
Step 4	**show ip route**	Show route rules

17.1.3 Key Chain

Key management is a method of controlling the authentication key used by a routing protocol. Not all protocols can use key management. The authentication key is available for EIGRP and RIP version 2. Authentication must be enabled before managing the authentication key. See the appropriate protocol section for how to enable authentication for this protocol. To manage an authentication key, you need to define a keychain that identifies the keys that belong to the keychain. Each key has its own key

identifier, which is stored locally. The key identifier and the combination associated with the message uniquely identify the use of the authentication algorithm and the MD5 authentication key. Multiple keys can be configured. Only one authentication package is sent, no matter how many valid keys exist. The software checks key figures from lowest to highest order and uses the first valid key it encounters.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**key chain** *key_chain_name*	Configure the key chain and enter the key chain configuration mode
Step 3	**key** *key_number*	Configure the key identifier，key_number range 0- 2147483647
Step 4	**key-string** *key_string*	Configure the authentication key
Step 5	**exit**	Exit to the global configuration mode
Step 6	**write**	Save configuration

To remove the key chain entry, use the command **no key chain**;To delete a key identifier, use the command **no key**;To delete the key, use the command **no key-string**.

18. RIP

18.1 RIP Overview

RIP (routing information protocol) is a simple internal gateway protocol. RIP is a routing protocol based on D-V algorithm. Hop Count is used to represent metrics. The hop count is the number of routers a datagram must pass to reach the destination. RIP considers that the path with the lowest number of hops is the optimal path, and the maximum number of hops supported is 15. If 16RIP is set, the network is unreachable. Therefore, RIP can only be adapted to small networks.

18.2 RIP Configuration

RIP configuration includes:

- Configure RIP basic parameters
- Configure RIP authentication
- Configure RIP Split Horizon

18.2.1 RIP Basic Configuration

To configure RIP, you enable RIP routing for a network and optionally configure other parameters.
Beginning in privileged EXEC mode, follow these steps to enable and configure RIP:

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router rip**	Enable a RIP routing process, and enter router configuration mode.
Step 3	**network** *A.B.C.D/M*	Associate a network with a RIP routing process. You can specify multiple network commands. RIP routing updates are sent and received

		through interfaces only on these networks.
Step 4	**neighbor** *A.B.C.D*	(Optional) Define a neighboring router with which to exchange routing information. This step allows routing updates from RIP (normally a broadcast protocol) to reach nonbroadcast networks.
Step 5	**offset-list** <*access-list number*| *name*> <in|out> (0-16) **vlan** (1-4094)	(Optional) Apply an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through RIP. You can limit the offset list with an access list or an interface.
Step 6	**timers basic** (5-2147483647) (5-2147483647) (5-2147483647)	seconds. •update—Time between sending routing updates. The default is 30 seconds. •invalid—Time after which a route is declared invalid. The default is 180 seconds. •holddown—Time before a route is removed from the routing table. The default is 180 seconds. •flush—Amount of time for

		which routing updates are postponed. The default is 240 seconds
Step 7	**version** (1|2)	(Optional) Configure the switch to receive and send only RIP Version 1 or RIP version 2 packets. By default, the switch receives Version 1 and 2 but sends only Version 1. You can also use the interface commands ip rip {send | receive} version 1 | 2 | 1 2} to control what versions are used for sending and receiving on interfaces
Step 8	**redistribute** (kernel|connected|ospf|static) **metric** (0-16)	(Optional) redistribute routes from kernel、connect、ospf and static.
Step 9	**distance** (1-255)	(Optional) Configure RIP protocol distance. Default 120.
Step 10	**exit**	Return to privileged EXEC mode.
Step 11	**show ip rip status**	Showing RIP current status. About the RIP timer, filter list,version,interface information.
Step 12	**show ip rip**	Showing RIP route

		information.
Step 13	**write**	Save configurations.

If you want to disable RIP routing, use the command **no router rip** in global configuration mode.

If you want to cancel the interface RIP process, you can use the command **no network ip-address/masklen** in RIP configuration mode.

If you want to restore the default timer value, you can use the command **no timers basic** in RIP configuration mode.

18.2.2 RIPv2 Authentication

RIP version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface. The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed, not even the default.

The OLT supports two modes of authentication on interfaces for which RIP authentication is enabled: plain text and MD5. The default is plain text.

Beginning in privileged EXEC mode, follow these steps to configure RIP authentication on an interface:

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** (1-4094)	Enter interface configuration mode, and specify the interface to configure.
Step 3	**ip rip authentication mode** (md5| text)	Configure the interface to use plain text authentication (the default) or MD5 digest authentication.
Step 4a	**ip rip authentication key-chain** *line*	Enable RIP authentication for MD5.
Step 4b	**ip rip authentication string** *line*	Enable RIP authentication

		for plain text.
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**show ip rip status**	Showing RIP current status. About the RIP timer, filter list,version,interface information.
Step 7	**show ip rip**	Showing RIP route information.
Step 8	**write**	Save configurations.

To restore clear text authentication, use the command **no ip rip authentication mode** interface configuration. To prevent authentication, use the command **no ip rip authentication key-chain** interface configuration.

18.2.3 Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature usually optimizes communication among multiple routers, especially when links are broken.
Beginning in privileged EXEC mode, follow these steps to set an interface to configuring split horizon on the interface:

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**Interface vlan** (1-4094)	Enter interface configuration mode, and specify the interface to configure
Step 3	**ip rip split-horizon**	Enable split horizon. Default enable
Step 5	**exit**	Return to privileged EXEC mode
Step 6	**show ip rip status**	Showing RIP current status. About the RIP timer, filter list,version,interface information

Step 7	**show ip rip**	Showing RIP route information
Step 8	**write**	Save configurations

To disable split horizon, use the **no ip rip split-horizon** interface configuration command.

18.2.4 RIP v1/2 Compatible Configuration

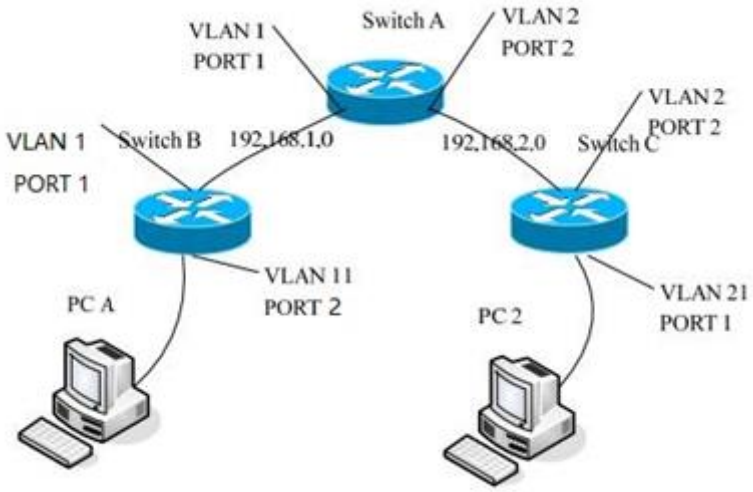
	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**Interface vlan** (1-4094)	Enter interface configuration mode, and specify the interface to configure.
Step 3	**ip rip receive version**（1|2）（1|2）	Configure receive v1 or v2 or v1 and v2.
Step 4	**ip rip send version**（1|2）（1|2）	Configure send v1 or v2 or v1 and v2.
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**show ip rip status**	Showing RIP current status. About the RIP timer, filter list,version,interface information.
Step 7	**show ip rip**	Showing RIP route information.
Step 8	**write**	Save configurations.

18.3 RIP Configuration Example

18.3.1 RIP General Configuration

1. Networking requirements
A small company office network needs to be able to communicate between any two nodes, and the network size is relatively small. Need equipment
Automatically adapt to network topology changes and reduce manual maintenance workload.
According to the user requirements and the user network environment, the RIP routing protocol is selected to implement interworking between user networks.

2. Networking topology



Configuration:
Switch A :VLAN 1 192.168.1.1, VLAN 2 192.168.2.1

interface vlan 1
ip address 192.168.1.1/24
exit
interface vlan 2
ip address 192.168.2.1/24
exit
interface gigabitethernet 0/1
switchport access vlan 1
interface gigabitethernet 0/2
switchport access vlan 2

Enable RIP and run RIP in the VLAN interface
network 192.168.1.0/24
network 192.168.2.0/24

/**********
Switch B:(Similar to switch A)
interface vlan 1
ip address 192.168.1.2/24
exit

interface vlan 11
ip address 192.168.11.2/24
exit

interface gigabitethernet 0/1

switchport access vlan 1

interface gigabitethernet 0/2
switchport access vlan 11

router rip
network 192.168.11.0/24
network 192.168.1.0/24

/**
Switch C:
interface vlan 1
ip address 192.168.21.3/24
exit

interface vlan 2
ip address 192.168.2.3/24
exit

interface gigabitethernet 0/1
switchport access vlan 21

interface gigabitethernet 0/2
switchport access vlan 2

router rip
network 192.168.21.0/24
network 192.168.2.0/24

18.3.2 RIP Offset-list Configuration

Connect switch A and switch B
Switch A:
configure terminal
ip access-list 5 permit 192.168.3.0 0.0.0.0

interface vlan 1
ip adderss 192.168.1.1/24
exit

interface vlan 2
ip adderss 192.168.2.1/24
exit

router rip
offset-list 5 in 3 vlan 1 //offset-list check the entry notification and add 3 to the item metrics that satisfy the list.networke 192.168.1.0/24
networke 192.168.2.0/24

Switch B:
configure terminal
access-list 5 permit 192.168.3.0 0.0.0.0 // Define the access list to determine which routes to match
interface vlan 1
ip adderss 192.168.1.2/24

interface vlan 3
ip adderss 192.168.3.1/24
exit

router rip
networke 192.168.1.0/24
networke 192.168.3.0/24

After configure offset-list,we can type command **show ip rip** in switch A,it show the route table 192.168.3.0 metric is 4, If not set offset-list,the metric is 2.

18.3.3 RIPv2 Authentication

RIPv2 protocol supports MD5 and t text authentication,the same
topology as above.
The configuration of Switch A and Switch B
configure terminal
key chain test // Configure a keychain called test
key 1 // The only key on this keychain is "key 1"
key-string admin // It contains an authentication password “admin”
exit
exit

interface vlan 1
ip rip authentication key-chain test
ip rip authentication mode md5

interface vlan 2
ip rip authentication key-chain test
ip rip authentication mode md5

the result:
Type command **show ip rip** in Switch A
It will show route table 192.168.2.0, not show route table 192.168.23.0.
Type command **show ip rip** in Switch B
It only show route table 192.168.12.0.
If Swith A and Switch B are not the same authentication mode, they can't obtain route table each other.

18.4 OSPF

18.4.1 OSPF Overview

Open Shortest Path First (OSPF) is a link state-based interior gateway protocol developed by the IETF organization. Currently using version 2 (RFC2328), its features are as follows:

- ✓ Adaptable to a wide range of networks - supporting networks of all sizes and supporting up to hundreds of routers.
- ✓ Fast convergence——sends the update packet immediately after the topology of the network changes, so that the change is synchronized in the autonomous system.
- ✓ No loopback——Because OSPF uses the shortest path tree algorithm to calculate routes based on the collected link state, the algorithm itself ensures that loopback routes are not generated.
- ✓ Area division——allows the network of the autonomous system to be divided into areas for management, and the routing information transmitted between the areas is further abstracted, thereby reducing the occupied network bandwidth.
- ✓ Equivalent routing——supports multiple equal-cost routes to the same destination address.
- ✓ Route grading——Use four different types of routes, in order of priority: intra-area routes, inter-area routes, first-class external routes, and second-type external routes.
- ✓ Supports authentication——supports interface-based packet authentication to ensure the security of route calculation.
- ✓ Multicast transmission——Protocol packets are sent in multicast mode.

18.4.2 OSPF Configuration

18.4.2.1 OSPF Basic Configuration

Enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range.
Beginning in privileged EXEC mode, follow these steps to enable OSPF:

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router ospf**	Enable OSPF routing, and enter router configuration mode.
Step 3	**router-id** *A.B.C.D*	(Optional)Configure router id.
Step 4	**network** *A.B.C.D/M* **area** <*A.B.C.D*|(0-4294967295)>	Define an interface on which OSPF runs and the area ID for that interface. The area ID can be a decimal value or an IP address.
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**write**	Save configurations.

To terminate an OSPF routing process, use the **no router ospf global** configuration command.

18.4.2.2 Configure OSPF Interface

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** (1-4094)	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 3	**ip ospf cost** (1-65535)	(Optional) Explicitly specify the cost of sending a packet on the interface.
Step 4	**ip ospf retransmit-interval** (3-65535)	(Optional) Specify the number of seconds between link state advertisement transmissions. The range is 1 to 65535 seconds. The default is 5 seconds.
Step 5	**ip ospf transmit-delay** (1-65535)	(Optional) Set the estimated number of seconds to wait before sending a link state update packet. The range is 1 to 65535 seconds. The default is 1 second.

Step 6	**ip ospf priority** (0-255)	(Optional) Set priority to help determine the OSPF designated router for a network. The range is from 0 to 255. The default is 1.
Step 7	**ip ospf hello-interval** (1-65535)	(Optional) Set the number of seconds between hello packets sent on an OSPF interface. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 10 seconds.
Step 8	**ip ospf dead-interval** (1-65535)	(Optional) Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 4 times the hello interval.
Step 9	**ip ospf authentication-key** *auth_key*	(Optional) Assign a password to be used by neighboring OSPF routers. The password can be any string of keyboard-entered characters up to 8 bytes in length. All neighboring routers on the same network must have the same password to exchange OSPF information.
Step 10	**ip ospf message-digest-key** (keyid:1-255) **md5** *key*	(Optional) Enable MDS authentication. •keyid—An identifier from 1 to 255. •key—An alphanumeric password of up to 16 bytes.
Step 11	**ip ospf authentication**	Enable ospf authentication.
Step 12	**ip ospf authentication message-digest**	Enable ospf MD5 authentication.

Step 13	**exit**	Return to privileged EXEC mode.
Step 14	**show ip ospf interface** [interface-name]	Display OSPF-related interface information.
Step 15	**write**	Save configurations.

18.4.2.3 Configure OSPF Area Parameters

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution.
Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the area range router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.
Beginning in privileged EXEC mode, follow these steps to configure area parameters:

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router ospf**	Enable OSPF routing, and enter router configuration mode.
Step 3	**area** *area-id* **authentication**	(Optional) Allow password-based protection against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address.

18.4.2.4 Configure OSPF Area Parameters

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area,

but can import AS external routes within the area by redistribution.
Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the area range router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.
Beginning in privileged EXEC mode, follow these steps to configure area ：

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router ospf**	Enable OSPF routing, and enter router configuration mode.
Step 3	**area** *<A.B.C.D|(0-4294967295)>* **authentication**	(Optional) Allow password-based protection against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address.
Step 4	**area** *<A.B.C.D|(0-4294967295)>* **authentication message-digest**	(Optional) Enable MD5 authentication on the
Step 5	**area** *<A.B.C.D|(0-4294967295)>* **stub** [no-summary]	(Optional) Define an area as a stub area. The no-summary keyword prevents an ABR from sending summary link advertisements into the stub area.
Step 6	**area** *<A.B.C.D|(0-4294967295)>* **nssa** [no-summary|translate-always|translate-candidate|translate-never]	(Optional) Defines an area as a not-so-stubby-area. Every router within the same area must agree that the area is NSSA. Select one of these keywords: •no-summary—Select to not send summary LSAs into the NSSA.
Step 7	**area** *<A.B.C.D|(0-4294967295)>* **range** *A.B.C.D/M*	(Optional) Specify an address range for which a single route is advertised. Use this command only with area border routers.
Step 8	**exit**	Return to privileged EXEC mode.
Step 9	**show running ip ospf**	Display OSPF running-config information.
Step 10	**show ip ospf database**	Display lists of information

		related to the OSPF database for a specific router.
Step 11	**write**	Save configurations.

18.4.2.5 OSPF Protocol Creates Default Routes

By default, an OSPF router in a normal OSPF area does not generate a default route even if it has a default route. When the default route in the network is generated by other routing processes, the router must advertise the default route to the entire OSPF autonomous domain. The implementation method is to manually configure the ASBR to generate a default route. After the configuration is complete, the router generates a default ASE LSA (Type 5 LSA) and advertises it to the entire OSPF autonomous domain.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router ospf**	Enter OSPF configure mode.
Step 3	**default-information originate** [always|metric (0-16777214)|metric-type (1-2)|route-map *WORD*]	Configure default route
Step 4	**exit**	Returen global configuration mode.

18.4.2.6 Show OSPF Configurate Information

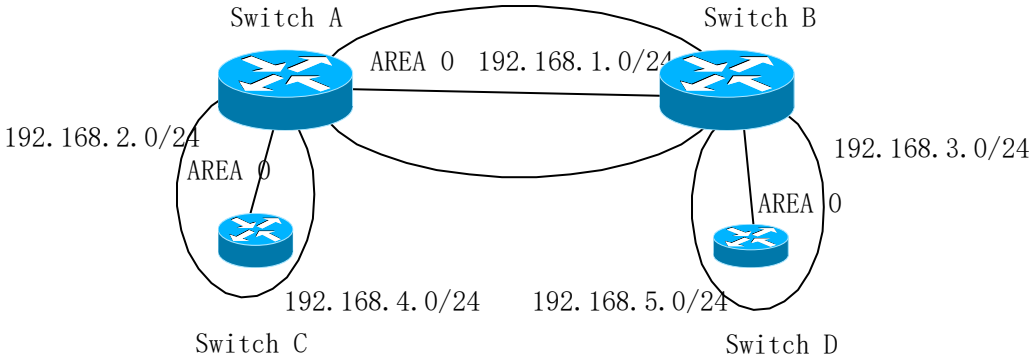
	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show ip ospf database** [asbr-summary|external|network|router|summary|nssa -external|opaque-link|opaque-area|opaque-as] [adv-router A.B.C.D|json]	Display lists of information related to the OSPF database.
Step 3	**show ip ospf route** [json]	Display lists of information related to the OSPF route.
Step 4	**show ip ospf interface**[json | vlan]	Display OSPF-related interface

		information.
Step 5	**show ip ospf neighbor**	Display OSPF interface neighbor information.

18.4.3 OSPF Configuration Example

18.4.3.1 Intra-area Routing

1. Purposes: Test OSPF intra-area route learning
2. Networking topology

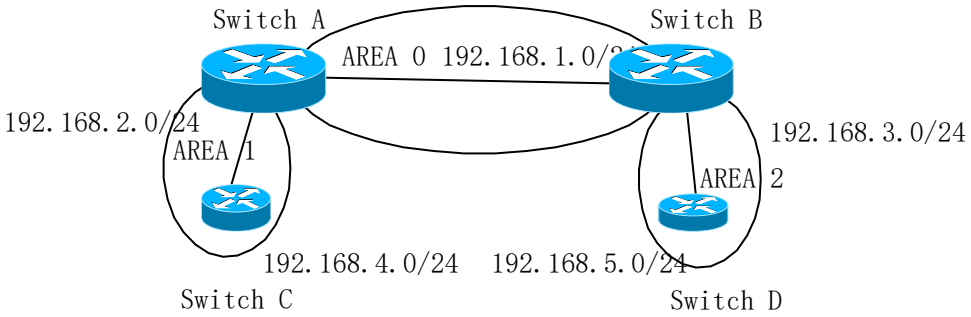


3.Configuration
Switch A create 2 VLAN interface,vlan1 ip 192.168.1.1/24, vlan2 ip 192.168.2.1/24
interface vlan 1
ip address 192.168.1.1/24
exit
interface vlan 2
ip address 192.168.2.1/24
exit
interface gigabitethernet 0/1
switchport access vlan 1
interface gigabitethernet 0/2
switchport access vlan 2
Enable ospf ， and configure these two network segments to run the ospf protocol.
router ospf
router-id 1.1.1.1
network 192.168.1.0/24 area 0
network 192.168.2.0/24 area 0
Switch B，Switch C，Switch D configuration is similar to Switch A.
4.Test result
Switch A route table:192.168.4.0 and 192.168.5.0
Switch B route table:192.168.4.0 and 192.168.5.0

Switch C route table:192.168.1.0 and 192.168.5.0
Switch D route table:192.168.1.0 and 192.168.4.0

18.4.3.2 OSPF Inter-area Routing

1. Purposes: Test OSPF inter-area route learning
2. Networking topology



3.Configuration
Switch A create 2 VLAN interface,vlan1 and vlan2，ip address 192.168.1.1/24，area 0 and 192.168.2.1/24, area 1。
Switch B，create 2 VLAN interface，vlan1 and vlan3，ip address 192.168.1.2/24，area 0 and 192.168.3.1/24, area 2。
Switch C，create 2 VLAN interface，vlan2 and vlan4，ip address 192.168.2.2/24，area 1 and 192.168.4.1/24, area 1。
Switch D create 2 VLAN interface，vlan3 and vlan5，ip address 192.168.3.2/24，area 2 and 192.168.5.1/24, area 2。
The configuration process refers to the route test configuration in the OSPF area.
Test result
Switch A route table：192.168.4.0 and 192.168.5.0；
Switch B route table：192.168.4.0 and 192.168.5.0；
Switch C route table：192.168.1.0 and 192.168.5.0；
Switch D route table：192.168.1.0 and 192.168.4.0.

18.4.3.3 OSPF Route Convergence

1.Purpose: Test OSPF route convergence speed
2.Networking Topology and configuration
Refer to OSPF intra-area route test and OSPF inter-area route test.
Test process

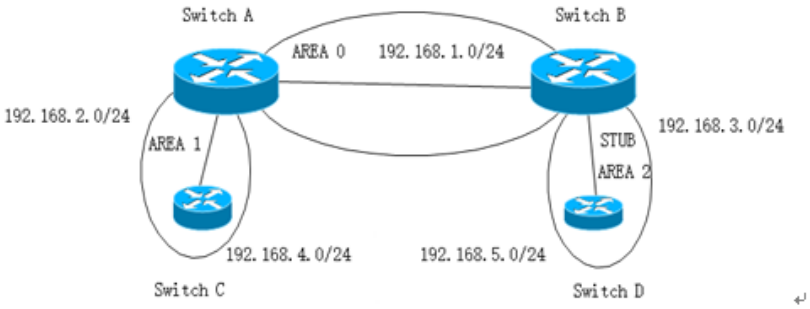
a. intra-area route are converged. Refer to the OSPF intra-area route test to disconnect 192.168.4.0/24 of Switch C.
b. intra-area route are converged. Refer to the OSPF intra-area route test to reconnect 192.168.4.0/24 of Switch C.
c. inter-area route are converged. Refer to the OSPF inter-area route test to disconnect 192.168.4.0/24 of Switch C.

d. inter-area route are converged. Refer to the OSPF inter-area route test to reconnect 192.168.4.0/24 of Switch C

Test result:
Check whether the time of deleting and adding the 192.168.4.0 network segment entries on Switch A, Switch B, and Switch D is the same as the configuration.

18.4.3.4 OSPF Stub Area

1.Purpose: Test OSPF stub area function.
2.Networking Topology



3.Configuration
Set the interconnection between Switch B and Switch D as STUB AREA by referring to the OSPF inter-area route test configuration.
Switch B:

router ospf

area 2 stub

Switch D:

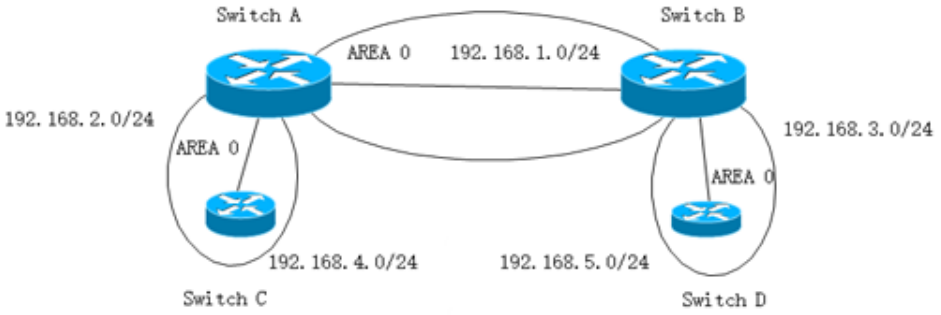
router ospf

area 2 stub

Test result:
After the OSPF inter-area route test is performed, the routing information of Switch A, Switch B, and Switch C is unchanged. The routing table of Switch D adds the default route to the original route entry. The next hop is Switch B.

18.4.3.5 OSPF Route Aggregation

1.Purpose: Test the route aggregation function.
2.Networking topology



3.Configuration

Refer to OSPF intra-area routing configuration.

Switch B learn route aggregation in area 2.

Switch B:

gpon-olt(config)# router ospf

gpon-olt (config-router-ospf)# area 2 range 10.1.0.0/16

Switch C

interface vlan 200

ip address 10.1.1.1/24

interface vlan 201

ip address 10.1.2.1/24

router ospf

network 10.1.1.0/24 area 2

network 10.1.2.0/24 area 2

4.Test result

Before configure route aggregation in SwitchB, Switch A show route 10.1.1.1/24 and 10.1.2.1/24 .After configure route aggregation in SwitchB, only route 10.1.0.0/16 can be seen in SwitchA.

Before aggregation Switch A	172.16.0.0/24 is subnetted, 2 subnets O 172.16.1.0 [110/2] via 192.168.2.2, 00:00:02, Vlan2 O 172.16.2.0 [110/2] via 192.168.2.2, 00:00:02, Vlan2 O 192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02, Vlan2 O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:00:02, Vlan1 10.0.0.0/24 is subnetted, 2 subnets O IA 10.1.2.0 [110/3] via 192.168.1.2, 00:00:02, Vlan1 O IA 10.1.1.0 [110/3] via 192.168.1.2, 00:00:02, Vlan1 C 192.168.1.0/24 is directly connected, Vlan1

	C 192.168.2.0/24 is directly connected, Vlan2 O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:00:03, Vlan1
After aggregation Switch A	172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks O 172.16.0.0/16 is a summary, 00:01:47, Null0 O 172.16.1.0/24 [110/2] via 192.168.2.2, 00:01:47, Vlan2 O 172.16.2.0/24 [110/2] via 192.168.2.2, 00:01:47, Vlan2 O 192.168.4.0/24 [110/2] via 192.168.2.2, 00:01:47, Vlan2 O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:47, Vlan1 10.0.0.0/16 is subnetted, 1 subnets O IA 10.1.0.0 [110/3] via 192.168.1.2, 00:00:16, Vlan1 C 192.168.1.0/24 is directly connected, Vlan1 C 192.168.2.0/24 is directly connected, Vlan2 O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:01:47, Vlan1

18.5 Manipulate Routing Updates

This section describes direct route redistribution for different routing protocols. Methods for controlling routing information sent between different routing protocols include: using a distribution list, using a routing map, and modifying management distances.

18.5.1 Route IP List

18.5.1.1 Configure Access-List

Access lists are typically used to control user data flow, but access lists do not affect the data flow generated by the current router. There is an implicit deny any statement at the end.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration

		mode.
Step 2a	**ip access-list** *access list entry* <remark|permit|deny> <*A.B.C.D*	Define a standard access-list, ， access list entry can be filled with strings, including but not limited to numbers, English, some special characters,
	ip access-list *access list entry* <permit|deny> host *A.B.C.D*	<A.B.C.D.><wildcard_mask>define standard IP access based on source IP address or mask: Hosts define standard IP access based on a single source IP address;
	ip access-list *access list entry* <permit|deny> **any**	Any standard IP access based on any source IP address;
Step 2b	**ip access-list** *access list entry* <permit|deny>**ip** <*A.B.C.D*> <*wildcard_mask*> <*A.B.C.D wildcard_mask* | host *A.B.C.D* | any>	Define an extended access-list, access list entry can be filled with strings, including but not limited to numbers, English, some special characters,
	ip access-list *access list entry* <permit|deny> **host** *A.B.C.D*	<A.B.C.D.><wildcard_mask>defines extended IP access based on the source IP address or mask;
	ip access-list *access list entry* <permit|deny> **any**	Host defines extended IP access based on a single source IP address; Any extended IP access based on any source IP address;
	no ip access-list *access list entry*	Delete access-list
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show access-list**	Show access-list information

Step 5	**write**	Save configurations.

18.5.1.2 Configure Prefix List

Prefix lists are similar to access lists, and the benefits of prefix lists include improved performance when loading and finding large lists, incremental update support, and greater flexibility.Filtering through the prefix list requires matching the routing prefix to the prefix listed in the prefix list, just as matching the access list.When there is a match, use routing.

By default, serial Numbers are generated automatically and incremented by 5.If automatic sequence number generation is disabled, you must specify a sequence number for each entry.You do not need to specify a serial number when deleting a configuration item.

The Prefix-List is identified by the Prefix List name, which can contain multiple table items.Each table item, in the form of a network prefix, specifies a matching range independently and is identified by a sequence_num.Sequence_num indicates the order in which matching checks are performed in the Prefix-List.Each table item has a "or" relationship, and during the match, the route checks sequence_num in ascending order for each table item identified by sequence_num.As long as one of the table items satisfies the condition, this means that the Prefix-List filter (which does not enter the match of the next table item) is passed.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2a	**ip prefix-list** *Prefix list entry name* **seq** (1-4294967295) <permit|deny> *<A.B.C.D/M* | any>	Create a list of prefixes with optional serial Numbers to deny or allow access to matching conditions. The sequence_num range is 1-4294967295; The ge_value range is 0-32; The range of le_value is 0-32; Ge and le values specify the range of prefix lengths to match, and the specified ge values and values must satisfy: prefix_len<Ge_value<le_value<32。
Step 2b	**no ip prefix-list** *prefix_list_name*	Delete prefix-list
Step 3	**exit**	Return to privileged EXEC mode.

Step 4	**show ip prefix-list** [*prefix_list_name* | detail | summary]	Show ip prefix-list information.
Step 5	**write**	Save configurations.

To remove the prefix list and all its entries, use the commsnd **no IP prefix-list** prefix_list_name .

The keywords ge and le are optional and are used to specify the range of prefix lengths to match, which must satisfy the condition: length < ge-value < le-value <=32.

1. IP prefix-list 2 permit 2.2.2.2.0/24 /(match the first 24 bits: 2.2.*, mask must be 24 bits)

2. IP prefix-list 2 permit 2.2.2.2.2/24 ge 25 le 30 //(match the first 24 bits :2.2.2.*, mask must be 25-30 bits)

3. IP prefix-list 2 permit 2.2.2.2/24 le 32 /(match the first 24 bits :2.2.2.*, mask must be 24-32 bits)

4. IP prefix-list 2 permit 2.2.2.2.2/24 ge 26 /(match the first 24 bits :2.2.2.*, mask must be 26-32 bits)

5. IP prefix-list 3 permit 0.0.0.0.0.0/0 le 32 /(matches all)）

18.5.2 Route Redistribution

Redistribution refers to the ability of boundary routers connected to different routing selection domains to exchange and notify routing selection information between different routing selection domains (autonomous systems).Redistribution is always outward, and the router performing the redistribution does not modify its routing selection table.Router configuration command:**default-metric** is used to specify the seed metric values for all redistribution routes. Specify the seed metric values in a redistribute, for which you can use the option metric or routing mapping table.

Manage distance.When using routing redistribution, it may occasionally be necessary to modify the protocol's administrative distance to make it a priority.

Seed measurements.When routing redistribution occurs, metrics must be specified for the rerouting route.This measure, called the seed measure or default measure, is defined during the redistribution configuration.After specifying the seed measure for the redistribute route, the measure will increase normally within the autonomous system.The only exception is the OSPF E2 routing, which keeps the initial value regardless of how far it is propagated within the autonomic system.

Default seed measurements.RIP, IGRP, and EIGRP default to treat the seed metric value 0 as infinity.An infinite number of measurements indicate to the router that the reroute is unreachable and therefore should not be notified.Therefore, when rerouting the route to RIP, IGRP, and EIGRP, it is necessary to manually specify its seed measurement value, otherwise the rerouting route will not be notified.In OSPF, the

redistributed routing defaults to 2 classes (E2), with a measurement value of 20.Except for the redistributed BGP routing, which defaults to 2 classes and measures 1.
Redistribute technology.Bidirectional redistribute: redistribute all routes between two routing selection processes.One-way redistribution: a default route is passed to a routing selection protocol, and only the network that is known through the routing protocol is passed to the other routing selection protocols.
Passive interface: on OSPF routers, allocation of passive - interface is used to make a specific interface can't accept that sends hello packets, also cannot form a neighbor relationship, using scene: 1: make a specific router interface does not participate in the process of routing protocol 2: without any neighbor relationship was established through a particular interface at the same time, also can notice of these interfaces are routing.

18.5.2.1 RIP Route Redistribution

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router rip**	Start RIP and enter RIP configuration mode
Step 3	**distance** (1-255)	Set the administrative distance, default is 120.
Step 4	**default-metric** (1-16)	Default measurement
Step 5	**redistribute** <kernel|connected|static|ospf|babel|bgp|eigrp|isis|nhrp|openfabric|table|vnc> [{metric (0-16)|metric-type (1-2)|route-map *WORD*}]	Inter-protocol route redistribution, These include direct connection, kernel, ospf, babel routing protocol, border Gateway protocol, Enhanced Internal Gateway Routing Protocol, Intermediate system to intermediate system, kernel routing, Next Hop resolution protocol, openfabric Routing protocol, Open Shortest Path First, non-main kernel routing table, virtual network control, and rip Static route information. Let rip publish.

Step 6	**passive-interface** <default|vlan> [(1-4094)]	Configure the passive interface
Step 7	**offset-list** *access-list name* <**in**|**out**)> (0-16) [vlan (1-4094)]	Used to adjust measurements
Step 8	**exit**	Return to privileged EXEC mode.
Step 9	**show running-config**	Show running-config information

18.5.2.2 OSPF Route Redistribution

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router ospf**	Start ospf and enter ospf configuration mode
Step 3	**distance** (1-255)	Set the administrative distance, default is 110.
Step 4	**default-metric** (0-16777214)	Used to specify the seed metric values for all redistribution routes
Step 5	**redistribute** <kernel|connected|static|ospf|babel|bgp|eigrp|isis|nhrp|openfabric|table|vnc> [{metric (0-16)|metric-type (1-2)|route-map *WORD*}]	Inter-protocol route redistribution, These include direct connection, kernel, ospf, babel routing protocol, border Gateway protocol, Enhanced Internal Gateway Routing Protocol, Intermediate system to intermediate system, kernel routing, Next Hop resolution protocol, openfabric Routing protocol, Open Shortest Path First, non-main kernel routing table, virtual network control, and rip Static route information. Let rip publish.
Step 6	**passive-interface** <default|vlan> [(1-4094)]	Configure the passive interface
Step 7	**exit**	Return to privileged EXEC mode.

Step 8	**show running-config**	Show running-config information

Example:

Configuration	Result
switch c: router ospf router-id 3.3.3.3 network 192.168.2.3/24 area 1 redistribute connected metric 30(10) redistribute rip metric 30(10)	When configured with metric of 30 on switch c， On switch a：O E2 192.168.4.0/24 [110/30] via 192.168.2.3, 01:01:27,Vlan2 When configured with metric of 10 on switch c， On switch a：O E2 192.168.4.0/24 [110/10] via 192.168.2.3, 01:01:27, Vlan2

18.5.3 Distribution List Control Routing Updates

A distribute-list distribution list is a tool used to control routing updates, filtering only routing information, not LSA.Therefore, it is suitable for distance vector routing protocols, such as RIP and EIGRP.Like the OSPF link state routing protocol, the IN direction (which affects local routing tables but is present IN LSDB), the OUT direction does not work.But local originating routes can be filtered because of reroute routing, not LSA delivery.The distribute-list out command filters routing selection updates from outbound routing updates from the interface or specifies routing selection updates for routing selection protocols;The istribute-list in command filters routing selection updates coming in from the specified interface.

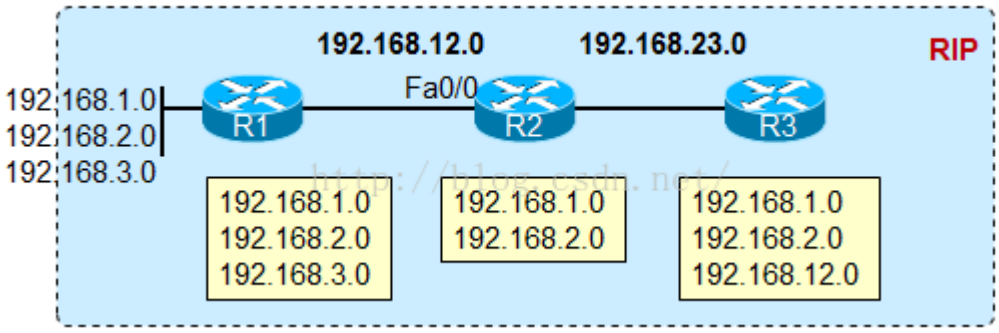
18.5.3.1 Distance Vector Routing Protocol RIP

Between routers, routing information is passed, and the distribution list has absolute control over routing information. Therefore, if it is in the direction, by deploying the distribution list, the specific route can be filtered, so that the local routing routing table of the distribution list is changed, and when the local router updates the routing information to the downstream router, the actually updated content is An entry that is affected by the distribution list.

At the same time in the out direction, there is no problem.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode..
Step 2	**router rip**	Start RIP and enter RIP configuration mode
Step 3	**distribute-list** *access-list name* <in|out> [*interface name*]	Filter routing using the access control list
Step 4	**distribute-list prefix** <in|out>[*interface name* |in [*interface name*] |out [*interface name*]]	Filter routing using prefix lists
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**show running-config**	Show running-config information

Configuration example 1 (in a single routing protocol environment-RIP)



Initially, R3 was able to learn the three loopback routes of R1, as well as the 192.168.12.0/24 routes.Now we don't want R3 to learn 192.168.3.0/24 routing, so we can configure R2 as follows:

R2(config)# access-list 1 deny 192.168.3.0

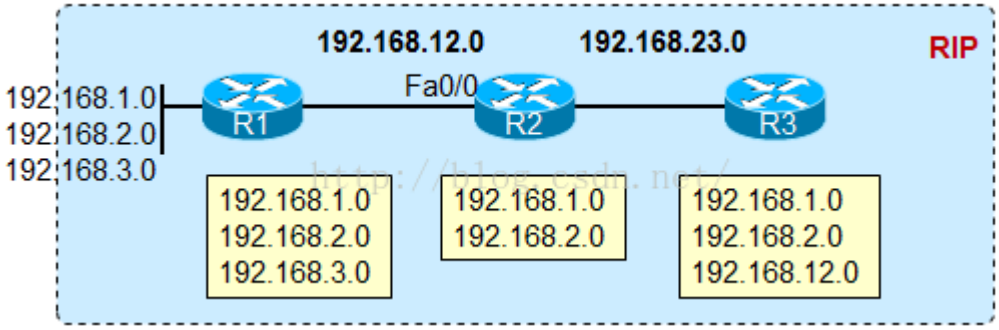
R2(config)# access-list 1 permit any

R2 (config) # router rip

R2(config-router)# redistribute -list 1 out ethv0.3

Of course, in - oriented distribution lists can have the same effect in R3.

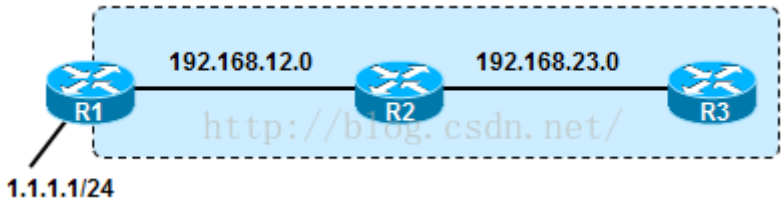
Configuration example 2 (in a single routing protocol environment-RIP)



In R2, if the following configuration is made:
R2(config)# access-list 1 deny 192.168.3.0
R2(config)# access-list 1 permit any
R2 (config) # router rip
R2(config-router)# redistribute -list 1 in ethv0.3
So, first of all, R2's own routing table will change, and 3.0's routing will be filtered out, and R3, the downstream RIP router, won't learn 3.0.

18.5.3.2 Link State Routing Protocol OSPF

Note that for a link-state routing protocol such as OSPF, the messages transmitted between routers are no longer routing information, but LSAs, and the distribution list cannot filter LSAs. Therefore, to deploy the distribution list in the link state protocol, you need to be aware of:
In the in direction, the distribution list can only filter the route when the LSA is received locally. When the route is generated, the router's own routing table that implements the distribution list will be affected by the distribution list (but the local LSDB still has the LSA), and The router still sends the LSAs in the LSADB to the neighbors. Therefore, the locally filtered routes and neighbors still exist.
In the outbound direction, the distribution list can only work on the ASBR that performs the route redistribution action, and can only work on externally imported routes. Because OSPF performs re-release, in fact, these external routes are introduced in the form of routes, so the distribution list can work normally in this case, but if it is not a local originating external route, or an internal OSPF route, out direction The distribution list is at a loss.



For example, redistribute directly into OSPF on R1, and use the outbound distribution list to filter out the 1.1.1.0 external route. However, R1 re-posts the incoming route. If the outbound distribution list on R2 attempts to block R3 from accepting the route or

LSA, it cannot, because this is not a locally originated external route.
OSPF distribution list command:

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode..
Step 2	**router ospf**	Start ospf and enter ospf configuration mode
Step 3	**distribute-list** *access-list name* **out** <kernel|connected|static|ospf|babel|bgp|eigrp|isis|nhrp|openfabric|rip|table|vnc>	Use the access control list for redistribution
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**show running-config**	Show running-config information

Configuration example 1--OSPF out directional distribution list in a single routing protocol environment

Distribution list, deployed in a link state routing protocol such as OSPF, can only be used if the out direction is used.
Pictured above, deployed on R1, R1 use redistribute direct way to introduce these three exterior routing and then out the direction of the distribution list, will be deployed on R1, and have effect on the three routing.
R1(config)# access-list 1 deny 192.168.3.0
R1(config)# access-list 1 permit any
R1 # router ospf (config)
R1 (config - the router) # redistribute connected subnets
R1(config-router)# network 192.168.12.1 255.255.255.0 area 0
R1 (config - the router) # distribute - list out 1
After the above configuration is implemented, R1 will filter out the 3.0 routing.
Configure example 2 -- deploy the distribution list when republished between protocols

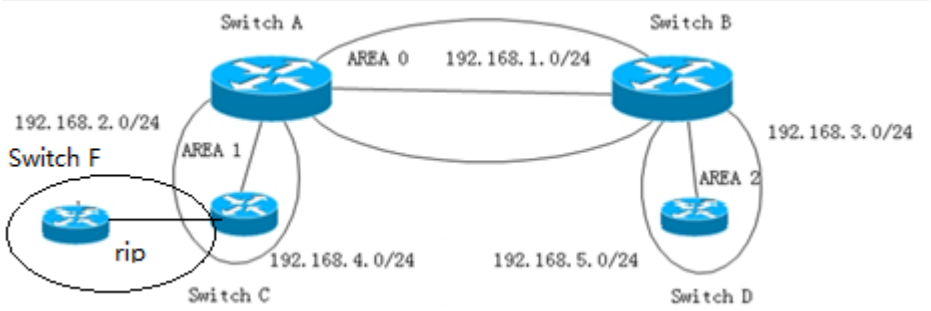
RIP redistributes into OSPF
Case 1
R2 is configured as follows:
Access - the list 1 permit 1.1.1.0
The router ospf
Redistribute rip metric 10 subnets
Distribute - list 1 out rip

What this command means here is that only 1.1.1.0 is allowed out of the reroute from the RIP routing protocol (to the OSPF protocol, there is no direction, as long as the interface running the OSPF)
In R3, there are only 1.1.1.0 routes

Case 2
Open loopback interface 2.2.2.2/24 on R2, R2 reissues RIP into OSPF and reissues direct access to OSPF
Access - the list 1 permit 1.1.1.0
The router ospf
Redistribute connected subnets
Redistribute rip metric 10 subnets
Network 192.168.23.0 0.0.255 area 0
Distribute - list out 1
// there are only 1.1.1.0 routes in R3, that is, the command redistribute -list 1 out here works for all routes injected from outside into the OSPF, and only 1.1.0 routes survive.The source of continuous routing is direct connection routing, or RIP.

Case 3
Open loopback interface 2.2.2.2/24 on R2, R2 reissues RIP into OSPF and reissues direct access to OSPF
Access - the list 1 permit 1.1.1.0
The router ospf
Redistribute connected subnets
Redistribute rip metric 10 subnets
Distribute - list 1 out rip
// R3 has routing in the routing table: 1.1.1.0, 2.2.0, 192.168.12.0
// that is, the routing other than 1.1.1.0 that was re-published from RIP was blocked and the local direct connection port was republished

Configuration example 3：



Configuration	Result
Configure switch c: ip access-list 1 deny 192.168.6.0 0.0.0.255 ip access-list 1 permit any router ospf ospf router-id 3.3.3.3 redistribute connected metric 30 redistribute rip metric 30 network 192.168.2.3/24 area 0.0.0.1 distribute-list 1 out rip	Result: Switch b: Unable to learn 192.168.6.0 segment of switch f; Learned 192.168.7.0 segment of switch f;

18.5.4 Routing Maps to Control Routing Updates

18.5.4.1 Configure Route Map

Route Map can be used for route redistribution and policy routing, and is often used in BGP. Policy routing is actually a complex static route. The static route is based on the destination address of the packet and forwarded to the specified next hop route. Policy routing can provide multiple types of filtering and classification.

The Switch can run multiple routing protocols simultaneously, which can redistribute information from one routing protocol to another. For example, you can instruct conversion to re-read IGRP-derived routes by using RIP or by re-reading static routes using IGRP. Reassigning information from one routing protocol to another applies to all supported IP-based routing protocols.

By defining a route map between two domains, it is possible to conditionally control the redistribution of routes between routing domains. Match and set the Route Map configuration command to define the conditional part of the roadmap. The Match command specifies that a standard must be matched; the Set command specifies the action that will be taken if the route update satisfies the conditions defined by the matching command. Although redistribution is a protocol-independent feature, some matching and setting Route Map configuration commands are specific to a particular protocol.

One or more matching commands and one or more Set commands follow a Route Map command. If there is no matching command, all match. If there is no command set, nothing is done except for the match. Therefore, you need at least one match or setup command.

Like the access list, there is an implicit deny any statement at the end of the route map. The result of this statement depends on the purpose of the route map.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**route-map** *route map tag*	Configure a route-map and

	<permit|deny|optimization> {(1-65535)}	enter the route-map configuration mode.
Step 3	**match ip address** *access_list_number*	Matching the specified access-list, the range of access_list_number is 1-2699, where 1-99 and 1300-1999 are standard access-list, and 100-199 and 2000-2699 are extended access-list.
Step 4	**match ip address prefix-list** *prefix_list_name*	Match the specified prefix-list.
Step 5	**match ip address prefix-len** (0-32)	Matches the specified prefix length.
Step 6	**match ip next-hop** *access_list_number*	Matching the next hop routing address through the specified access-list, the access_list_number range is 1-2699, where 1-99 and 1300-1999 are standard access-list, 100-199 and 2000-2699 are extended access-list.
Step 7	**match ip next-hop prefix-list** *prefix_list_name*	Match the next hop routing address through the specified prefix-list.
Step 8	**match ip next-hop prefix-len** (0-32)	Matches the length of the next hop route through the specified prefix list.
Step 9	**match ip next-hop address** *A.B.C.D*	The specified prefix list matches the ip address of the next hop route.

Step 10	**match ip next-hop type blackhole**	Type black hole that matches the next hop route through the specified prefix list.
Step 11	**match interface** *IFNAME*	Matches the route of the next outgoing interface as one of the specified interfaces
Step 12	**match metric** *metric_value*	Matches the metrics for the reroute routing, and metric_value ranges from 0-4294967295.
Step 13	**match tag** *tag_value*	Matches the tag for the redistributed routing.
Step 14	**match metric** (0-4294967295)	Set the metrics for the reroute routing, and metric_value ranges from 0-4294967295.
Step 15	**set metric-type** <type-1|typ2-2>	Sets the measurement value type for the redistributed routing.
Step 16	**set tag** tag_value	Sets the tag for the redistributed routing.
Step 17	**set ip next-hop** (<A.B.C.D>|peer-address|unchanged)	Specify the ip address of the next hop
Step 18	**exit**	Return to privileged EXEC mode.
Step 19	**exit**	Return enable node
Step 20	**show route-map**	Show route-map information
Step 21	**write**	Save configurations.

To delete a route-map entry, use the command **no route-map map_name**.Delete the match entry and use the command **no match**.Delete a set entry, using the command **no set**.

18.5.4.2 Link Status Routing Protocol OSPF

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.

Step 2	**router ospf**	Start ospf and enter ospf configuration mode
Step 3	**redistribute** <kernel|connected|static|ospf|babel|bgp|eigrp|isis|nhrp|openfabric|rip|table|vnc> [{ metric (0-16777214) | metric-type <1|2> |route-map *Pointer to route-map entries* }]	Redistribute direct connection, kernel, ospf protocol, babel Routing protocol, border Gateway Protocol, Enhanced Internal Gateway Routing Protocol, Intermediate System to intermediate system, kernel routing, Next Hop Resolution protocol, openfabric Routing Protocol, Routing Information Protocol, Open Shortest Path First, non-main kernel routing table, Virtual Network Control, to The static route information of rip is reassigned to rip.Get the ospf protocol out there.
Step 4	**exit**	Return to global configuration mode.
Step 5	**show running-config**	Show running-config information

For example

Configuration	Result
switch c: ip access-list 1 permit 192.168.6.0 0.0.0.255 ip access-list 2 permit 192.168.7.0 0.0.0.255 ip prefix-list 1 seq 5 permit 192.168.6.0/24 ip prefix-list 2 seq 5 permit	1）switch c execute：redistribute rip route-map test1 Switch b result ========== OSPF external routing table ========== N E1 192.168.6.0/24 [302] tag: 0 via

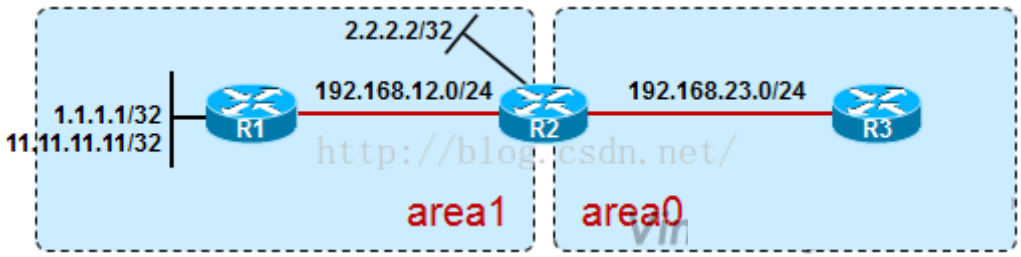
192.168.7.0/24 route-map test1 permit 10 match ip address 1 set metric 300 set metric-type type-1 ! route-map test1 permit 30 match ip address 2 set metric 500 ! route-map test2 permit 20 match ip address 2 set metric 500 ! route-map test3 permit 40 match ip address prefix-list 1 set metric 400 ! route-map test3 permit 50 match ip address prefix-list 2 set metric 600 !	192.168.1.1, ethv0.1 N E2 192.168.7.0/24 [2/500] tag: 0 via 192.168.1.1, ethv0.1 2）switch c execute：redistribute rip route-map test2 switch b result N E2 192.168.7.0/24 [2/500] tag: 0 via 192.168.1.1, ethv0.1 3）switch c execute：redistribute rip route-map test3 switch b result N E2 192.168.6.0/24 [2/400] tag: 0 via 192.168.1.1, ethv0.1 N E2 192.168.7.0/24 [2/600] tag: 0 via 192.168.1.1, ethv0.1

18.5.5 Prefix Lists to Filter Routing

Methods of OSPF filtering LSA: area filter-list prefix; **only those three types of LSA produced from the ABR can be filtered.**

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router ospf**	Enter the OSPF configuration mode.
Step 3	**area** < (0-4294967295) | A.B.C.D > **filter-list prefix** *Name of an IP prefix-list* <in|out>	Configure the list of prefixes within the region.
Step 4	**exit**	Return to privileged EXEC mode.

Filter three types of LSA on ABR.



By default, R3 can learn the inter-area routes of 1.1.1.1, 11.11.11.11, 2.2.2.2, and 192.168.12.0.These routes are calculated by R3, which collects and calculates "three LSA classes injected from R2 into area0".So what if we don't want R3 to learn the 11.11.11.11/32 route?

```
ip prefix-list 100 deny 11.11.11.11/32
ip prefix-list 100 permit 0.0.0.0/0 le 32
!
router ospf
 area 0 filter-list prefix 100 in
```

The above command means that the prefix list filter is executed when three classes of LSA are injected from other regions into the area0 region.If it's area1 filter-list prefix 100 out, this command means to perform the prefix filter when injecting 3 classes of LSA from area1 into all other areas.

Note that when we deploy on ABR filtering scheme of this three kinds of LSA, able to filter only those generated from the three kinds of ABR LSA, above area0 by default in the flood of 1.1.1.1, 11.11.11.11, 2.2.2.2, 192.168.12.0 routing of these three kind of LSA are produced from R2, so can be filtered by prefix list.

.

19. IPv6

19.1 VLAN IPv6 Address

Start from privileged configuration mode, configure or delete IPv6 address and prefix of VLAN as the following table shows.

	Command	Function
Step 1	**config terminal**	Enter global configuration mode.
Step 2	**interface vlan** (1-4094)	enter VLAN interface configuration *vlan_id* range:1~4094
Step 3a	**ipv6 address** *X:X::X:X/M[eui-64]*	Configure the IPv6 address and prefix length of the vlan interface. By default, the interface automatically generates a link-local address. **Eui-64**, which is an optional parameter, is used to automatically fill the low 64-bit of IPv6 address according to the eui-64 specification.
	ipv6 address *X:X::X:X* ***link-local***	Configure the IPv6 link-local address of the vlan interface.
Step 3b	**no ipv6 address** *X:X::X:X/M*	Delete specified IPv6 address of VLAN interface.
	no ipv6 address	Delete all IPv6 addresses of the VLAN interface.
	no ipv6 address *X:X::X:X* ***link-local***	Restore the default link-local address of VLAN interface.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show interface vlan** (1-4094)	Verify the configuration information.
Step 6	**write**	Save configurations.

19.2 IPv6 Static Neighbour

The neighbor items are the neighbor information of the device in the link range. The device neighbor items can be created dynamically through the neighbor request message NS and the neighbor advertisement message NA; it also can be created manually.
The device identifies a static neighbor item uniquely based on the IPv6 address of the neighboring node and the interface number that connected to the neighboring node.
When you delete a static neighbor item corresponding to a VLAN interface, you only need to specify the VLAN interface.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 neighbor** *X:X::X:X* **vlan** (1-4094) *HHHH: HHHH:HHHH*	Add a static item to the neighbor discovery table, you must specify the network interface and link layer address.
Setp 3	**no ipv6 neighbor** *X:X::X:X* **vlan** (1-4094)	Delete the specified item of the neighbor discovery table.
Step 4	**show ipv6 neighbors**	Show the neighbor items in the current neighbor discovery table.

19.3 IPv6 SLAAC

An IPv6 address consists of two parts: prefix and interface ID. A big feature of IPv6 is that it supports plug and play. IPv6 address stateless auto-configuration means that the node configures an IPv6 address automatically based on the information assigned by the router discovery/prefix discovery. Router discovery/prefix discovery means that when a node is connected to an IPv6 link, it can discover the local router, obtain the neighbor router information and the prefix of the network, and other configuration parameters from the received RA message but not by Dynamic Host Configuration Protocol (DHCPv6).
The device can obtain the IPv6 address prefix which carried in the RA message (Router-Advertisement, ICMPv6 Type 134), and generate the interface ID automatically through the interface, so as to get a completed 128-bit IPv6 address. By default, the RA message is sent once every 600s. The device can also send an RS (router solicit, ICMPv6 Type = 133) message to obtain the prefix.
Parameter Discovery: A node can discover the parameters of the link it is connected to, such as the MTU of the link and the hop limit.

19.3.1 IPv6 SLAAC Work Processes

The router discovery/prefix discovery is implemented by router solicitation message RS and router advertisement message RA. The specific process is as follows:
(1) When the node starts up, it sends a request to the router through RS message, requesting the prefix and other configuration information for the configuration of the node.
(2) The router responds a RA message, which includes the prefix information option (the router also sends the RA message periodically). The prefix information option includes not only the prefix information of IPv6 address but also the preferred lifetime and valid lifetime of the prefix. After receiving the periodical RA message, the node will update the preferred lifetime and valid lifetime of the prefix based on the message.
(3) The node configures IPv6 address and other information of the interface automatically by using the prefix and other configuration parameters in the RA message responded by the router. During the valid lifetime, the automatically generated address can be used normally; after the valid lifetime expired, the automatically generated address will be deleted.

19.3.2 IPv6 SLAAC Configuration

Start from privileged configuration mode, configure or delete IPv6 address and prefix of VLAN as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** (1-4094)	Enter VLAN interface configuration. *vlan_id* range: 1-4094.
Step 3	**no ipv6 nd suppress-ra**	Disable RA message suppression. The interface sends RA messages periodically (default 600S). By default, RA message suppression is enabled.
	ipv6 nd suppress-ra	Enable RA message suppression.
Setp 4a	**ipv6 nd ra-interval** (1-1800)	Configure the interval for sending RA messages in second. The minimum value is 1s and the maximum value is 1800s. The default is 600s.

Step 4b	**ipv6 nd ra-interval msec** (70-1800000)	Configure the interval for sending RA messages in millisecond. The minimum value is 70ms and the maximum value is 1800000ms. The default is 600000ms.
Step 5	**ipv6 nd ra-lifetime** (*0-9000*)	Configure the lifetime of the RA message. The minimum value is 0s and the maximum value is 9000s. The default is 1800s.
Step 6	**ipv6 nd reachable-time** (1-3600000)	Specify the reachability interval of a new neighbor. It is used to detect neighbors that are unreachable in the neighbor discovery table. The minimum value is 1s and the maximum value is 3600000s. The default is 0s.
Step 7	**ipv6 nd home-agent-config-flag**	The set/unset flag in IPv6 router advertisement message is used to indicate to the host that the router acts as a home agent and includes the home agent option. It is not set by default.
Step 8	**ipv6 nd home-agent-preference** (0-65535)	When the local proxy configuration flag is set, this value indicates the host proxy preference. The default value 0 indicates the lowest priority.
Step 9	**ipv6 nd home-agent-lifetime** (0-65520)	When the local proxy configuration flag is set, this value indicates the host agent lifetime. The default value is 0.
Step 10	**ipv6 nd adv-interval-option**	Advertisement Interval option indicates the maximum time (in milliseconds) between consecutive unsolicited router advertisements.
Step 11	**ipv6 nd managed-config-flag**	This flag bit indicates which automatic configuration mode is used to obtain the IPv6 address. When the M bit is set to 1, the device that received this RA message will use the configuration protocol (such as DHCPv6) to obtain an IPv6 address. By default, this flag bit is 0.
Step 12	**ipv6 nd other-config-flag**	This flag bit indicates which mode is used to configure other configuration information (such as DNS, domain name, etc.) except IPv6 address. When the O bit is set to 1, the device that received this RA message will use the configuration protocol (such as

		DHCPv6) to obtain configuration information except IPv6 address. By default, this flag bit is 0.
Step 13	**ipv6 nd prefix** *X:X::X:X/M* [< (0-4294967295) | off-link | infinite | no-autoconfig | router-address >]	Configure the parameters of the prefix declared on the network interface; **Valid-lifetime:** The length of time (in seconds) that the prefix is valid. The value *infinite* means infinity. Range: <0-4294967295| infinite> Default: 2592000 **Preferred-lifetime:** The preferred length of time (in seconds) for the prefix. Range: <0-4294967295| infinite> Default: 604800 **off-link:** Indicates that the link or link attribute does not declare a prefix. **no-autoconfig**: Indicates to the device on the link that the specified prefix cannot be used for IPv6 autoconfiguration. **router-address**: The R flag indicates to the host on the local link that the specified prefix contains the full IPv6 address.
Step 14	**ipv6 nd router-preference** < high|medium|low >	Set router preferences.
Step 15	**ipv6 nd mtu** (1-65535)	Configure the interface MTU. MTU range: 1-65535. The default is 0.

19.4 DHCPv6

19.4.1 DHCPv6 Overview

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) is a protocol designed for IPv6 addressing schemes that assigns IPv6 prefixes, IPv6 addresses, and other network configuration parameters to hosts.

Compared with other IPv6 address allocation methods (manual configuration, stateless autoconfiguration through network prefix in router advertisement messages, etc.), DHCPv6 has the following advantages:

- Not only IPv6 addresses, but also IPv6 prefixes can be assigned to facilitate automatic configuration and management of the whole network.
- Better control of address allocation. Not only can DHCPv6 record the address/prefix assigned to the host, but it can also assign a specific address/prefix

to a specific host for network management.

- In addition to the IPv6 prefix and IPv6 address, it can also assign network configuration parameters such as DNS server and domain name to the host.

19.4.1.1 DHCPv6 Network Composition

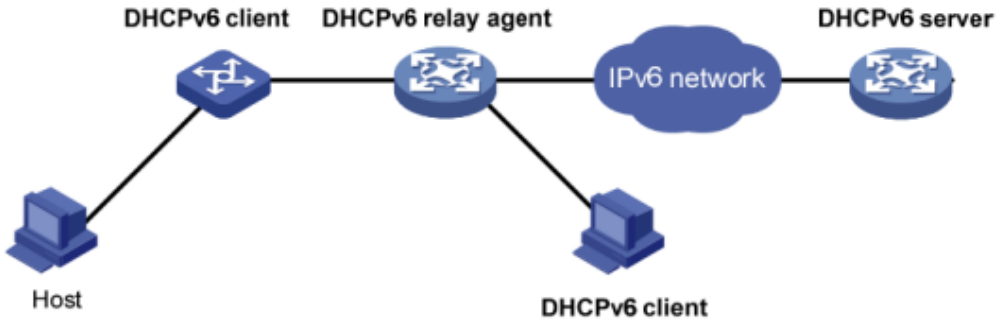


Figure 1：DHCPv6 network Composition

As shown in figure 1, the DHCPv6 networking includes the following three roles:

DHCPv6 client: A device that dynamically obtains IPv6 addresses, IPv6 prefixes, or other network configuration parameters.

DHCPv6 server: A device responsible for assigning IPv6 addresses, IPv6 prefixes, and other network configuration parameters to DHCPv6 clients. A DHCPv6 server can not only assign an IPv6 address to a DHCPv6 client, but also assign an IPv6 prefix to it. As shown in figure 1, after the DHCPv6 server assigns an IPv6 prefix to the DHCPv6 client, the DHCPv6 client sends an RA message containing the prefix information to the network, so that hosts on the network automatically configure an IPv6 address based on the prefix.

DHCPv6 relay: The DHCPv6 client communicates with the DHCPv6 server through the link-local multicast address to obtain IPv6 addresses and other network configuration parameters. If the server and the client are not on the same link, you need to forward packets through the DHCPv6 relay. This prevents the DHCPv6 server from being deployed on each link. This saves costs and facilitates centralized management.

19.4.1.2 DHCPv6 DUID Configuration

The server uses the DUID (DHCP Unique Identifier) to identify different clients, and the client uses the DUID to identify the server. The contents of the client and server DUID are carried in the Client Identifier and Server Identifier options in the DHCPv6 message. The format of the two options is the same. The value of the option-code field is used to distinguish between the Client Identifier and the Server Identifier option.

The minimum length is 12 bytes (96 bits) and the maximum length is 20 bytes (160 bits). The actual length depends on its type. The server compares the DUID to its database and sends the configuration data (address, lease, DNS server, etc.) to the client

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**duid** <duid-llt|duid-ll|duid-en> (1-2147483647) identifier *Identifier string*	Configure DUID.
Step 3	**show ipv6 dhcp duid**	Display DUID configuration.
Setp 4	**write**	Save configuration.

19.4.2 DHCPv6 Server

19.4.2.1 DHCPv6 Address/Prefix Allocation Process

The process of assigning addresses/prefixes to clients by the DHCPv6 server is divided into two categories:

- Quickly allocation process with two messages exchanging.
- Allocation process with four messages exchanging.

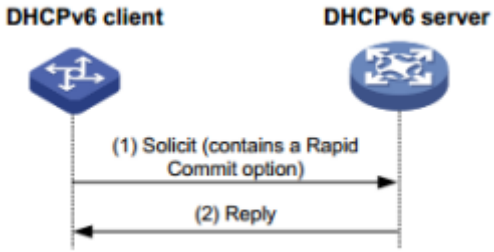


Figure 2：Quickly allocation process with two messages exchanging

As shown in figure 2, the address/prefix quick assignment process is:

(1) The DHCPv6 client carries the Rapid Commit option in the sent Solicit message, indicating that the client wants the server to quickly assign an address/prefix and network configuration parameters to it;

(2) If the DHCPv6 server supports the fast allocation process, it directly returns a Reply message to assign the IPv6 address/prefix and other network configuration parameters to the client. If the DHCPv6 server does not support the fast assignment process, the client is assigned an IPv6 address/prefix and other network configuration parameters using an assignment process that interacts with four messages.

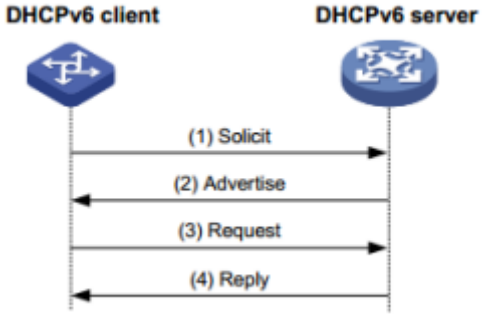


Figure 3：Allocation process with four messages exchanging

Step	Message type	Description
(1)	Solicit	The DHCPv6 client sends the message requesting the DHCPv6 server to assign an IPv6 address/prefix and network configuration parameters to it.
(2)	Advertise	If the Rapid Commit option is not carried in the Solicit message, or the Rapid Commit option is carried in the Solicit message, but the server does not support the fast allocation process, the DHCPv6 server replies to the message, notifying the client of the address/prefix and network configuration parameters that can be assigned to it.
(3)	Request	If the DHCPv6 client receives Advertise messages from multiple servers, it selects one of the servers according to the order in which the messages are received, the server priority, etc., and sends a Request message to the server, requesting the server to confirm the address/prefix. And network configuration parameters
(4)	Reply	The DHCPv6 server replies to the message, confirming that the address/prefix and network configuration parameters are assigned to the client.

19.4.2.2 DHCPv6 Server Lease Renewal Process

The IPv6 address/prefix assigned to the client by the DHCPv6 server has a certain lease term. The rental period is determined by the valid life period (Valid Lifetime). After the lease time of the address/prefix reaches the valid lifetime, the DHCPv6 client can no longer use the address/prefix. If the DHCPv6 client wishes to continue using the address/prefix before the valid lifetime expires, the address/prefix lease needs to be updated.

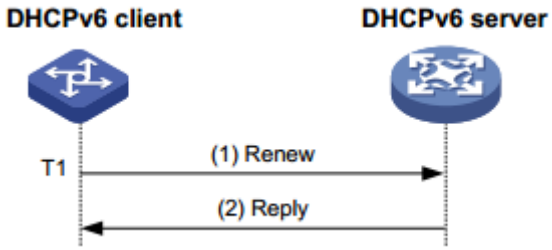


Figure 4：Update address/prefix lease by renew

As shown in Figure 4, when the address/prefix lease time arrival time T1 (the recommended value is half of the preferred lifetime Preferred Lifetime), the DHCPv6 client unicasts the Renew message to the DHCPv6 server that assigns the address/prefix to it. Update the address/prefix lease. If the client can continue to use the address/prefix, the DHCPv6 server responds with a successful Reply packet, informing the DHCPv6 client that the address/prefix lease has been successfully updated; if the address/prefix cannot be reassigned to the client, The DHCPv6 server responds with a Reply packet that failed to renew, notifying the client that it cannot obtain a new lease

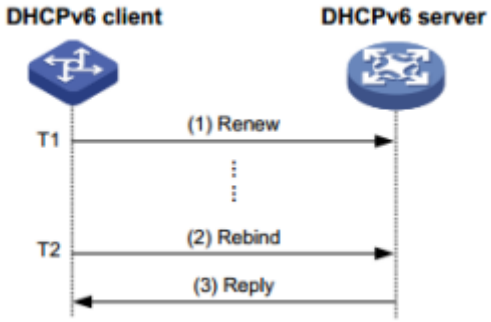


Figure 5：Update address/prefix lease by rebind

As shown in Figure 5, if Renew is sent to update the lease at T1, but the response packet from the DHCPv6 server is not received, the DHCPv6 client will send all DHCPv6 to T2 (recommended value is 0.8 times of the preferred lifetime). The server multicasts the Rebind message and requests to update the lease. If the client can continue to use the address/prefix, the DHCPv6 server responds with a successful Reply message, informing the DHCPv6 client that the address/prefix lease has been successfully updated; if the address/prefix cannot be reassigned to the client, The DHCPv6 server responds to the Reply packet with the renewal failure, notifying the client that the new lease cannot be obtained. If the DHCPv6 client does not receive the response packet from the server, the client stops using the address/prefix after the valid lifetime expires.

19.4.2.3 DHCPv6 Server Stateless Configuration

The DHCPv6 server can assign additional network configuration parameters to clients that already have an IPv6 address/prefix. This process is called a DHCPv6 stateless configuration.

After the DHCPv6 client successfully obtains an IPv6 address through the stateless

auto-configuration function, the M flag (Managed address configuration flag) in the RA (Router Advertisement, Router Advertisement) packet is 0. If the other stateful configuration flag (1), the DHCPv6 client automatically starts the DHCPv6 stateless configuration function to obtain other network configuration parameters except the address/prefix.

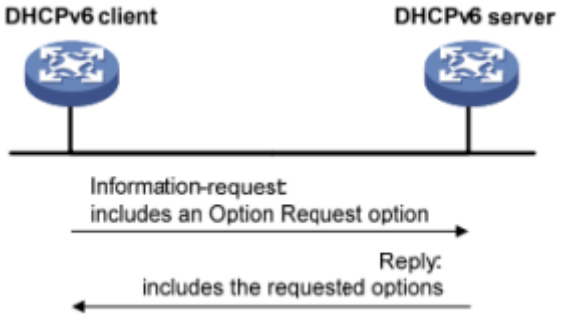


Figure 6：DHCPv6 stateless configuration process

As shown in Figure 6, the specific process of DHCPv6 stateless configuration is as follows:

(1) The client sends an Information-request packet to the DHCPv6 server in multicast mode. The packet carries the Option Request option to specify the configuration parameters that the client needs to obtain from the server.

(2) After receiving the Information-request packet, the server allocates network configuration parameters to the client and sends a Reply packet to the client to return the network configuration parameters to the client.

(3) The client provides the information provided in the Reply packet. If the configuration parameter is the same as the one specified in the Reply message, the network configuration is performed according to the parameters provided in the Reply packet. Otherwise, the parameter is ignored. If multiple Reply packets are received, the client selects the first reply packet and completes the stateless configuration of the client according to the parameters provided in the packet.

19.4.2.4 DHCPv6 Server Configurations

Start from privileged configuration mode, configure DHCPv6 server as the following table shows.

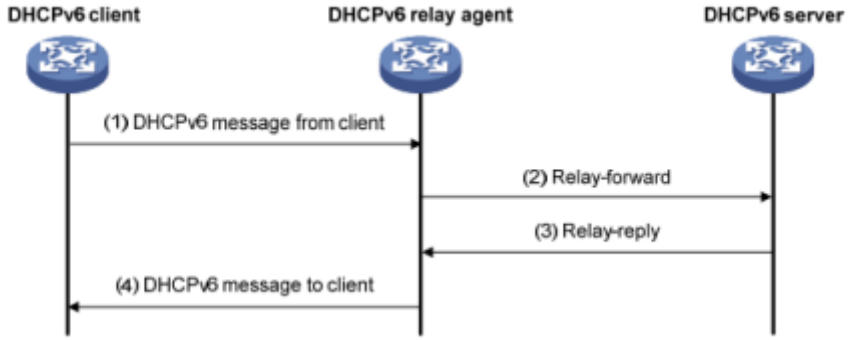
	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 dhcp pool** *DHCP pool name*	Configure an IPv6 DHCP address pool.
Step 3	**prefix-delegation** *X:X::X:X/M* [< *X:X::X:X/M*| lifetime < (60-4294967295)|infinite> < (60-4294967295)|infinite>]	Configure prefix delegation and its lifetime.

Setp 4	**address** *X:X::X:X/M X:X::X:X/M* [lifetime < (60-4294967295)|infinite> < (60-4294967295)|infinite>]	Configure IPv6 address prdfix and its lifetime.
Step 5	**dns-sever** *X:X::X:X*	Configure the DNS server IPv6 address.
Step 6	**domain-name** *A domain name*	Configure domain name.
Step 7	**interface vlan** (1-4094)	Add VLAN and enter VLAN interface configuration. vlan_id(1－4094)；
Step 8	**ipv6 dhcp server** *Name of IPv6 DHCP pool* [<preference (0-255) |<allow-hint | rapid-commit> >]	Configure and enable the DHCPv6 server address of the network segment on the interface.
Step 9	**exit**	Exit to global configuration mode.
Step 10	**show ipv6 dhcp pool**	View DHCPv6 address pool information..
Step 11	**show ipv6 dhcp interface vlan** (1-4094)	Show information about the device DHCPv6 interface
Step 12	**write**	Add VLAN and enter VLAN interface configuration. vlan_id(1－4094)；

19.4.3 DHCPv6 Relay

19.4.3.1 DHCPv6 Relay Work Processes

During the process of obtaining the IPv6 address/prefix and other network configuration parameters dynamically through the DHCPv6 relay, the DHCPv6 client and the DHCPv6 server are processed in the same way as when the DHCPv6 relay is not processed.
DHCPv6 relay forwarding process：



(1) The DHCPv6 client sends a request to the multicast address FF02::1:2 of all DHCPv6 servers and relays;

(2) After receiving the request, the DHCPv6 relay encapsulates the relay-forward packet in the relay message option and sends the relay-forward packet to the DHCPv6 server.

(3) The DHCPv6 server parses the client's request from the relay-forward packet, selects the IPv6 address and other parameters for the client, constructs a response message, and encapsulates the response message in the relay message option of the Relay-reply message. Send the Relay-reply message to the DHCPv6 relay.

(4) The DHCPv6 relay resolves the response from the server to the DHCPv6 client from the relay-reply packet. The DHCPv6 client performs network configuration based on the IPv6 address/prefix and other parameters assigned by the DHCPv6 server.

19.4.3.2 DHCPv6 Relay Configuration

Start from privileged configuration mode, configure DHCPv6 relay as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** (1-4094)	Add VLAN and enter VLAN interface configuration *vlan_id(*1-4094);
Step 3	**ipv6 dhcp relay destination** *X:X::X:X*	Configure the DHCPv6 relay server address on the network segment of the interface and enable the DHCPv6 relay service.
Setp 4	**exit**	Exit to global configuration mode.
Step 5	**show ipv6 dhcp interface**	Show information about the device DHCPv6 interface.
Step 6	**write**	Save configurations.

19.4.3.3 DHCPv6 Relay Option 37 Configuration

Start from privileged configuration mode, configure DHCPv6 relay option 37 as the following table shows.

Step 1	**configure terminal**	Enter global configuration mode.
	ipv6 dhcp relay remote-id option	Enable relay support option 38 option function
Step 2	**interface vlan** (1-4094)	Add VLAN and enter VLAN interface configuration.vlan_id(1-4094);
Step 3	**ipv6 dhcp relay remote-id** *remote id*	Configure the remote-id value of the custom option37.
Step 4	**exit**	Exit to global configuration mode.
Step 5	**show ipv6 dhcp relay option**	Display configuration information about trunk related options.
Step 6	**write**	Save configurations.

19.4.3.4 DHCPv6 Relay Option 38 Configuration

Start from privileged configuration mode, configure DHCPv6 relay option 38 as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
	ipv6 dhcp relay subscriber-id option	Enable relay support option 38 option function
Step 2	**interface vlan** (1-4094)	Add VLAN and enter VLAN interface configuration.vlan_id(1-4094);
Step 3	**ipv6 dhcp relay subscriber-id** *subscriber id*	Configure the custom subscriber-id value of option38.
Step 4	**exit**	Exit to global configuration

		mode.
Step 5	**show ipv6 dhcp relay option**	Display configuration information about trunk related options.
Step 6	**write**	Save configurations.

19.5 IPv6 Route

19.5.1 IPv6 Static Route Configuration

IPv6 Static Routes Introduction

A static route is a special type of route that is manually configured by an administrator. When the network structure is relatively simple, you only need to configure a static route to make the network work normally. Static routes cannot automatically adapt to changes in network topology. After the network fails or the topology changes, the configuration must be manually modified by the network administrator. IPv6 static routes are similar to IPv4 static routes and are suitable for some IPv6 networks with simple structures.

Default Routes Introduction

The IPv6 default route is the route used when the router does not find a matching IPv6 routing entry. There are two ways to generate IPv6 default routes:

- The first type is manually configured by the network administrator. The function address specified during configuration is ::/0 (prefix length is 0).
- The second type is dynamic routing protocol generation (such as OSPFv3, IPv6 IS-IS, and RIPng). Routers with strong routing capabilities advertise IPv6 default routes to other routers. Other routers generate pointers to them in their routing tables. The default route of the router.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 route** *X:X::X:X/M X:X::X:X*	Add a static route.
Step 3	**no ipv6 route** *X:X::X:X/M X:X::X:X*	Delete static route.
Step 4	**show ipv6 route**	Show current routing configuration

19.5.2 View IPv6 Hardware Routing Information

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration

		mode.
Step 2a	**show ipv6 route subnet-route**	View IPv6 hardware subnet routing information
Step 2b	**show ipv6 route host-route**	View the routing information about the IPv6 hardware host

19.6 IPv6 Connectivity Test

Ping IPv6 is mainly used to check network connectivity and host reachability for IPv6.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**Ping ipv6** *<X:X::X:X>* [-i *vlan <1-4094>*] [-s <*packetsize*>]	Packetize: The length of the packet to be sent, in bytes. Ping the link local address to specify the interface.

20. PON Management

20.1 Show PON Port Info and Optical Power

20.1.1 Show PON Port Info

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON interface configuration mode.
Step 3	**show pon statistics**	Enter PON interface configuration mode.

20.1.2 Show PON Port Optical Power

Optical module parameters contain transmit optical power, receive optical power, temperature, voltage and bias current. These 5 parameters decide whether the optical module can work normal or not. Any of them is abnormal may cause ONU deregister or lose packets.
Start from privileged configuration mode, show PON port optical module parameters as the following table shows.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON interface configuration mode.
Step 3	**show pon optical transceiver**	Show pon optical parameters.

20.1.3 Show ONU Optical Transceiver

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.

Step 2	**interface gpon** *slot/port*	Enter PON interface configuration mode.
Step 3	**show onu** [(1-256)|all] **rx-power**	Show ONU optical transceiver

20.1.4 Display the Manufacturer Information

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show idprom interface** <gpon|gigabitEthernet> <S/P> [<vendor|manufacture>]	Display PON port Optical module manufacturer information

20.2 PON Port Configuration

20.2.1 Enable/Disable PON

Start from privileged configuration mode, enable or disable PON port as the following table shows.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON interface configuration mode.
Step 3a	**shutdown**	Disable pon port
Step 3b	**no shutdown**	Enable pon port

20.2.2 Configure the P2P Function

Start from the privileged configuration mode, enable or disable the PON port P2P function, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show p2p**	Show PON port P2P

		configuration
Step 3	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 4	**p2p** <enable|disable>	Enable/disable P2P function
Step 5	**show p2p**	Show This parameter specifies the P2P configuration of the PON port

20.2.3 Configure PON Port Range

Start from the privileged configuration mode, configure the PON port Range function, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**show pon range**	Show PON port registration distance configuration
Step 3	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 4	**range min** (0-599) **max** (1-600)	Configure PON Minimum and maximum registered distance of a PON port
Step 5	**no range min** (0-599) **max** (1-600)	Delect Minimum and maximum registered distance of a PON port
Step 6	**show pon range**	Show The registered distance of the current PON port is specified

20.2.4 Display PON Protection Information

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**pon-protection**	Enter PON Protection configuration mode
Step 3	**show pon-protection group all**	Show Information about all PON protected groups of the device
Step 4	**show pon-protection group name** *string*	Displays protected group information based on the protected group name.

20.2.5 Configure PON Protected Groups

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**pon-protection**	Enter PON Protection configuration mode
Step 3	**pon-protection group name** *string* **master-pon** (1-8) **slave-pon** (1-8) **local** [*type-c*]	set Single-owning PON protected groups
Step 4	**pon-protection group name** *string* **master-pon** (1-8) **slave-pon** (1-8) **local-ip** *A.B.C.D* **remote-ip** *A.B.C.D* [*type-c*]	Set a dual-homing PON protected group
Step 4	**no pon-protection group name** *string*	Delete a PON protected group by its name
Step 5	**pon-protection group name** *string* **auto-sync** <enable|disable> **time** (60-3600)	Set the port synchronization time of the protected group
Step 6	**pon-protection group name** *string* <lock|unlock>	Set the lock mode for a protected port. After lock is enabled, the working port of a protected group does not switch over
Step 7	**pon-protection group name** *string* **revertive** <enable|disable> **time** (60-3600)	Set Port switchover time of a protected group
Step 8	**pon-protection group name** *string* **switchover**	Manually change the working port of the protected group
Step 9	**pon-protection group name** *string* **sync-config**	Manually synchronize port configurations of protected groups

21. ONU management

21.1 ONU Basic Configuration

21.1.1 Display Auto-find ONU

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show onu auto-find**	Display auto-find ONU
Step 4	**show onu auto-find aging-time**	Display auto-find indicates the aging time of the ONU

21.1.2 ONU Automatic Authorization

OLT enable/disable automatic authorization mode. When the ONU is online, the ONU will automatically authorize the ONU.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show onu auto-learn**	Display auto-learn

21.1.3 Display ONU Authorization Information

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show onu** < (1-256)|all > **info**	Diaplay authorization message

21.1.4 Display ONU Authorization Details

It can display ONU vendor ID, version, serial number, product code...

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show onu detail-info** <(1-256)|all >	Displays onu details or can select ranges

21.1.5 Activate/deactivate the ONU

When you activate/deactivate the ONU, the ONU goes online/offline

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** <(1-256)|all > <activate|deactivate>	Activate/disable the ONU on the PON port

21.1.6 ONU Authorization

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu add** (1-256) **profile** *onu_profile_name <loid+pw|loid|sn>*	Authorization ONU

21.1.7 Configure ONU Description

	Command	Function
Step 1	**configure terminal**	Enter global configuration

		mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**onu** <(1-256)|all> **desc** *description*	ONU add description string
Step 4	**show onu desc** <(1-256)|all>	Display ONU description

21.1.8 Configure ONU Whitelist

Whitelist To enable ONU authentication. Supports filtering based on the source SN and Vendor ID.
Start from the privileged configuration mode, configure the onu whitelist function of the device, as shown in the following table:

	Command	Function
Step 1a	**onu allowlist sn-auth** *sn_string*	Whitelist based on Vendor ID. The value is a four-digit string
Step 1b	**no onu allowlist sn-auth** *sn_string*	Delete the whitelist based on the Vendor ID
Step 2a	**onu allowlist** sn-auth *sn_string* [*sn_end_string*]	Whitelist based on SN. The value is a 12-digit string. You can set only the start SN or the range SN (start SN and end SN).
Step 2b	**no onu allowlist sn-auth** [*sn_string*|*sn_end_string*]	Delete the SN whitelist

21.1.9 Display ONU Statistics

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON port
Step 3	**show onu statistics all**	Display ONU send and receive data messages

21.1.10 Configure Plug and play

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**plug_and_play vlan** (1-4094)	Configure ONU plug and play and VLAN
Step 3	**interface gpon** *slot/port*	Enter PON port
Step 4	**plug-and-play disable**	Disable the ONU plug and play function

21.1.11 Configure ONU Delete Automatically

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**onu auto-delete**	Enable ONU automatic deletion function
Step 3	**onu auto-delete timeout** (5-44640)	Set Time when the ONU is automatically deleted
Step 4	**onu auto-delete timeout default**	Restores the default time when the ONU is automatically deleted
Step 5	**show onu auto-delete**	Display ONU auto-delete configuration

21.2 ONU Remote Configuration

21.2.1 Display ONU SFP Information

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show onu optical-info** <(1-256)|all>	Display onu SFP information

21.2.2 Upgrade the ONU

The ONU can only be upgraded if the ONU has authorization on the OLT.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**upgrade load tftp image** *filename A.B.C.D*	Configure the ONU firmware name and TFTP server
Step 3	**upgrade select pon** *slot/port* [*onuid_list*]	Select ONU
Step 4	**upgrade start** <activate|commit|download|mix|quick-acitve>	Download the ONU firmware and save it in memory, then update the ONU
Step 5	**upgrade stop**	Delete firmware from memory and delete the upgrade program information
Step 6	**show upgrade** <status|info| onu-version|onu-firmware> [*slot/port onu_list*]	Displays gpon upgrade status, upgrade information, and firmware information

attention：

1. Do not turn off the power when updating. When the update is complete, the OLT notifies the ONU that the update was successful and resets the ONU with the new firmware.
2. After the ONU update restarts, the OLT sends the commit command to confirm the new version.
3. Run the upgrade load image <filename> delete command to delete the firmware and upgrade Settings.
4. Run the show upgrade status command to display the upgrade progress of the ONU.
5. Run the show upgrade info command to display the ONU upgrade Settings.
6. Run the upgrade stop command to stop the ONU upgrade.

21.2.3 ONU Automatic Upgrade

The OLT will compare the device id and onu information, and if they agree, the upgrade will begin

Command	**Function**

Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**auto-upgrade onu equipment_id** *string* **version** *string* **image** *filename* **tftp** *A.B.C.D*	Configure the onu device, id, version, file name, and file address
Step 3	**no auto-upgrade equipment_id** *string*	Delete an onu
Step 4	**show auto-upgrade** <status|config>	Display automatic upgrade

21.2.4 Restart the ONU

Restart the authorized ONU

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** <all|(1-256)> **reboot**	Restart one of the ONUs or all ONUs on the PON

21.2.5 T-cont Configuration

Create/modify TCONT and bind it to the DBA configuration file.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **tcont** (1-255) {name *string*|dba *string*|profile_dba_id (0-128)}*1	Configure the created ONU TCONT, dba, and alloc-id.
Step 3b	**no onu** (1-256) **tcont** (1-255)	Delete TCONT

21.2.6 GEMPORT Configuration

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration

		mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **gemport** (1-255) **tcont** (1-255) *gemport_name* **portid** (129-4095)	Configure GEMPORT to bind TCONT. You can also select the port id and downstream traffic profile
Step 3b	**onu** (1-256) **gemport** (1-255) [tcont] (1-255) **down-traffic-limit** <traffic profile name> **onu** (1-256) **gemport** (1-255) **down-traffic-limit cir** (0-4294967295)	Configure GEMPORT to bind the traffic limiting profile
Step 4	**no onu** (1-256) **gemport** (1-255)	Delete the ONU GEMPORT

21.2.7 ONU Service Configuration

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **service** *service_name* **gemport** (1-255) **vlan** *vlan_list* **iphost** (1-255)	Configure the ONU service using vlans
Step 3b	**onu** (1-256) **service** *service_name* **gemport** (1-255) **untag** ethuni (1-32)	Configure the ONU service without vlan
Step 4	**no onu** (1-256) **service** *service_name*	Delete the ONU service

21.2.8 Service Port Configuration

Delete the ONU service

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **service-port** (1-256) **gemport** (1-256) **uservlan** (1-4094) [**to** (1-4094)] **transparent**	Configure the vlan Transparent mode

Step 3b	**onu** (1-256) **service-port** (1-256) **gemport** (1-256) **uservlan** (1-4094) **vlan** (1-4094)	Configure the VLAN conversion mode
Step 3c	**onu** (1-256) **service-port** (1-256) **gemport** (1-256) **uservlan untag vlan** (1-4094)	Configure the vlan untagged mode
Step 4	**onu** (1-256) **service-port** (1-128) **description** *desc*	Configure the description of the service port
Step 6	**no onu** (1-256) **service-port** (1-256)	Delete a service port

21.2.9 ONU UNI Configuration

Including LAN, VEIP, IPHOST

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **portvlan** <eth|wifi|veip> (1-32) **mode transparent**	Set the UNI mode to transparent
Step 3b	**onu** (1-128) **portvlan** [eth|wifi|veip] (1-32) **mode trunk**	Set the UNI mode to trunk
Step 3c	**onu** (1-128) **portvlan** [eth|wifi|veip] (1-32) **mode tag vlan** (1-4094) [pri (0-7)]	Set the UNI mode to access and bind vlan
Step 3d	**onu** (1-128) **portvlan** [eth|wifi|veip] (1-32) **mode hybrid def_vlan** (1-4094) [def_pri (0-7)]	Set the UNI mode to hybrid and bind vlan
Step 3e	**onu** (1-128) **portvlan** [eth|wifi|veip] (1-32) **vlan** *vlan_list*	Set UNI vlan list

21.2.10 Display ONU Service

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show running-config onu** [(1-256)]	Display onu running-config

21.2.11 Display the ONU Capability

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**show onu** <(1-256)|all> **capability**	Displays ONU capability values

21.3 ONU Remote port Configuration

21.3.1 ONU Port Enabled/Disabled

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**onu** (1-128) **eth** (1-32) **state** <disable|enable>	disable / enable a port

21.3.2 ONU Port Auto-negotiation

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**onu** (1-256) **eth** (1-32) **speed** <auto|full-10|full-100|full-1000|half-10|half-100|half-1000>	ONU Port auto-negotiation

21.3.3 ONU Configure Port Flow Control

Start from privileged configuration mode, configure ONU port flow control, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3	**onu** <(1-256)|all> **eth** (1-32) **pause-time** (0-65535)	Configure flow control

21.3.4 Multicast VLAN Configuration

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **mvlan** *vlanList*	Add a multicast vlan
Step 3b	**no onu** (1-256) **mvlan** <all|*vlanList*>	Delete a multicast vlan

21.3.5 Configure an ONU Iphost

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** (1-256) **iphost** (1-255) **id** *desc*	Set an iphost description
Step 3b	**onu** (1-256) **iphost** (1-255) **dhcp**	Set this parameter to dhcp mode
Step 3c	**onu** (1-256) **iphost** (1-255) **static-ip** *A.B.C.D A.B.C.D* [*A.B.C.D*]	Set this parameter to static mode, subnet mask, and gateway
Step 3d	**onu** (1-256) **iphost** (1-255) **primary-dns** A.B.C.D <[second-dns] A.B.C.D>*1	Configure DNS
Step 3e	**no onu** (1-256) **iphost** (1-255)	Delete an iphost configuration

21.3.6 ONU Configure the Port Multicast label

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON Interface configuration mode
Step 3a	**onu** *(1-256)* **mvlan** *[tag-strip]* **eth** *(1-32)*	Configure the multicast label
Step 3b	**no onu** *(1-256)* **mvlan** *[tag-strip]* **eth** *(1-32)*	Delete configuration

21.3.7 SFU Example

1GE ONU with vlan 100. Upstream DBA mode: 10 Mbit/s maximum. Gemport 1 with a 20 Mbit/s downlink.

1. Create an onu configuration file with one eth port
   profile onu name 1GE_SFU
   port eth 1
   commit
   exit
2. Create a dba configuration file. Ensure that a maximum of 10 MB is 20 MB
   profile dba name 20M
   type 3 assured 10240 maximum 20480
   commit
   exit
3. Create a traffic profile to limit the downlink speed
   profile traffic name DN_20M
   sir 20480 pir 20480
   commit
   exit
4. Register the onu and configure the service

interface gpon 0/1
show onu auto-find
onu add 1 profile 1GE_SFU sn GPON00000031
onu 1 tcont 1 dba 20M
onu 1 gemport 1 tcont 1
onu 1 service 1 gemport 1 vlan 100
onu 1 service-port 1 gemport 1 user-vlan 100 vlan 100
onu 1 portvlan eth 1 mode tag vlan 100

5. Create vlan 100

vlan 100

exit
6. Bind the vlan to the uplink port
interface gigabitethernet 0/1
switchport hybrid pvid vlan 100

21.3.8 HGU Example

4FE ONUs with vlan 41 and vlan 46. Upstream DBA mode: 10 Mbit/s maximum. Gemport 1 with a 20 Mbit/s downlink. vlan 46 is used for tr069, DBA mode: fixed 2M

1. Create an onu profile with one veip port
profile onu name HGU
port veip 1
commit
exit
2. Create a dba configuration fileprofile dba name 20M
type 3 assured 10240 maximum 20480
commit
exit
profile dba name 2M
type 1 fixed 2048
commit
exit
3. Create a traffic profile to limit the downlink speed
profile traffic name DN_20M
sir 20480 pir 20480
Commit
exit
4. Register the onu and configure the service
interface gpon 0/1
show onu auto-find
onu add 1 profile HGU sn GPON000000AB
onu 1 tcont 1 dba 20M
onu 1 tcont 2 dba 2M
onu 1 gemport 1 tcont 1
onu 1 service HSI gemport 1 vlan 41
onu 1 service-port 1 gemport 1 user-vlan 41 vlan 41
onu 1 gemport 2 tcont 2
onu 1 service TR69 gemport 2 vlan 46
onu 1 service-port 2 gemport 2 user-vlan 46 vlan 46
onu 1 portvlan veip 1 mode transparent
4. Create vlan41 and VLAN46 and bind them to uplink ports
vlan 41
exit
vlan 46

exit
interface gigabitethernet 0/10
switchport mode trunk
switchport trunk vlan 41
switchport trunk vlan 46

5. Log in to the onu network interface and create two WAN connections, one is the Internet using vlan41; The other is tr069 with vlan46

21.4 Private Configuration

21.4.1 Configure ONU ACL Rules

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**onu** (1-256) **pri acl [fttp|http|https|ping|telnet|tftp]** [enable|disable]	Configure the corresponding acl rules
Step 4	**onu** (1-256) **pri show**	Show results

21.4.2 Configure ONU CATV Status

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**onu** (1-256) **pri catv** [enable|disable]	Configure the catv status
Step 4	**show onu** (1-256) **pri catv_status**	Show results

21.4.3 Configure ONU DHCPv4 Server

	Command	Function
Step 1	**configure terminal**	Enter the global

		configuration mode
Step 2	**interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**onu** (1-256) **pri dhcp_server** *A.B.C.D A.B.C.D* <enable|disable|relay>	Configure the dhcp server status
Step 4	**onu** *1* **pri dhcp_server** *192.168.1.1 255.255.255.0* **enable** *10000 192.168.1.2 192.168.1.254* **stb** *8.8.8.8 114.114.114.114 192.168.1.1*	Example of configuring the dhcp server state: Create a dhcp server whose gateway is 192.168.1.1, address pool is 192.168.1.2 to 192.168.1.254, lease is 10000S, and DNS is 8.8.8.8 114.114.114.114
	Show onu (1-256) **pri dhcp_server**	Display result

21.4.4 Configure ONU DHCPv Server

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**onu** (1-256) **pri dhcp_server ipv6** *X:X::X:X* <*enable*|*disable*|*relay*>	Configure the dhcpv6 server status
Step 4	**onu** *1* **pri dhcp_server ipv6** *2550::11* **prefix_mode auto server enable preference** *10000* **valid** *5000 2000::1 2000::10 stb dns 204f::1 204f::2 gw 2550::11*	Example: Create a gateway with 2550::1,PD mode is automatic, preference time is 10000s, live time is 5000s, address pool range is 2000::1 to 2000::10,dns The dhcpv6 server is 204f::1 204f::2
	Show onu (1-256) **pri dhcp_server_ipv6**	Display result

21.4.5 Configure ONU Equid Server

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode

Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri equid** *(word)*	Example Change the id of an ONU device
Step 4	**Show running config onu** (1-256)	Display result

21.4.6 Restore ONU to Factory Defaults

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri factory_reset**	Restore the ONU to factory defaults

21.4.7 Configure ONU Firewall

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri firewall level** {disable|low|middle|high}*	Configure the ONU firewall

21.4.8 Configure ONU IGMP Mode

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri igmp** <*enable*|*disable*>	Configure ONU igmp

Step 4	**Show onu** (1-256) **pri igmp_status**	Display result

21.4.9 Configure ONU LAN Binding Mode

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri lan_bind_mode port** (1-255) **mode vlan lanVlan0** (1-4094) **wanVlan0** (1-4094)	Set the ONU LAN binding mode to vlan
Step 4	**Onu** (1-256) **pri lan_bind_mode port** (1-255) **mode port**	Set the ONU LAN binding mode to vlan
Step 5	**Show Onu** (1-256) **pri lan_bind_mode**	Display result

21.4.10 Configure ONU Loopback

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri loopback_detect** *<enable|disable>*	Configure ONU loopback
Step 4	**Show Onu** (1-256) **pri loopback**	Display result

21.4.11 Configure ONU MAC Connection

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON

		port
Step 3	**Onu** *(1-256)* **pri mac_aging_time** <0-65535>	Set the ONU MAC aging time
Step 4	**Onu** (1-256) **pri mac_clean**	Clear the ONU mac table
Step 5	**Onu** (1-256) **pri mac_limit pon** <0-65535>	Example Set the aging time of an ONU mac address
	Show Onu (1-256) **pri mac_addr_table**	The ONU MAC table is displayed

21.4.12 Configure ONU Port Isolation

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri port** <disable|enable>	Configure ONU port isolation

21.4.13 Configure ONU Voice Port

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri pots** (1-255) **sip_user_config active enable acconut** <word max length 16> **name** <*word max length 16*> **pwd** <*word max length 16*>	Configure ONU voice port information
Step 4	**Show Onu** (1-256) **pri pots** <1-255 >	Display result

21.4.14 Save ONU Configuration

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri save_config**	Save The ONU configuration

21.4.15 Configure ONU Voice SIP Service

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri pots** <1-255> **sip_global_param mg_port** (1-255) **proxy_serv** *WORD* <0-65535(port)> **backup_proxy_serv** *WORD* <0-65535(port)> **reg_serv** *WORD* <0-65535(port)>	Configure ONU sip server information
Step 4	**Onu** *(1-256)* **pri sip show json**	Display result

21.4.16 Configure ONU RSTP

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri spanning_tree** <enable|disable>	Configure ONU RSTP

21.4.17 Configure ONU Upstream Speed Limit

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri speed_limit us** （1-9953000,kbps)	Configure ONU uplink limiting

21.4.18 Configure ONU TR069 Management Information

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri tr069_mng enable ace_server url** *WORD* **username** *WORD* **password** *WORD* **certificate** <disable|enable> **inform** <disable|enable> **inform_interval** （0-4294967295)	Configure ONU TR069 management information
Step 4	**Onu** (1-256) **pri tr069_stun** <disable|enable> **server** *WORD* **port** (1-65535) **username** *WORD* **password** *WORD*	Configure the ONU TR069 Stun server
Step 5	**Show Onu** (1-256) **pri tr069**	Display result

21.4.19 Configure ONU UPnP

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri upnp status** <*disable/enable*> **wan_index** (1-8)	Configure ONU UPNP

21.4.20 Configure ONU WAN Information

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri wan_adv index** *(1-8)* **route** <ipv4|ipv6|both> <dhcp|pppoe|static> **dns** *WORD* **nat** <disable|enable>	Example of configuring ONU route wan
Step 4	**Onu** (1-256) **pri wan_adv index** (1-8) **bridge** <ipv4|ipv6|both>	Example of configuring ONU bridge wan
Step 5	**Onu** (1-256) **pri wan_adv index** (1-8) **bind** [lan|ssid]	Configure WAN bond ports
Step 6	**Onu** (1-256) **pri wan_adv index** (1-8) **delete**	Deleting a WAN
Step 7	**Onu** (1-256) **pri wan_adv commit**	Commit WAN
Step 8	**Show Onu** (1-256) **pri wan_adv**	Display result

21.4.21 Configure ONU WIFI SSID

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**Interface gpon** *slot/port*	Enter the corresponding PON port
Step 3	**Onu** (1-256) **pri wifi_ssid** (1-8) **disable**	Turn off wifi
Step 4	**Onu** (1-256) **pri wifi_ssid** (1-8) **name** *WORD* **hide** <disable|enable>	Set whether the WIFI SSID is hidden
Step 5	**Onu** (1-256) **pri wifi_ssid** (1-8) **name** <*word* > **hide disable**	Configure WAN bond ports
Step 6	**onu** (1-256) **pri wifi_switch** (1-2) **enable{**fcc|etsi|ic|spain|france|mkk|isreal|mk k2|mkk3|russian|cn|global|world-wide|mkk1|ncc][auto|chl_34|chl_36|chl_38|chl_40|chl_42|ch	Configure WIFI channels, protocols, etc

	l_44|chl_46|chl_48|chl_52|chl_56|chl_60|chl_64|chl_100|chl_104|chl_108|chl_112|chl_116|chl_120|chl_124|chl_128|chl_132|chl_136|chl_140|chl_144|chl_149|chl_153|chl_157|chl_161|chl_165]<80211ac0|80211acA|80211acN|80211acAN|80211acNAC|80211acANAC|80211acax|80211acanacax}*(0-20) {20|40|80|20/40|20/40/80|160}* {easy_mesh <enable|disable>}*	
Step 7	**Show Onu** (1-256) **pri wifi_ssid**	The wifi ssid information is displayed
Step 8	**Show Onu** (1-256) **pri wifi_switch**	The wifi channel information is displayed

21.5 Rogue ONU Configuration

An ONU that does not follow the specified timestamp to send an optical signal is called a rogue ONU.
There are two main types of rogue ONUs:
1) Long time Glowing rogue ONU: ONU is glowing (glowing at any time).
2) Luminous rogue ONU: The ONU is not assigned a timestamp in the OLT, which may be premature luminous, or delayed shutdown, and so on.

21.5.1 Rogue ONU Detection

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**rogue-onu-detect auto-shutdown** <enable|disable>	Enter the corresponding PON port
Step 3	**show rogue-onu-detect config**	Display configuration
Step 4	**show rogue-onu-detect info** pon (1-8)	Display result

21.5.2 Rogue ONU Status

	Command	**Function**
Step 1	**configure terminal**	Enter the global

		configuration mode
Step 2	**show rogue-onu-detect config**	Display configuration

22. ONU Profile Management

22.1 Summary of ONU Profile

The template is under the "config" node, and the operation steps are as follows:
1. Create the profile
profile <onu|dba|traffic|line|srv|voip|alarm> <id (1-32767)>*1 <name string>*1
2.Enter the corresponding profile node via profile_id
profile <onu|dba|traffic|line|srv|voip|alarm> <id (1-32767)>*1 <name string>*1
3.Modifying profile parameters
modify …
4.Exit profile node
exit
5.Bind the profile to the onu device
Interface <gpon|xgpon>S（0）/P（1-x）
onu add *1* **profile** *string*
onu <onuid> **profile** <line|srv> *string*
6.Query the onu device binding profile
Interface <gpon|xgpon>S（0）/P（1-x）
show profile <onu|dba|traffic|line|srv|voip|alarm> *<id (1-32767)>*1 <name string>*1*
7.Query profile configuration information
Show profile <onu|dba|traffic|line|srv|voip|alarm> *<id (1-32767)>*1 <name string>*1 used-info*

22.2 ONU Profile Configuration

ONU profile are used for ONU authorization, and only one ONU profile can be specified for each ONU during authorization. The ONU template specifies the capabilities of that ONU.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile onu** {id (1-128) |name *name }*1*	Create or enter the onu profile you created earlier.
Step 3a	**tcont-num** (1-255) **gemport-num** (1-255)	Configure the maximum tcont and gemport supported by the onu.
Step 3b	**switch-num** (1-255) **flow-num** (1-255)	Configure the maximum switching port and traffic supported by the onu

Step 3c	**port-num** {{eth(0-64)|pots(0-64) iphost (0-255)}*1 <ipv6host (0-255) |veip(0-127)>}*1	Configure onu eth/pots/iphost/ipv6host/veip
Step 3d	**service-ability n:1** <yes|no> **1:p** <yes|no>**1:m** <yes|no>	Capability value configuration
Step 4	**commit**	Commit the configuration file. The Settings can only be committed by typing "commit"
Step 5	**exit**	

22.3 DBA Profile Configuration

The default system will have a dba profile with id 0, this template parameter cannot be modified, and all ONUs will be in the template when the default binding is created. Each ONU must bind a dba template.
It have 5 dba filre:
Typr1: fix, integral
Type2: assure, integral
Type5: fix, assure, max, integral
Fix<=assure<=max.

BW Type	Delay Sensitive	Applicable T-CONT types				
		Type 1	Type 2	Type 3	Type 4	Type 5
Fixed	Yes	X				X
Assured	No		X	X		X
Non-Assured	No			X		X
Best Effort	No				X	X
Max.	No			X	X	X

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile dba** <id (1-128) |n*ame name*>	Create/modify dba configuration files
Step 3a	**type 1 fixed** (256-9953280)	Configure type 1 to be fixed

Step 3b	**type 2 assured** (256-9953280)	Configure type 2 to be guaranteed
Step 3c	**type 3 assured** (256-9953280) **maximum** (256-9953280）	Configure type 3 with guaranteed and maximum values
Step 3d	**type 4 maximum** (256-9953280)	Configures type 4 with the maximum value
Step 3e	**type 5 fixed** (256-9953280) **assured** (256-9953280) **maximum** (256-9953280)	Configure type 5 with fixed, guaranteed, maximum values

22.4 Traffic Profile Configuration

The default system will have a traffic profile with id 0, this profile parameter cannot be modified and all gemports are in the profile when the default binding is created. Each GEMPORT must be bound to a traffic profile.

parameter	Detail	Range
Sir	Receptive information rate	*0-10000000*kbps
Pir	Peak information rate	*0-10000000*kbps
Cbs	Commitment message size	*0-536870911*kbytes
pbs	Peak burst size	*0-536870911*kbytes

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile traffic** <id (1-128)| name *name*>	Create/modify traffic profiles
Step 3	**sir** (0-10000000) **pir** (64-10000000) [**cbs** (0-1023) **pbs** (0-1023)]	Configuring cir and pri, cbs and pbs is optional
Step 4	**Exit**	

22.5 Line Profile Configuration

The default system will have a line profile with id 0, this profile parameter cannot be modified

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile line** <id (1-128)|name *name*>	Create a modified line

		profile
Step 3	**tcont** (1-255) {name WORD|dba WORD | profile_dba_id (0-128)}*1	Bind the tcont configuration file
Step 4	**gemport** (1-255) **tcont** (1-255) **gemport_name** *gemport_name*	Binding the gemport configuration file
Step 5a	**service** *service_name* **gemport** (1-255) **vlan** <0|*VLAN_LIST*> [ethuni (1-32)|iphost (1-255)]	Bind gemport with vlan to the service
Step 5b	**service** <*service_name*> **gemport** (1-255) [untag] [ethuni (1-32)|iphost (1-255)]	Bind gemport without vlan to the service
Step 5c	**mvlan** *vlanlist*	Create a multicast vlan
Step 6a	**service-port** (1-128) **gemport** (1-128) **uservlan** (1-4094) **to** (1-4094)	Configure vlan mode to pass-through
Step 6b	**service-port** (1-128) **gemport** (1-128) **uservlan** (1-4094) **vlan** (1-4094) [svlan (1-4094)]	Configure VLAN mode to translate, QinQ
Step 6c	**service-port** (1-128) **gemport** (1-128) **uservlan untag vlan** (1-4094) [svlan (1-4094)]	Configure vlan mode to untag, QinQ
Step 6d	**service-port** (1-128) **description** *desc*	Add a service port description
Step 7	**commit**	Submitting configuration
Step 8	**Exit**	
Step 9	**no service-port** (1-128)	Remove a service port
Step 10	**no mvlan** <all|*vlanlist*>	Delete the multicast vlan
Step 11	**no tcont** (1-255)	Delete tcont
Step 12	**no gemport** (1-255)	Delete gemport
Step 13	**no service** *service_name*	Delete service

22.6 Service Profile Configuration

The system will have an SRV profile with id 0 by default and this template parameter cannot be modified

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile srv** [id (1-128)] **name** *name*	Create/modify srv profile
Step 3a	**portvlan <**eth|wifi|veip> (1-32) **mode** transparent	Configure portvlan mode to transparent
Step 3b	**portvlan <**eth|wifi|veip> (1-32) **mode**	Configure the portvlan mode

	trunk	to trunk
Step 3c	**portvlan** <eth|wifi|veip> (1-32) **mode tag** vlan (1-4094) **pri** (0-7)	Configure portvlan mode to tag, and configure pri
Step 3d	**portvlan**<eth|wifi|veip> (1-32) **mode hybrid def_vlan** (1-4094) **def_pri** (0-7)	Configure portvlan mode to hybird
Step 4a	**mvlan tag-strip eth** (1-32)	Configure the LAN port to untag mode
Step 4b	**no mvlan tag-strip eth** (1-32)	Remove LAN port untag mode
Step 5b	**iphost** (1-255) **dhcp**	Configure iphost to dhcp mode
Step 5c	**iphost** (1-255) **static-ip** *A.B.C.D A.B.C.D* [*A.B.C.D]*	Configure iphost to static mode
Step 5d	**Iphost** (1-255) **primary-dns** *A.B.C.D* **second-dns** *A.B.C.D*	Configuring DNS
Step 5e	**no iphost** (1-255)	Delete the iphost configuration
Step 6	**Commit**	Submitting configuration
Step 7	**Exit**	

22.7 Alarm Threshold Profile Configuration

Alarm thresholds can only be configured via profile. Start from the privileged configuration mode, configure the alarm threshold profile as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile alarm** [id (1-128)] **name** *name*	Create or enter a configuration file
Step 3a	**sf-sd-threshold sf** (3-8) **sd** (4-10)	Configure the range of sf and sd
Step 3b	**rx-optical low** (-27~-8) **high** (-27~-8)	Configure rx optical range
Step 3c	**tx-optical low** (1-5) **upper** (1-10)	Configure the range of tx optical
Step 4	**Commit**	Submitting configuration
Step 5	**Exit**	

22.8 Private Profile Configuration

Command	**Function**

Step 1	**configure terminal**	Enter global configuration mode
Step 2	**profile pri** *id* <1-128> *name* <*string*>	Create/modify the pri profile
Step 3	**wan_adv add** <bridge|route>	Add a route/bridge WAN
Step 4	**wan_adv index** (1-8) **bind** {lan1|lan2|lan3|lan4|lan5|lan6|lan7|lan8|ssid1|ssid2|ssid3|ssid4|ssid5|ssid6|ssid7|ssid8|ssid9|ssid10}*1	Binding port
Step 5	**wan_adv index** *(1-8)* **bridge** {internet|other} **mtu** *(576-1500)* [ipv4|ipv6|both]	Configuring Bridge WAN
Step 6a	**wan_adv index** *(1-8)* **route both pppoe proxy** <enable|disable> **user** *NAME* **pwd** *WORD [server NAME]* **mode** <auto|payload> **nat** <enable|disable> **slaac** <enable|disable>	Configure pppoe mode routing WAN
Step 6b	**wan_adv index** (1-8) **route both static ipv4** *A.B.C.D* **mask** *A.B.C.D* **gw** *A.B.C.D* **dns** <primary|master> <*A.B.C.D*> <secondary|slave> <*A.B.C.D*> **nat** <enable|disable> **ipv6** *X:X::X:X/M* **gw** *X:X::X:X* **dns** <primary|master> *X:X::X:X* <secondary|slave> *X:X::X:X*	Configuring a routing WAN in static mode
Step 6c	**wan_adv index** (1-8) **route** <*both*|*ipv6*> **client_address** <enable|disable> **client_prifix** <enable|disable> **aftr_mode** <*dhcpv6*|*manual*> **address_type** <*ipv6*|*dns WORD*>	Configure the client_address, client_prifix, and aftr_mode of the routing WAN
Step 6d	**wan_adv index** *(1-8)* **route both dhcp** [dns-v4 <primary|master> *A.B.C.D* <secondary|slave> *A.B.C.D]* [nat <enable|disable>] [dns-v6 <primary|master> *X:X::X:X* <secondary|slave> *X:X::X:X]* [slaac <enable|disable>]	Configure dhcp mode routing WAN
Step 7	**wan_adv index** (1-8) **route mode <**internet|multicast|tr069|tr069_internet|tr069_voip|voip_internet|tr069_voip_internet|voip|other}* [mtu (576-1500)]	Configure the mode of routing WAN
Step 8a	**wan_adv index** (1-8) **vlan disable** [qos <enable|disable>]	VLAN to disenable WAN

Step 8b	**wan_adv index** (1-8) **vlan tag** [wan_vlan (1-4095) (0-7)] [qinq tpid (1-65534) vlan (1-4095) cos (0-7)] [qos {enable|disable}]	Configure the VLAN mode to tag
Step 8c	**wan_adv index** (1-8) **vlan transparent** [wan_vlan (1-4095) (0-7)] [tranlation (1-4095) (0-7)] [qinq tpid (1-65534) vlan (1-4095) cos (0-7)] [qos {enable|disable}]	Configure VLAN mode to transparent
Step 9	**wan_adv index** (1-8) **bind** <lan|ssid>	Bind lan port and ssid
Step 10	**wan_adv commit**	Submitting WAN
Step 11	**wan_adv index** (1-8) **delete**	Removing index
Step 12	**dhcp_server** *A.B.C.D A.B.C.D* **disable**	disenable the dhcp server
Step 13a	**dhcp_server** *A.B.C.D A.B.C.D* **enable** (0-4294967295) *A.B.C.D A.B.C.D* [pc|camera|stb|ip_phone]*A.B.C.D A.B.C.D A.B.C.D*	Configure the dhcp server
Step 13b	**dhcp_server ipv6** X:X::X:X **prefix_mode** {auto|static X:X::X:X/M|wan_delegated (1-8)}* **server enable preference** (0-4294967295) **valid** (0-4294967295) *HHHH:HHHH:HHHH:HHHH HHHH:HHHH:HHHH:HHHH* <pc|camera|stb|ip_phone> **dns** *X:X::X:X X:X::X:X* **gw** *X:X::X:X* [ra manage <enable|disable> other <enable|disable> max_interval (1-1800) min_interval (1-1800)]	Configure the dhcpv6 server
Step 13c	**dhcp_server ipv6** *X:X::X:X* **prefix_mode** {auto|static *X:X::X:X/M*|wan_delegated (1-8)}*1 **server disable** [ra manage {enable|disable} other {enable|disable} max_interval (1-1800) min_interval (1-1800)]	To enable dhcpv6 server
Step 13d	**dhcp_server ipv6** *X:X::X:X* [prefix_mode static *X:X::X:X/M*]	Configuring dhcpv6 in static mode server
Step 13e	**dhcp_server ipv6** *X:X::X:X* [prefix_mode wan_delegated (1-8)]	Configure the dhcpv6 server in wan_delegated mode
Step 14a	**wifi_ssid** (1-8) **name** *WORD* **hide** {enable|disable} **auth_mode** {open|shared|wepauto}*1 **encrypt_type** *wep* **encryptionlevel** <64|128> **keyindex** (1-4) **key1** *WORD* **key2** *WORD* **key3** *WORD* **key4** *WORD*	Configure the dhcpv6 server in wan_delegated mode

Step 14b	**wifi_ssid** (1-8) **name** *WORD* **hide** <enable|disable **auth_mode** <*wpapsk*|*wpa2psk*|*wpapsk_wpa2psk*|*wpa3psk*|*wpa2psk_wpa3psk*> **encrypt_type** <*tkip*|*aes*|*tkipaes*>*1 **shared_key** *WORD* [rekey_interval (0-4194303)]	Configure the dhcpv6 server in wan_delegated mode
Step 15	**wifi_ssid** (1-8) **disable name** *WORD*	To enable ssid
Step 16a	**wifi_switch** (1-2) **enable** [fcc|etsi|ic|spain|france|mkk|isreal|mkk2|mkk3|russian|cn|global|world-wide|mkk1|ncc] (0-14) [80211b|80211g|80211bg|80211n|80211bgn|80211ax|80211bgnax|80211gn] (0-20) <20|40|20/40>	Configure 2.4G wifi_switch
Step 16b	**wifi_switch** (1-2) **enable** [fcc|etsi|ic|spain|france|mkk|isreal|mkk2|mkk3|russian|cn|global|world-wide|mkk1|ncc] *[auto|chl_34|chl_36|chl_38|chl_40|chl_42|chl_44|chl_46|chl_48|chl_52|chl_56|chl_60|chl_64|chl_100|chl_104|chl_108|chl_112|chl_116|chl_120|chl_124|chl_128|chl_132|chl_136|chl_140|chl_144|chl_149|chl_153|chl_157|chl_161|chl_165] * {80211ac0|80211acA|80211acN|80211acAN|80211acNAC|80211acANAC|80211acax|80211acanacax] (0-20) [<20|40|80|20/40|20/40/80|160>] [easy_mesh <enable|disable>]	Config 5G wifi_switch
Step 17	**wifi_switch** (1-2) **disable**	Disable the wifi
Step 18	**no wifi_ssid** (1-8)	Delete Wi-Fi ssid configuration
Step 19	**no wifi_switch** (1-2)	Delete Wi-Fi switch Configuration
Step 20a	**sip_global_param mg_port** (0-65535) **proxy_serv** WORD (0-65535) [backup_proxy_serv WORD (0-65535)] **reg_serv** WORD (0-65535) [backup_reg_serv WORD (0-65535)] **out_bound_serv WORD** (0-65535) **reg_interval** (1-10000000) **heartbeat** <active|passive> (1-65535) (1-65535)	Configure SIP to enable heartbeat packets.
Step 20b	**sip_global_param mg_port** (0-65535)	Configure SIP to close

	proxy_serv WORD (0-65535) [backup_proxy_serv WORD (0-65535)] **reg_serv** WORD (0-65535) [backup_reg_serv WORD (0-65535)] **out_bound_serv** WORD (0-65535) **reg_interval** (0-10000000) **heartbeat** disable	heartbeat packets
Step 21	**no sip_global_param**	Delete SIP configuration
Step 22	**pots** (1-255) **parameter vad** <enable|disable> **echo_cancel** <enable|disable> **input_gain** WORD(-32-32) **output_gain** WORD(-32-32) **dtmf_mode** <transparent|rfc2833|rfc2833_redundancy|outband>	Configure pots advanced parameters
Step 23a	**pots** (1-255) **sip_user_config active** disable	Disable pots
Step 23b	**pots** (1-255) **sip_user_config active** enable **account** WORD **name** WORD **pwd** WORD	Configure the pots user parameters
Step 24	**no pots** (1-255) **parameter**	Delete the pots' configuration
Step 25a	<port_isolate|spanning_tree|catv|igmp> <enable|disable>	Configure port isolation、stp、catv、igmp
Step 25b	**speed_limit us** (1-9953000) **ds** (1-9953000)	Configure rate limit
Step 25c	**mac_aging_time** (0-65535)	Configure the mac aging time
Step 25d	**mac_limit pon** (0-65535) **lan** (0-65535)	Configure the mac aging time
Step 26a	**nat_type** <nat1|nat2|nat3|nat4-napt>	Configure the nat type
Step 26b	**upnp status disable**	Disable the upnp
Step 26c	**upnp status enable wan_index** (1-8)	Configure upnp
Step 26d	**no** <nat_type|upnp>	Delete NAT/UPNP configuration
Step 27a	**onu_mode status** disable	Disable the onu mode state
Step 27b	**onu_mode status** enable **mode** <sfu|hgu|auto>	Configure the onu mode status
Step 28	**username admin_control enable** *WORD WORD* **user_control enable** *WORD WORD*	Configure the account number and password of the admin users and user users
Step 29	**firewall level** <disable|low|middle|high>	Configure firewall
Step 30	**acl** <telnet|ftp|http|https|tftp|ping|ssh> **control enable lan** <enable|disable> **wan**	Configure ACL

	enable ipv4_control enable *A.B.C.D A.B.C.D* **ipv6_control enable** *X:X::X:X/M* [port (0-65535)]	
Step 31	**loopback_detect** <enable|disable> [loopcheck_interval (1-60000)] [recover_interval (1-1800)] [ethernet_type WORD] [vlan (1-4094)] [dest_mac_type <broadcast_address|bpdu_address>] [port_closing_time (1-1800)] [alarm <enable|disable>] [portdislooped <enable|disable>]	Configure loop detection
Step 32a	**tr069_mng** disable	Disable tr069 manage
Step 3b	**tr069_mng** enable **acs_server url** *WORD* **username** *WORD* **password** *WORD* **certificate** <enable|disable> **inform** <disable|enable inform_interval (0-4294967295)> **reverse_connection username** *WORD* **password** *WORD*	Disable tr069 manage
Step 32c	**tr069_stun** disable	Disable tr069 stun
Step 32d	**tr069_stun** *enable* **server** *WORD* **port** (1-65535) [username *WORD* password *WORD*]	Configure tr069 stun
Step 33	**show profile pri id** (1-128) **name** *string*	Show the private profile configuration
Step 34	**Exit**	Exit

22.9 IGMP Profile Configuration

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**profile igmp** {id <1-128>}*1 {name <string>}*1	Configure the igmp profile
Step 3	**igmp-mode** <snooping|spr|proxy>	Configure the igmp mode
Step 4	**igmp-rate-limit** (0-4294967294)	Configure the igmp rate limit
Step 5	**igmp-version** <igmp-v1|igmp-v2|igmp-v3|mld-v1|mld-v2>	Configure the igmp version
Step 6	**show profile igmp** *[id* (1-128)|name WORD|running-config]	Show the igmp configuration

22.10 Format Profile Configuration

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**profile format** {id <1-128>}*1 {name <string>}*1	Configure the format profile
Step 3	**switch** [option82 <enable|disable>] [option18 <enable|disable>] [option37 <enable|disable>] [pppoe-plus <enable|disable>]	Add exchange configuration
Step 4	**format type** <custom|ctc|unicom>	Configure the format type
Step 5	<circuit-id|remote-id> **index** (1-22) <cvlan|devtype|acnoid|slotno|ponno|onuno|onutype|onusn|oltmac|end>	Configure the circuit-id and remote-id parameters
Step 6	**show profile format** [id (1-128)|name WORD|running-config]	Show the format configuration

22.11 ONU Binding Profile Configuration

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface gpon** *slot/port*	Enter the PON interface configuration mode
Step 3	**onu** <all|(onu_list)> **profile** <line|srv|alarm|pri|format> <name WORD|id (1-32767)>	Give the ONU binding profile configuration
Step 4	**no onu** <all|(onu_list)> **profile** <line|srv|alarm|pri|format>	Give the ONU to unbind the profile configuration
Step 5	**show onu** <all|(onu_list)> **profile**	Show the ONU profile configuration

22.12 Show/Delete the Profile

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode

Step 2	**no profile** <dba|srv|traffic|alarm|format|igmp|line|onu|pri> **id** <1-128>	Remove the profile
Step 3a	**show profile** <dba|srv|traffic|alarm|format|igmp|line|onu|pri> **id** <1-128>	Show the profile

23. ONU Auto-learn Configuration

23.1 ONU Automatic Learn

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**onu auto-learn bind** (line-profile|srvline-profile|alarmline-profile|formatline-profile|onuline-profile|priline-profile) *equipid profile_name*	Bind the onu device to the line | srv | alarm | format | onu | pri profile
Step 3	**no onu auto-learn bind** (line-profile|srvline-profile|alarmline-profile|formatline-profile|onuline-profile|priline-profile) *equipid profile_name*	Remove the binding settings
Step 5	**show onu auto-learn bind** (line-profile|srvline-profile|alarmline-profile|formatline-profile|onuline-profile|priline-profile)	Show the devices and configuration files

23.2 Enable Automatic Learn

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gpon** *slot/port*	Enter PON interface configuration mode.
Step 3a	**onu auto-learn** <alarm-profile|format-profile|line-profile|pri-profile|srv-profile)> **name** *name*	Enable the auto-learn function.It support to select onu profile.will bind the default profile if not select.
Step 3b	**no onu auto-learn**	Disable the auto-learn
Step 4	**show onu auto-learn**	Show the auto-learn

24. System Management

24.1 Configuration Management

24.1.1 Save the Configuration

After you modify the configurations, you should hold them unchanged so that they can take effect on the next restart. Save the configuration by using the following command.

	Command	Function
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**write**	Save the configuration

24.1.2 Erase Configuration

If you need to reset to factory defaults, you can erase all configurations using the following command. After the erase, the device will automatically restart.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**erase startup-config**	Erase all configurations

24.1.3 Display the Boot Configuration

Use the following command to display the saved configuration.。

	Command	Function
Step 1	**configure terminal**	Use the following command to display the saved configuration.
Step 2	**show startup-config**	Show the configuration

24.1.4 Display the Running Configuration

Use the following command to display the running configuration. These running configurations may not be saved in the flash memory。

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show running-config**	Show the running configuration

24.1.5 Upload/Download the Configuration File

Use the following command to upload the configuration file to the PC, and download the configuration file to the device.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**debug mode**	Enter the debug mode
Step 3a	**upload tftp configuration** *filename* *<A.B.C.D|X:X::X:X>*	filename Is the upgrade file, A.B.C. D is the TFTP server IP
Step 3b	**download tftp configuration** *filename* *<A.B.C.D|X:X::X:X>*	filename Is the upgrade file, A.B.C. D is the TFTP server IP

24.2 Display System information

24.2.1 Display System Operation Information

Use the following command to view the system information.

Command	Function
show sys arp	Show the ARP table
show sys cpu	Show the CPU information
show sys cpu-usage	Show the CPU utilization rate
show sys mem	Show the system memory
show sys ps	Show the system process
show top	Show the CPU utilization rate
show task	Show the thread name

24.2.2 Display Version Information

Use the following command to check the version information, including the hardware version, software version, software creation time, etc.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show version**	Show the version information

24.2.3 Display the System Running Time

Use the following command to display the running time of the system after the power is turned on.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show sys running-time**	Show the system running time

24.3 System Basic Configuration

24.3.1 Configure the System Name

Change the system name by using the following command. This modification will take effect immediately. You will see it in the command-prompt prefix. Start from the privileged configuration mode, press the configuration system name as shown in the table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**hostname** *name*	Configure the system name. It must begin with a letter.
Step 3	**hostname default**	Restore the default

24.3.2 Configure the Terminal Timeout Value

Use the following command to configure the terminal timeout value. The default value is for 10 minutes.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode

Step 2	**line vty**	Enter the line node
Step 3a	**exec-timeout** (0-35791)	Set the command-line timeout time
Step 3b	**no exec-timeout**	Set the command line timeout to the default value
Step 4	**show exec-timeout**	Show plays command line timeout

24.4 System Basic Operations

24.4.1 Upgrade the System

Upgrade the device by using the following command.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**download tftp image** *filename* *<A.B.C.D|X:X::X:X>*	Filename Is the upgrade file with a header h,A.B.C. D is the TFTP server IP

24.4.2 Restart the System

Restart the system by using the following command

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**reboot**	Restart the system

24.4.3 Telnet

You can remotely connect to the system via an out-of-band or in-band management IP. The default management IP is 192.168.8.100.

	Command	**Function**
Step 1	**telnet** *A.B.C.D*	Telnet To the application layer of the system. Login name is admin and password is Xpon@Olt9417#.
Step 2	**telnet** *A.B.C.D* port (1-65535)	Telnet To the system kernel. The login name is the

		default.
Step 3	**switch**	Telnet To the system kernel. The login name is the default.(only for console)

24.4.4 Configure the RTC System Time

Use the following command to configure the RTC system time

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**time set year** (2000-2099) **month** (1-12) **day** (1-31) **hour** (0-23) **minute** (0-59) **second** (0-59)	Configure the RTC clock
Step 3	**show time**	Show the system time

24.4.5 NTP Client

When you enable NTP, the device automatically updates the time

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**ntp server** *Hostname or IP address* [*backup server*]	Configure the NTP server and enable it
Step 3	**no ntp server**	Disable the NTP server
Step 4	**show time**	Show the system time

24.4.6 Configure Time Zone

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**time zone** *timezone*	Configure time zone
Step 3	**show sys timezone**	Show time zone

24.4.7 Fan Control

Use the following command to control the fan running attributes.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**fan temperature** (20-80)	Configure fan temperature
Step 3	**fan mode** <open|close|auto>	Configure the fan operation mode
Step 4	**show fan**	Show the fan configuration and the current device temperature

24.4.8 PON Mode Switching

Change the PON mode with the following command.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show pon mode**	Show the current PON mode
Step 3	**debug mode**	Enter the debug mode
Step 4	**set slot** (0-2) **pon mode** <gpon|xgpon|xgspon>	Configure the PON mode

25. User management

25.1 User privilege

The user has two permissions, the administrator user and the ordinary user. Ordinary users are read-only users, who can only view the system information, but can not view the user information, configuration. The administrator user can view all the information and configure all the parameters.

25.2 Default User

By default, there is an administrator user, admin, whose password is Xpon@Olt9417#. The default user cannot be deleted, modify, but you can change their password.

25.3 Add User Account

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**user add** *user-name* **login-password** *login-password*	Add a new user account
Step 3	**user role** *user-name* (admin|normal) **enable-password** *enable-password*	Specify the user role, the new user is the normal privileged user

25.4 Display List of User Accounts

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**user list**	Show a list of user accounts

25.5 Delete User Account

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode

Step 2	**user delete** *username*	Delete user account

25.6 Change Password

Each user can change their own password, while administrator users can change the passwords of other users. Change the password, as shown in the table below.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**user login-password** *user-name*	Configure the user's login password
Step 3	**user enable-password** <*user-name*>	Configure the user's configuration mode password

26. Login Management

26.1 Overview

Login management is mainly used as a way to manage access to olt, service port number, login verification code, timeout time, and modify the language of the web page. In addition, we can only see the number of users of telnet logged in.

26.2 Login Access list Configuration

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**login-access-list** <enable|disable>	Open / close the login access control list
Step 3	**login-access-list** < <deny|permit> <web|telnet|snmp|ssh|ping> *A.B.C.D A.B.C.D* |ipv6 <deny|permit> <web|telnet|snmp|ssh|ping> x:x::x:x/m >	Configure the login access list
Step 4	**no login-access-list** < <deny|permit> <web|telnet|snmp|ssh|ping> *A.B.C.D A.B.C.D* |ipv6 <deny|permit> <web|telnet|snmp|ssh|ping> x:x::x:x/m ><*A.B.C.D/M*>|*X:X::X:X/M*| *A.B.C.D A.B.C.D*>	Clear the login access list configuration
Step 5	**show login-access-list**	Show the login access list configuration

26.3 Service Port Configuration

Start from the privileged configuration mode, configure the group name as shown in the table.

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**telnet port** <(1-65535)|default>	Configure the service port for the telnet
Step 3	**exit**	Returns to the global configuration mode

Step 4	**ssh port** <(1-65535)|default>	Configure the service port for the ssh
Step 5	**exit**	Returns to the global configuration mode
Step 6	**snmp-server agent port** (1-65535)	Configure the service port for the snmp
Step 7	**exit**	Returns to the global configuration mode
Step 8	**web**	Show the web mode
Step 9	**web port** <(1-65535)|default>	Configure the service port for the web
Step 10	**exit**	Returns to the global configuration mode
Step 11	**write**	Save configuration

26.4 Login Configuration

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**web login timeout** (1-180)	Configure the login time-out time for the web
Step 3	**show web login timeout**	Show the login timeout time of the web
Step 4	**web verification-code** <enable|disable>	Configure the login verification code for the web
Step 5	**show web verification-code**	Show the login verification code enabling status of the web

26.5 Telnet Management

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 3	**show telnet login-user**	Show the telnet login user
Step 4	**no telnet login-user** T*EL_USER* [vty	Exit the login of individual

	index]	telnet users
Step 5	**exit**	Returns to the global configuration mode

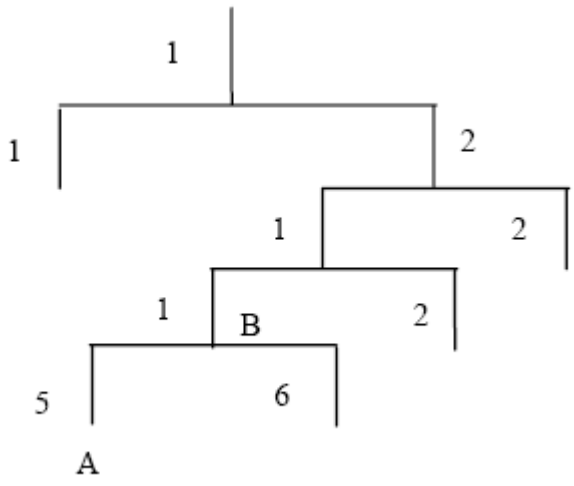
27. SNMP Configuration

27.1 Overview

SNMP(Simple Network Management Protocol)is a currently widely used network management protocol. It is an industry standard for transmitting management information between two devices. Network administrators can search for information, modify information, troubleshoot, diagnose faults, plan capacity, and generate responses. SNMP uses a polling mechanism that provides basic functions, especially suitable for small, fast, and low-cost situations. It is based on the transport layer protocol UDP.
SNMP has two parts, NMS (Network Management Station) and agent. The NMS is a workstation running a client program, while the agent is a server program running in the device. The NMS can send the GetRequest, GetNextRequest, and SetRequest messages to the agent. The agent will then execute the read or write commands and respond to the NMS. The agent also sends a trap message to the NMS when the device is abnormal.

27.2 SNMP Version and MIB

To uniquely label the management variables of the device, SNMP identifies management objects through a hierarchy name scheme. The object set is like a tree, and the nodes represent the managed objects, as shown in the figure below.



MIB(Management Information Base)is a set of variable definitions of devices used to describe the hierarchy of the tree. For the curated object B in the figure above, we can uniquely describe it using a string of numbers <1.2.1.1>. This number string is the object identifier. GPON OLT Support for SNMP V1, V2C, and V3. Common MIB is shown in the table below.

MIB attribute	MIB content	Refer to
Public MIB	MIB II based on TCP/IP	RFC1213
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
Private MIB	VLAN MIB	
	Device management	
	Interface management	

27.3 SNMP Configuration

27.3.1 Configure the Group Name

Start from the privileged configuration mode, configure the group name as shown in the table.

	Command	Function
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**snmp-server community** *name* <ro| rw >	Configure the SNMP community string
Step 3	**show snmp-server community**	Show the SNMP community configuration
Step 5	**exit**	Returns the privileged user configuration mode from the global configuration mode
Step 6	**write**	Save configuration

27.3.2 Configure the Trap Server Address

Use the following command to configure or delete the target host IP address. Start from the privileged configuration mode, configure the trap target host address, as shown in the following table.

	Command	Function
Step 1	**config terminal**	Enter the global configuration mode
Step 2a	**snmp-server host** *A.B.C.D* < community *WORD* |udp-port (1-65535) |version <1|2c|3> >	Configure the trap target host address. Configure the community string value

Step 2b	**no snmp-server host** *A.B.C.D* **version** <1|2c|3> *community_string or user_name*	Remove the trap target host address
Step 3	**write**	Save configuration

27.3.3 Configure Association Information

Start from the privileged configuration mode, configure the association information, as shown in the following table.

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**snmp-server contact** *line*	Configure the contact string value
Step 3	**show snmp-server contact**	Check the SNMP contact configuration
Step 4	**write**	Save configuration

27.3.4 Configure location Information

Start from the privileged configuration mode, configure the location information, as shown in the following table.

	Command	**Function**
Step 1	**config terminal**	Enter the global configuration mode
Step 2	**snmp-server location** *line*	Configure the location string value
Step 3	**show snmp-server location**	Check the SNMP location configuration
Step 4	**write**	Save the configuration.

28. Alarm and Event Management

28.1 Description of Alarms and Events

If you enable alarm reporting, it will trigger an alarm event when the system makes an error or performs some important action. Alarm information will be saved in the buffer; You can run commands such as show syslog to display this. All alerts can be sent to specific service providers. Alarm includes fault alarm and recovery alarm. The fault alert will not go away until the fault is fixed and the alarm cleared. Events include runtime environment and security events, which are notifications that are generated and notified to administrators under normal circumstances. The difference between an event and an alert is that an event is generated under normal conditions, while an alert is generated under abnormal conditions. The "Show Alarm Event Information" command is used to display the description, level, type, and category of all alarms and events.

28.2 Alarm Management

Alert severity levels include major, major, minor, and warning. The corresponding levels in the system logs are Alert, Critical, critical, and Warning. Alarm types include equipment alarm, communication alarm and disposal alarm.

- Device alerts include low temperature, high temperature, CPU usage, memory usage, fans, PON, optical power, and more.
- Communications alarms include port on/down, loopback, PON deregistration, PON registration failure, PON-LOS, ONU deregistration, illegal ONU registration, ONU authorization failure, ONU MAC merge, ONU LOID merge, ONU-link-LOS, ONU dying alarm, ONU link failure, and ONU-link events, ONU extended OAM notifications, etc.
- Clearing an alarm includes upgrade failure, configuration file upload failure, and configuration file download failure.

28.2.1 System Alarm

System alerts show the performance and security of the system. The following table shows a list of system alerts.

System alarm	Reason	Default
temp-high	The device temperature is higher than the threshold	disable

temp-low	The device temperature is lower than the threshold	disable
cpu-usage-high	The CPU usage exceeds the threshold	disable
mem-usage-high	The memory usage exceeds the threshold	disable
fan	Fan switch	disable
download-file-failed	Failed to download file	enable
upload-file-failed	Failed to upload file	enable
upgrade-file-failed	Failed to upgrade firmware	enable
port-updown	Port opening and closing	enable
port-loopback	Port loop	disable

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**alarm** <temp-high|temp-low| cpu-usage-high|mem-usage-high|....> <all|print|record|remote|trap> enable	Enable system alarm reporting
Step 2b	**alarm** <temp-high|temp-low| cpu-usage-high|mem-usage-high|....> <all|print|record|remote|trap> disable	disable system alarm reporting
Step 3	**show alarm configuration**	Displays system alarm configuration

28.2.2 PON Alarm

By monitoring PON alarms, you can eliminate problems caused by PON ports or optical fibers and ensure that the PON works properly. The following table shows a list of PON alerts.

PON alarm	Reason	Default
pon-txpower-high	The send power of the PON port exceeds the threshold	enable
pon-txpower-low	The sending power of the PON port is lower than the threshold	enable

pon-txbias-high	The PON port bias current is higher than the threshold	enable
pon-txbias-low	The bias current of the PON port is lower than the threshold	enable
pon-vcc-high	The PON port voltage is higher than the threshold	enable
pon-vcc-low	The PON port voltage is lower than the threshold	enable
pon-temp-high	The temperature of the PON port exceeds the threshold	enable
pon-temp-low	The PON port temperature is lower than the threshold	enable
pon-los	The optical fiber is not connected or the link is faulty	enable
deregister	PON cancellation	disable
register-failed	PON registration failed	enable

Configure global PON alarms, as shown in the following table.

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**alarm** <pon-register-failed|pon-deregister> <all|print|record|remote|trap> <enable|disable>	Enable or disable PON alarm reporting
Step 2a	**alarm** <pon-txpower-high| pon-txpower-low|pon-txbias-high| pon-txbias-low|pon-vcc-high| pon-vcc-low|pon-temp-high| pon-temp-low| pon-los> <all|print|record|remote|trap> <enable|disable>	Enable or disable PON port alarm reporting
Step 3	**show alarm configuration**	Display alarm configuration

Configure the PON port alarm as shown in the following table. Before doing so, you must enable global PON alerts. By default, global PON alarms are enabled and are recorded in the system log.

Command	**Function**

Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**interface gpon** *slot/port*	The PON interface configuration mode is displayed
Step 3a	**alarm pon optical** <tx_power_high|tx_power_low| tx_bias_high|tx_bias_low|vcc_high|vcc_low| temp_high|temp_low> **disable**	Disable PON port alarm reporting
Step 3b	**alarm pon optical** [tx_power_high|tx_power_low| tx_bias_high|tx_bias_low|vcc_high| temp_high|temp_low] **enable** *alarm-value clear-value*	Enable PON port alarm reporting and configure alarm parameters. Alarm value: alarm threshold. Clear value: Clear threshold.
Step 4	**show alarm pon optical configuration**	Displays PON port alarm configuration

28.2.3 ONU Alarm

ONU alarms can also help administrators troubleshoot ONU faults. The following table shows the list of ONU alarms.

ONU alarm	Reason	Default
onu-deregister	ONU cancellation	enable
onu-link-lost	The ONU optical fiber is not connected or the link is faulty	disable
onu-illegal-register	illegal ONU registration	enable
onu-auth-failed	ONU LOID Authorization Failed in automatic authorization mode or failed due to packet loss.	enable
onu-mac-conflict	The current PON port conflicts with the authorized ONU in the system.	enable
onu-loid-conflict	The current PON port conflicts with the authorized ONU in the system.	enable
onu-critical-event	ONU critical link event	enable
onu-dying-gasp	ONU power failure	enable

onu-link-fault	The ONU link is faulty	enable
onu-link-event	ONU link event	disable
onu-event-notific	ONU extends OAM notifications	enable

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**syslog alarm** <onu-deregister|onu-link-lost| onu-illegal-register|onu-auth-failed| onu-mac-conflict|onu-loid-conflict| onu-critical-event|onu-dying-gasp| onu-link-fault|onu-link-event| onu-event-notific> <all|print|record|remote|trap> <enable|disable>	Enable or disable ONU alarm reporting
Step 3	**show alarm configuration**	Displays system alarm configuration

28.3 Event Management

Severity levels include major, major, minor, and warning. The corresponding levels in the system logs are Alert, Critical, critical, and Warning. Event types include device events, communication events, and dipole events.

- Device events include device restart events and PON events.
- Communication events include PON registration, PON los recovery, ONU registration, ONU search, ONU authorization success, and ONU deregistration success.
- Handle events include configuration events that are saved, erased, downloaded, uploaded, and unencoded.

28.3.1 System Event

System events are used to monitor system performance and security to ensure the normal running of the system.

System event	Reason	Default
reset	Equipment reset	disable
config-save	Save configuration	enable
config-erase	Erase configuration	enable

download-file-success	Download file successfully	enable
upload-file-success	File uploaded successfully	enable
upgrade-file-success	Firmware upgrade successful	enable

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**event reset** <all|print|record|remote|trap> <enable|disable>	Firmware upgrade successful
Step 3	**show alarm-event configuration**	Displays the system event configuration

28.3.2 PON Event

By monitoring PON events, eliminate problems caused by PON ports or optical fibers, and ensure that PON is working properly. The following table shows a list of PON events.

PON event	Reason	Default
pon-register	PON registration	disable
pon-los-recovery	PON LOS recovery	enable

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**syslog event** <pon-register|pon-los-recovery> <all|print|record|remote|trap> <enable|disable> <*all*|print|record|remote|trap>	Enable or disable the syslog event
Step 3	**show alarm-event configuration**	Enable or disable PON event reporting

28.3.3 ONU Event

ONU events can also help administrators troubleshoot some ONU failures. The following table shows the list of ONU events.

ONU event	Reason	Default

onu-register	ONU Registration	enable
onu-link-discover	ONU discovery	disable
onu-auth-success	OLT authorizes ONU to succeed	enable
onu-deauth-success	OLT successfully deauthorized ONU	disable

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2b	**event** <onu-register|onu-link-discover| onu-auth-success|onu-deauth-success|onu-finish|onu-vlan-pool|> <all|print|record|remote|trap> <enable|disable>	Enable or disable ONU event reporting
Step 3	**show alarm-event configuration**	Displays the system event configuration

29. System Log

29.1 Introduction

System logs record the operating status of the entire system and user operations. It helps administrators understand and monitor the working status of the system and record abnormal information. System logs come from all running modules of the system. The log system collects, manages, saves, and displays information. When you need to debug or check the status of the system, it can be displayed in the design, or it can be sent to the server for long-term running status and operation tracking.

29.1.1 Log Type

System log has five types:

- Abnormal information log
  Abnormal information log mainly records the abnormal phenomenon of each module, such as abnormal response, inside state machine error, key process execute error and so on.
- Alarm log
  Alarm log mainly records the information from alarm module. Critical alarm, major alarm, minor alarm and warning are corresponding with alerts, critical, major, warnings log level respectively.
- Event log
  Event log mainly records the information from event module. Critical event, major event, minor event and warning are corresponding with alerts, critical, major, warnings log level respectively.
- Operation log
  Operation log mainly records the informations from CLI and SNMP.
- Debug log
  Debug log mainly records the information from networking debugging, such as received IGMP messages, RSTP BPDU messages, state machine skip and so on.

29.1.2 System Log Level

Syslog information level reference:

Log level	Log contrast
7:emergencies	Abnormal log
6:alerts	Alarm/event log(urgent) Abnormal log

5:critical	Alarm/event log(major) Abnormal log
4:major	Alarm/event log(minor) Abnormal log
3:warnings	Alarm/event log(warning) Abnormal log
2:notifications	Operation log
1:informational	Operation log
0:debugging	Debug log

29.2 Configure System Log

29.2.1 Display System Log

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**syslog flash level** <debug|info|notice| warning|major|critical|alert|emerg>	Displays all system logs or logs of a specific level

29.2.2 Clear System Log

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**clear syslog level** <debug|info|notice| warning|major|critical|alert|emerg>	Clear all system logs or logs of a specific level

29.2.3 Configure System Log Server

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2a	**syslog server** <ip *A.B.C.D*|ipv6 *X:X::X:X*> **port** (1-65535)	Configure the IP address and port number of the system log server.
Step 2b	**no syslog server** <ip|ipv6>	Delete system log server configuration.
Step 3	**show syslog server** [ipv6]	Show system log server configuration.

29.2.4 Configure Storage Level

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**syslog flash level** <debug|info|notice| warning|major|critical|alert|emerg>	System log will be saved to flash if it is higher than you set.
Step 3	**show syslog flash level**	Show system log level in flash.

29.2.5 Save System Logs to the Flash

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**save syslog flash**	Save system log to flash.

29.2.6 Clear System Logs in the Flash

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**clear syslog flash**	Clear system log in flash.

29.2.7 Upload System Log

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 3	**upload tftp syslog** *filename* <*A.B.C.D*|*X:X::X:X*> [format <pdf|txt]	Upload system log to local host byTFTP.

30. SSH Function

You can use SSH to remotely connect to the system via either an out-of-band or in-band management IP address.

30.1 SSH Configuration

30.1.1 Enable the SSH Server

Start from the privileged configuration mode, enable the SSH server of the device, as shown in the following table.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**sshd** <disable|enable|reload>	Shut down, start, and reload the server

30.1.2 Maximum Authentication Times of SSH

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**ip ssh authentication-retries** <(0-6)|default>	Specifies the number of authentication retries

30.1.3 SSH Authentication Timeout Period

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**ip ssh time-out** <(1-120)|default>	Authentication timeout times

30.1.4 Maximum Number of SSH Connections

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**ip ssh max-startups** <(1-5)|default>	Maximum connection number

30.1.5 Maximum Number of SSH Sessions

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**ip ssh max-sessions** <(1-12)|default>	Maximum sessions

30.1.6 SSH Encryption Module

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**crypto key generate rsa usage-keys modulus** (1024-4096)	module

30.2 Display SSH Info

30.2.1 Display SSH Connections

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show ssh**	Show SSH connections

30.2.2 Display The SSH Key

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show crypto key mypubkey** <rsa|ecdsa|ed25519|all>	The SSH key is displayed

30.2.3 Display SSH Configuration

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 3	**show ip ssh**	Show SSH configuration

31. Diagnose Function

31.1 Diagnose Configuration

31.1.1 Network Connection Test

Run the ping command to check the network connection.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**ping** <*IP address or Domain Name|X:X::X:X*>	Network test

31.1.2 Network Tracking Test

Use the traceroute command to check the network connection.

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**traceroute** <*A.B.C.D|X:X::X:X*>	Network tracking

32. TACACS+ Authentication

Terminal Access Controller Access-Control System Plus (TACACS+) is a network protocol used to provide device Access Control and authentication services. It is an enhanced version of TACACS and focuses on Authentication, Authorization, and Accounting (AAA, Authentication, Authorization, and Accounting) services in the field of network security.

32.1 Display TACACS+ Authentication Configuration

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show radius**	The Tacacs+ authentication configuration is displayed

32.2 TACACS+ Authentication Configuration

32.2.1 Enable AAA Authentication

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**aaa authentication enable default group tacacs+**	AAA authentication was enabled.
Step 3	**no aaa authentication enable default**	AAA authentication was disabled.

32.2.2 Enable Login Authentication

Command	Function

Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**tacacs** <console|web> **login**	Login authentication was enabled on the device serial port or web page
Step 3	**no tacacs** <console|web> **login**	Login authentication was disabled on the device serial port or web page.

32.2.3 Configure TACACS+ Server Address

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**tacacs-server host** *A.B.C.D*	The Tacacs+ server address is configured
Step 3	**no tacacs-server host** *A.B.C.D*	Delete the Tacacs+ server address
Step 4	**tacacs key** *shared-key*	Configure Tacacs+ shared keys
Step 5	**no tacacs key**	Example Delete a Tacacs+ shared key

32.2.4 TACACS+ Authentication Settings

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**aaa authentication** <dot1x|enable|login> **default group tacacs+** [enable]	The Tacacs+ authentication mode is configured local: Local authentication is used when the server does not exist none: No authentication is enabled and any password can be used to log in tacacs+: Enables tacacs+

		authentication
Step 3	**no aaa authentication** <login|enable> **default**	Example Delete the Tacacs+ authentication mode

32.2.5 TACACS+ Authorization Settings

	Command	**Function**
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**aaa authorization** <exec|commands> **default group tacacs+** [local]	The Tacacs+ authorization mode is configured local: Local authentication is used when the server does not exist none: No authentication is enabled and any password can be used to log in tacacs+: Enables tacacs+ authentication
Step 3	**no aaa authorization** <exec|command> **default**	Example Delete the Tacacs+ authorization mode
Step 4	**aaa authorization commands** <0|1|15> **default group tacacs+** [local]	Configure Tacacs+ authorization levels 0: Authentication is performed in user mode 1: Authentication is performed in privileged mode 15: Authorization is performed in global mode

32.2.6 TACACS+ Audit Settings

	Command	**Function**
Step 1	**configure terminal**	Enter the global

		configuration mode
Step 3	**aaa accounting exec default start-stop group**	Configure the Tacacs+ audit mode
Step 4	**no aaa accounting exec default**	Example Delete the Tacacs+ audit mode
Step 5	**aaa accounting commands** <0|1|15> **default start-stop group tacacs+**	Configure the Tacacs+ audit level 0: Authentication is performed in user mode 1: Authentication is performed in privileged mode 15: Authorization is performed in global mode

33. RADIUS Authentication

Remote Authentication Dial-In User Service (RADIUS) is a widely used client/server protocol for remote user authentication, authorization, and auditing (AAA). It was originally designed to manage dial-up network access, but has been extended to network services that need to verify user credentials. It uses UDP as the transport protocol and all its information (including passwords) is transmitted in the same channel, which simplifies deployment, while Tacacs+ is able to encrypt each message on a per-message basis, which also means that it is less secure than Tacacs+.

33.1 Display RADIUS Authentication Configuration

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**show radius**	The radius authentication configuration is displayed

33.2 RADIUS Authentication Configuration

33.2.1 Enable AAA Authentication

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**aaa authentication enable default group radius** [enable]	AAA authentication was enabled
Step 3	**no aaa authentication enable default**	AAA authentication was disabled

33.2.2 Enable Login Authentication

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**radius** <console|web> **login**	Login authentication was enabled on the device serial port or web page
Step 3	**no radius** <console|web> **login**	Login authentication was disabled on the device serial port or web page.

33.2.3 Configure RADIUS Server Address

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**radius-server host** *A.B.C.D* **key** *shared-key*	The radius server address and shared key are configured
Step 3	**no radius-server host** *A.B.C.D*	The radius server address and shared key are deleted

33.2.4 RADIUS Authentication Settings

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**aaa authentication** <dot1x|enable|login> **default group radius** [enable]	The radius authentication mode is configured local: Local authentication is used when the server does not exist none: No authentication is enabled and any password can be used to log in radius: Enables radius

	authentication

33.2.5 RADIUS Audit Settings

	Command	Function
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**aaa accounting** <dot1x|exec> **default group radius**	The radius login audit function was enabled
Step 3	**no aaa accounting** <dot1x|exec> **default**	The radius login audit was disabled. Procedure

Thank you!