

**GPON OLT CLI**

**USER MANUAL**

**Version V2.1**

**Release Date 2021-4-25**

**CONTENTS**

[1. Access OLT 11](#_Toc9240224)

[2. Command Line Interface 14](#_Toc9240225)

[2.1 Abstract 14](#_Toc9240226)

[2.2 CLI Configuration Mode 14](#_Toc9240227)

[2.3 CLI Specialities 15](#_Toc9240228)

[2.3.1 Online Help 15](#_Toc9240229)

[2.3.2 Display Specialities 20](#_Toc9240230)

[2.3.3 History Commands 20](#_Toc9240231)

[2.3.4 Error Messages 21](#_Toc9240232)

[2.3.5 Edit Specialities 22](#_Toc9240233)

[3. OLT Management Configuration 24](#_Toc9240234)

[3.1 Configure Outband Management 24](#_Toc9240236)

[3.1.1 Enter AUX Port Configuration Mode 24](#_Toc9240237)

[3.1.2 Outband Management IP address 24](#_Toc9240238)

[3.1.3 Outband Management IPv6 Address 25](#_Toc9240239)

[3.1.4 Show AUX Port Information 26](#_Toc9240240)

[3.2 Configure Inband Management 26](#_Toc9240241)

[3.3 Configure Manangement Gateway 27](#_Toc9240242)

[3.4 Configure DNS 29](#_Toc9240243)

[4. Port Configuration 30](#_Toc9240244)

[4.1 Port Configuration 30](#_Toc9240246)

[4.1.1 Enter Port Configuration Mode 30](#_Toc9240247)

[4.1.2 Enable /Disable Port 30](#_Toc9240248)

[4.1.3 Configure Port Description 31](#_Toc9240249)

[4.1.4 Configure Port Duplex Mode 32](#_Toc9240250)

[4.1.5 Configure Port Speed 33](#_Toc9240251)

[4.1.6 Configure Port Rate Limitation 34](#_Toc9240252)

[4.1.7 Configure Port VLAN Mode 35](#_Toc9240253)

[4.1.8 Configure Hybrid Port VLAN 36](#_Toc9240254)

[4.1.9 Configure Trunk Port VLAN 37](#_Toc9240255)

[4.1.10 Configure Port PVID 38](#_Toc9240256)

[4.1.11 Configure Access Port VLAN 39](#_Toc9240257)

[4.1.12 Configure Port Flow Control 40](#_Toc9240258)

[4.1.13 Configure Port Broadcast Suppression 40](#_Toc9240259)

[4.1.14 Configure Port Multicast Suppression 41](#_Toc9240260)

[4.1.15 Configure Port Unknown Unicast Suppression 42](#_Toc9240261)

[4.1.16 Configure Port Isolation 43](#_Toc9240262)

[4.1.17 Configure Port Loopback 44](#_Toc9240263)

[4.1.18 Configure Port Loopback Detection 45](#_Toc9240264)

[4.1.19 Configure Port Jumboframe 46](#_Toc9240265)

[4.1.20 Show Port Statistics 47](#_Toc9240266)

[4.1.21 Clean Port Statistics 48](#_Toc9240267)

[4.1.22 Show Interface Configurations 48](#_Toc9240268)

[4.2 Example 50](#_Toc9240269)

[5. Port Aggregation Configuration 52](#_Toc9240270)

[5.1 Introduction 52](#_Toc9240272)

[5.2 Port Aggregation Configuration 52](#_Toc9240273)

[5.2.1 Create Static Aggregation Group 52](#_Toc9240274)

[5.2.2 Configure Load Balancing Policy of Group 53](#_Toc9240275)

[5.2.3 Configure Member Port of Group 54](#_Toc9240276)

[6. VLAN Configuration 56](#_Toc9240277)

[6.1 VLAN Configuration 56](#_Toc9240279)

[6.1.1 Create/Delete VLAN 56](#_Toc9240280)

[6.1.2 Configure/Delete VLAN Description 57](#_Toc9240281)

[6.1.3 Configure/Delete IP Address and Mask of VLAN 58](#_Toc9240282)

[6.2 Show VLAN Information 59](#_Toc9240283)

[7. VLAN Translation/QinQ 61](#_Toc9240284)

[7.1 Configure VLAN Translation/QinQ 61](#_Toc9240286)

[7.2 Example 62](#_Toc9240287)

[8. ARP Proxy 63](#_Toc9240288)

[9. MAC Address Configuration 64](#_Toc9240289)

[9.1 Overview 64](#_Toc9240291)

[9.2 Configure MAC Address 65](#_Toc9240292)

[9.2.1 Configure MAC address Table 65](#_Toc9240293)

[9.2.2 Configure MAC Address Aging Time 66](#_Toc9240294)

[9.2.3 Clean MAC Address Table 66](#_Toc9240295)

[9.2.4 Configure Maximum Learnt MAC Enties of Port 67](#_Toc9240296)

[9.3 Show MAC Address Table 67](#_Toc9240297)

[9.3.1 Show MAC Address Table 67](#_Toc9240298)

[9.3.2 Show MAC Address Aging Time 68](#_Toc9240299)

[10. Configure Port Mirroring 69](#_Toc9240300)

[10.1 Configure Mirroring Destination Port 69](#_Toc9240301)

[10.2 Configure Mirroring Source Port 69](#_Toc9240302)

[10.3 Delete Port Mirroring 70](#_Toc9240303)

[11. IGMP Configuration 72](#_Toc9240304)

[11.1 IGMP Snooping 72](#_Toc9240306)

[11.1.1 Enable/Disable IGMP Snooping 72](#_Toc9240307)

[11.1.2 Configure Multicast Data Forwarding Mode 72](#_Toc9240308)

[11.1.3 Configure Port Multicast VLAN 73](#_Toc9240309)

[11.1.4 Configure Multicast Router Port 74](#_Toc9240310)

[11.1.5 Configure Static Multicast 75](#_Toc9240311)

[11.1.6 Configure Fast Leave 75](#_Toc9240312)

[11.1.7 Configure Multicast Group Limit 76](#_Toc9240313)

[11.1.8 Configure Parameters of Special Query 77](#_Toc9240314)

[11.1.9 Configure Parameters of General Query 78](#_Toc9240315)

[11.1.10 Configure Source IP of Query 78](#_Toc9240316)

[11.1.11 Configure Multicast Member Aging Time 79](#_Toc9240317)

[11.1.12 Show Multicast Gourp Information 80](#_Toc9240318)

[11.1.13 Configure Multcast on PON 80](#_Toc9240319)

[11.2 Example 81](#_Toc9240320)

[12. ACL Configuration 84](#_Toc9240321)

[12.1 Overview 84](#_Toc9240323)

[12.2 ACL Confiuration 85](#_Toc9240324)

[12.2.1 IP Standard ACL 85](#_Toc9240325)

[12.2.2 IP Extended ACL 86](#_Toc9240326)

[12.2.3 ACL Based on MAC Address 87](#_Toc9240327)

[12.2.4 ACL Based on Port Binding 89](#_Toc9240328)

[12.2.5 ACL Based on QoS 90](#_Toc9240329)

[12.2.6 ACL Rule Apply to Port 92](#_Toc9240330)

[12.3 Example 93](#_Toc9240331)

[13. QoS Configuration 95](#_Toc9240332)

[13.1 Configure Queue Scheduling Mode 95](#_Toc9240334)

[13.2 Configure Queue Mapping 96](#_Toc9240335)

[14. STP Configuration 98](#_Toc9240336)

[14.1 STP Default Settings 98](#_Toc9240338)

[14.2 Cofigure STP 98](#_Toc9240339)

[14.2.1 Enable STP Function 99](#_Toc9240340)

[14.2.2 Enable Port STP 100](#_Toc9240341)

[14.2.3 Configure Bridge Priority 100](#_Toc9240342)

[14.2.4 Configure Forward Delay 101](#_Toc9240343)

[14.2.5 Configure Hello Time 103](#_Toc9240344)

[14.2.6 Configure Max Aging Time 104](#_Toc9240345)

[14.2.7 Configure Priority of Designated Port 105](#_Toc9240346)

[14.2.8 Configure Path Cost of Designated Port 106](#_Toc9240347)

[14.2.9 Configure Edge Port 107](#_Toc9240348)

[14.2.10 Configure Point to Point Mode 108](#_Toc9240349)

[14.3 Show STP Information 109](#_Toc9240350)

[15. DHCP Management Configuration 110](#_Toc9240351)

[15.1 Configure DHCP Server 110](#_Toc9240352)

[15.2 Configure DHCP Relay 111](#_Toc9240353)

[15.3 Configure DHCP Snooping 113](#_Toc9240354)

[16. L3 Route Configuration 119](#_Toc9240355)

[16.1 L3 Route Configuration 119](#_Toc9240356)

[16.1.1 Hardware Router Table 119](#_Toc9240357)

[16.1.2 Static Route 119](#_Toc9240358)

[16.1.3 Key Chain 120](#_Toc9240359)

[16.2 RIP 121](#_Toc9240360)

[16.2.1 RIP Overview 121](#_Toc9240361)

[16.2.2 RIP Configuration 122](#_Toc9240362)

[16.2.3 RIP Configuration Example 131](#_Toc9240363)

[16.3 OSPF 138](#_Toc9240364)

[16.3.1 OSPF Overview 138](#_Toc9240365)

[16.3.2 OSPF Configuration 139](#_Toc9240366)

[16.3.3 OSPF Configuration Example 150](#_Toc9240367)

[16.4 Manipulate Routing Updates 158](#_Toc9240368)

[16.4.1 Route IP List 158](#_Toc9240369)

[16.4.2 Route Redistribution 164](#_Toc9240370)

[16.4.3 Distribution List Control Routing Updates 168](#_Toc9240371)

[16.4.4 Routing Maps to Control Routing Updates 177](#_Toc9240372)

[16.4.5 Prefix Lists to Filter Routing 183](#_Toc9240373)

[17 IPv6 186](#_Toc9240374)

[17.2 VLAN IPv6 Address 186](#_Toc9240375)

[17.3 IPv6 Static Neighbour 187](#_Toc9240376)

[17.4 IPv6 SLAAC 188](#_Toc9240377)

[17.4.1 IPv6 SLAAC Work Processes 189](#_Toc9240378)

[17.4.2 IPv6 SLAAC Configuration 190](#_Toc9240379)

[17.4.3 Example(pending) 195](#_Toc9240380)

[17.5 DHCPv6 195](#_Toc9240381)

[17.5.1 DHCPv6 Overview 195](#_Toc9240382)

[17.5.2 DHCPv6 Server 198](#_Toc9240383)

[17.5.3 DHCPv6 Relay 207](#_Toc9240384)

[17.6 IPv6 Route 212](#_Toc9240385)

[17.6.1 IPv6 Static Route Configuration 212](#_Toc9240386)

[17.6.2 View IPv6 Hardware Routing Information 213](#_Toc9240387)

[17.7 IPv6 Connectivity Test 214](#_Toc9240388)

[18 PON Management 215](#_Toc9240389)

[18.2 Show PON Port Info and Optical Power 215](#_Toc9240391)

[18.2.1 Show Pon Port Statistics 215](#_Toc9240392)

[18.2.2 Show PON Port Optical Power 215](#_Toc9240393)

[18.2.3 Show ONU Optical Transceiver 216](#_Toc9240394)

[18.3 PON Port Configuration 216](#_Toc9240395)

[18.3.1 Enable/Disable PON 216](#_Toc9240396)

[17.1 ONU auto-learn configuration 218](#_Toc9240397)

[19 ONU Management 219](#_Toc9240398)

[19.2 ONU Basic Configuration 219](#_Toc9240400)

[19.2.1 Show Auto-find ONU 219](#_Toc9240401)

[19.2.2 ONU Automatic Authorize 219](#_Toc9240402)

[19.2.3 Show ONU Authorized Info 220](#_Toc9240403)

[19.2.4 Show ONU Authorized Detail-info 220](#_Toc9240404)

[19.2.5 Activate|Deactivate ONU 221](#_Toc9240405)

[19.2.6 ONU Authorization 221](#_Toc9240406)

[19.2.7 Configure ONU Description String 222](#_Toc9240407)

[19.3 ONU Remote Configuration 223](#_Toc9240408)

[19.3.1 Show ONU SFP Info 223](#_Toc9240409)

[19.3.2 Upgrade ONU 223](#_Toc9240410)

[19.3.3 Auto-upgrade ONU 225](#_Toc9240411)

[19.3.4 Reboot ONU 225](#_Toc9240412)

[19.3.5 TCONT Configuration 226](#_Toc9240413)

[19.3.6 GEMPORT Configuration 227](#_Toc9240414)

[19.3.7 ONU Service Configuration 228](#_Toc9240415)

[19.3.8 Service-port Configuration 229](#_Toc9240416)

[19.3.9 ONU UNI Configuration 231](#_Toc9240417)

[19.3.10 ONU FEC Configuration 233](#_Toc9240418)

[19.3.11 Show ONU Service 233](#_Toc9240419)

[19.3.12 Show ONU Capability 233](#_Toc9240420)

[19.4 ONU Remote Port Configuration 234](#_Toc9240421)

[19.4.1 ONU Port Enable|Disable 234](#_Toc9240422)

[19.4.2 ONU Port Autonegotiation 234](#_Toc9240423)

[19.4.3 ONU Port Flow Control Configuration 235](#_Toc9240424)

[19.4.4 Multicast VLAN Configuration 235](#_Toc9240425)

[19.4.5 Configure ONU Iphost 236](#_Toc9240426)

[19.4.6 ONU Port Multicast Tag-strip Configuration 237](#_Toc9240427)

[19.4.7 Example for SFU 237](#_Toc9240428)

[19.4.8 Example for HGU 239](#_Toc9240429)

[19.5 Rogue-onu Configuration 242](#_Toc9240430)

[19.5.1 Rogue-onu-detect 242](#_Toc9240431)

[19.5.2 Rogue-onu status 243](#_Toc9240432)

[20 ONU Template Management 244](#_Toc9240433)

[20.2 Summary of ONU Template 244](#_Toc9240435)

[20.3 ONU Template Configuration 245](#_Toc9240436)

[20.4 DBA Template Configuation 246](#_Toc9240437)

[20.5 Traffic Template Configuation 248](#_Toc9240438)

[20.6 Line Template Configuation 249](#_Toc9240439)

[20.7 Service Template Configuation 253](#_Toc9240440)

[20.8 Alarm Threshold Template Configuration 255](#_Toc9240441)

[20.9 Show/Delete Profile Configuration 256](#_Toc9240442)

[21 ONU Auto-learn Configuration 257](#_Toc9240444)

[21.2 ONU Auto-learn 257](#_Toc9240446)

[21.3 Enable Auto-learn 258](#_Toc9240447)

[22 System Management 259](#_Toc9240448)

[22.2 Configuration Management 259](#_Toc9240453)

[22.2.1 Save Configurations 259](#_Toc9240454)

[22.2.2 Erase Configurations 259](#_Toc9240455)

[22.2.3 Show Startup Configurations 260](#_Toc9240456)

[22.2.4 Show Running Configurations 260](#_Toc9240457)

[22.2.5 Upload/Download Configuration File 260](#_Toc9240458)

[22.3 Check System Information 261](#_Toc9240459)

[22.3.1 Check System Running Information 261](#_Toc9240460)

[22.3.2 Check Version Information 261](#_Toc9240461)

[22.3.3 Check System Running Time 262](#_Toc9240462)

[22.4 System Basic Configurations 262](#_Toc9240463)

[22.4.1 Configure System Name 262](#_Toc9240464)

[22.4.2 Configure Terminal Display Attribute 263](#_Toc9240465)

[22.4.3 Configure Terminal Time-out Value 263](#_Toc9240466)

[22.5 System Basic Operations 264](#_Toc9240467)

[22.5.1 Upgrade System 264](#_Toc9240468)

[22.5.2 Network Connectivity Test 265](#_Toc9240469)

[22.5.3 Reboot System 265](#_Toc9240470)

[22.5.4 Telnet 265](#_Toc9240471)

[22.5.5 Configure RTC System Time 266](#_Toc9240472)

[22.5.6 NTP Client 266](#_Toc9240473)

[22.5.7 Timezone Configuration 267](#_Toc9240474)

[22.5.8 Fan Control 267](#_Toc9240475)

[22.6 Debug Information 268](#_Toc9240476)

[22.6.1 Enable/Disable CPU Debug Information 268](#_Toc9240477)

[22.6.2 Enable/Disable Functional Module Debug Information 269](#_Toc9240478)

[23 User Management 270](#_Toc9240479)

[23.2 User Privilege 270](#_Toc9240481)

[23.3 Default User 270](#_Toc9240482)

[23.4 Add User Account 270](#_Toc9240483)

[23.5 Show User Account List 271](#_Toc9240484)

[23.6 Delete User Account 271](#_Toc9240485)

[23.7 Modify Password 271](#_Toc9240486)

[24 SNMP Configuration 273](#_Toc9240487)

[24.2 SNMP Introduction 273](#_Toc9240488)

[24.3 SNMP Version and MIB 273](#_Toc9240489)

[24.4 SNMP Configuration 275](#_Toc9240490)

[24.4.1 Configure Community 275](#_Toc9240491)

[24.4.2 Configure Trap Server Address 275](#_Toc9240492)

[24.4.3 Configure Contact Information 276](#_Toc9240493)

[24.4.4 Configure Location Information 277](#_Toc9240494)

[25 Alarm and Event Management 278](#_Toc9240495)

[25.2 Alarm and Event Introduction 278](#_Toc9240497)

[25.3 Alarm Management 278](#_Toc9240498)

[25.3.1 System Alarms 279](#_Toc9240499)

[25.3.2 PON Alarms 281](#_Toc9240500)

[25.3.3 ONU Alarms 283](#_Toc9240501)

[25.4 Event Management 285](#_Toc9240502)

[25.4.1 System Events 286](#_Toc9240503)

[25.4.2 PON Events 287](#_Toc9240504)

[25.4.3 ONU Events 287](#_Toc9240505)

[26 System Log 289](#_Toc9240506)

[26.2 System Log Introduction 289](#_Toc9240508)

[26.2.1 Log Type 289](#_Toc9240509)

[26.2.2 System Log Level 290](#_Toc9240510)

[26.3 Configure System Log 291](#_Toc9240511)

[26.3.1 Show System Log 291](#_Toc9240512)

[26.3.2 Clear System Log 291](#_Toc9240513)

[26.3.3 Configure System Log Server 292](#_Toc9240514)

[26.3.4 Configure Save Level of System Log 292](#_Toc9240515)

[26.3.5 Save System Log to Flash 293](#_Toc9240516)

[26.3.6 Clear System Log in Flash 293](#_Toc9240517)

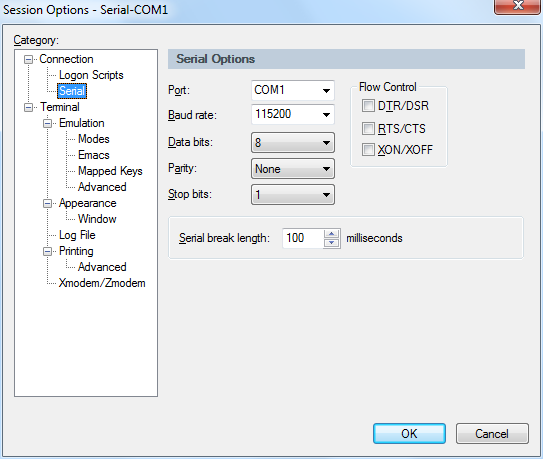
[26.3.7 Upload System Log 293](#_Toc9240518)

# Access OLT

You can access OLT by CLI (Command Line Interface) via console cable or telnet. This charpter 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.

# Command Line Interface

## Abstract

GPON 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 “?”.

## 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** |

## CLI Specialities

### Online Help

GPON 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

1. 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.

1. 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.

<6000-6999> Port quality of service access list.

<7000-7999> Port Ipmc Vlan translation of service access list.

1. Input a character string end with “?”, it will display all key words that Begin at 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

1. Input a command and a character string end with “?”, it will display all key words Begin at this character sring.

gpon-olt (config)# show ver

version show version command.

1. Input a character string end with “Tab”, it will display completely key words that Begin at this character string when it is unique.

### Display Specialities

GPON OLT CLI provides the following display specialities. 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 |

### 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. |

### 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 |

### Edit Specialities

CLI provides basic edit function. Every command supports maxum 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. |

# OLT Management Configuration



## Configure Outband Management

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

### Enter AUX Port Configuration Mode

Begin at 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. |

### Outband Management IP address

Begin at 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> net-mask* | 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. |

### Outband Management IPv6 Address

Begin at 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> [eui-64]* | Configure IPv6 addressand 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. |

### Show AUX Port Information

Begin at 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. |

## Configure Inband Management

This device provides inband management which can be managed from uplink port.

Begin at 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> net-mask* | Configure IP address and mask. |
| **Step 5b** | **no ip address** *<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. |

## Configure Manangement Gateway

When OLT management IP and management server are not in the same network segment, it needs to configure a gateway.

Begin at 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 0.0.0.0/0** <*A.B.C.D>* | Configure management gateway. |
| **Step 3** | **no ip route 0.0.0.0/0** <*A.B.C.D>* | Delete management gateway. |
| **Step 4** | **show ip route** | Show management gateway configuration. |
| **Step 5** | **write** | Save configurations. |

## Configure DNS

It can configure two DNS server

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **ip dns** <*A.B.C.D> {<A.B.C.D>}* | Configure DNS |
| **Step 3** | **show ip dns** | Show management gateway. |
| **Step 4** | **write** | Save configurations. |

# Port Configuration



## Port Configuration

### Enter Port Configuration Mode

Begin at 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. |

### 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.

Begin at 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. |

### Configure Port Description

This command is used to configure port description. There is no description by default.

Begin at 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. |

### 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.

Begin at 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. |

### 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.

Begin at 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. |

### Configure Port Rate Limitation

Begin at 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} bps** *value* | Configure port rate limitation. Value range: 64-1000000, 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. |

### 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.

Begin at 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.

### 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.

Begin at 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.

### Configure Trunk Port VLAN

Trunk mode port can belong to several VLAN. It is usually used to connect with switches routers.

Begin at 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.

### Configure Port PVID

Only under hybrid mode and trunk mode can set up PVID.

Begin at 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. |

### Configure Access Port VLAN

Only one untagged mode VLAN can be set to access port. Port’s PVID is the same as VLAN ID.

Begin at 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. |

### Configure Port Flow Control

Begin at 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. |

### Configure Port Broadcast Suppression

Begin at 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 bps** *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. |

### Configure Port Multicast Suppression

Begin at 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 bps** *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. |

### Configure Port Unknown Unicast Suppression

Begin at 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 unicast bps** *value* | Configure unknown unicast suppression.  Value range: 64-1000000, it should be integral multiple of 64kbps. |
| **Step 3b** | **no storm-control unicast** | 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. |

### 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.

Begin at 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 port** | Show isolation group. |
| **Step 6** | **write** | Save configurations. |

### Configure Port Loopback

Begin at privileged configuration mode, configure port loopback 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** | **loopback [internal | external | outside]** | Internal means cpu inner loopback.  External means cpu outer loopback.  Outside means external data loopback. |
| **Step 4** | **exit** | Exit to global configuration mode. |

**Notice:**

When testing port loopback function, please disable port loopback detection. Please refer to 3.1.18.

### Configure Port Loopback Detection

Begin at privileged configuration mode, configure port loopback detection 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** | **no loopback detect** | Disable port loopback detection. |
| **Step 3** | **show loopback detect** | Show port loopback detection status. |
| **Step 4** | **exit** | Exit to global configuration mode. |

### Configure Port Jumboframe

Begin at 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. |

### Show Port Statistics

Begin at 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. |

### Clean Port Statistics

Begin at privileged configuration mode, clean port statistics as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show interface** *{interface\_type slot/port}* | Show port statistics. | |
| **Step 3** | **clean statistics** | Clean port statistics. |

### 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.

For example, display configurations of uplink port 5.

gpon-olt (config)# show interface gigabitethernet 0/5

Interface gigabitEthernet0/5's information.

GigabitEthernet0/5 current state : Down

Hardware Type is Gigabit Ethernet, Hardware address is 0:0:0:0:0:0

The Maximum Transmit Unit is 1500

Media type is twisted pair, loopback not set

Port hardware type is 1000Base-TX

Link speed type: autonegotiation, Link duplex type: autonegotiation

Current link state: Down

Current autonegotiation mode: enable

Current link speed: 1000Mbps, Current link mode: half-duplex

Flow Control: disable MDIX Mode: force

The Maximum Frame Length is 1536

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 learn state : enable, no limit

Port priority: 0

PVID: 1

Port combo mode: null

Isolate member : yes

Port link-type: hybrid

Untagged VLAN ID: 1

Tagged VLAN ID : 100

Last 300 seconds input: 0 packets 0 bytes

Last 300 seconds output: 0 packets 0 bytes

Input(total): 1113473691 packets, 4081075466 bytes

0 broadcasts, 1113473687 multicasts

Input(normal): 1113473691 packets, 4081075466 bytes

0 broadcasts, 1113473687 multicasts, 0 pauses

Input: 0 input errors, 0 runts, 0 giants, 0 throttles, 4 CRC

0 overruns, 0 aborts, 0 ignored, 0 parity errors

Output(total): 4371 packets, 351860 bytes

1280 broadcasts, 3091 multicasts, 0 pauses

Output(normal): 4371 packets, 351860 bytes

1280 broadcasts, 3091 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

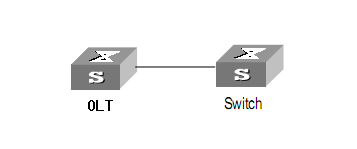
## Example

Configure VLAN and broadcast suppresstion 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 5.1.1.

(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 pps 64

# Port Aggregation Configuration



## 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.

## Port Aggregation Configuration

### Create Static Aggregation Group

At most 4 groups can be created. You can add 4 member ports altogether in every group and at most 4 ports will come into being aggregation at the same time.

Every group is defined as a channel group; the commands are centre on channel group.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **channel-group** *<1-4>* **mode static** | Create static aggregation group. |
| **Step 2b** | **no channel-group** *<1-4>* | Delete static aggregation group. |
| **Step 3** | **show channel-group summary** | Show static aggregation group configuration. |

### 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** *<1-4>* **load-balance {smac|dmac|sdmac|sip|dip|sdip}** | Specify which link is used to transmit traffic in aggregation group. |
| **Step 3** | **show channel-group summary** | Show aggregation configurations. |

### Configure Member Port of Group

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface** *{interface\_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **channel-group** *<1-4>* | Add current port to specific channel group. |
| **Step 3b** | **no channel-group** *<1-4>* | Delete current port from specific channel group. |
| **Step 4** | **exit** | Exit global configuration mode. |
| **Step 5** | **show channel-group summary** | Show aggregation gourp configurations. |

# VLAN Configuration



## VLAN Configuration

VLAN configuration mainly contains:

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

### Create/Delete VLAN

Begin at 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 4a** | **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 4b** | **show vlan** | Show information of all existed VLAN. |
| **Step 5** | **write** | Save configurations. |

### Configure/Delete VLAN Description

Begin at 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** | **interface 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”. | | |

### Configure/Delete IP Address and Mask of VLAN

Begin at 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> net-mask* | Configure IP address and mask of VLAN. |
| **Step 3b** | **no ip address** *<A.B.C.D>* | 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. |

## 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 in vlan 100

Vlan ID : 100

Name : vlan100

Mac address : 00:90:4c:06:a5:73

Tagged Ports : gpon0/1

Untagged Ports : ge0/8

**Notice**:

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

Vlan ID : 1

Name : vlan1

Mac address : 00:90:4c:06:a5:73

Tagged Ports :

Untagged Ports : ge0/1 ge0/2 ge0/3 ge0/4 ge0/5 ge0/6 ge0/7 ge0/8

ge0/9 ge0/10 ge0/11 ge0/12

gpon0/1 gpon0/2 gpon0/3 gpon0/4 gpon0/5 gpon0/6 gpon0/7 gpon0/8

# VLAN Translation/QinQ



## Configure VLAN Translation/QinQ

Begin at 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-maping** *ori\_vlan* **{any|** *ori\_vlan\_pri***}** *tra\_vlani* **{any|tra\_vlan\_pri} {db-tag|one-tag}** | Configure VLAN translation/QinQ.  db-tag means QinQ.  one-tag means translation. |
| **Step 3b** | **no dot1q-tunnel vlan-maping** *ori\_vlan**tra\_vlanid* | Delete VLAN translation/QinQ. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show vlan vlan-maping interface** *{interface\_type slot/port}* | Show VLAN translation/QinQ configurations. |
| **Step 6** | **write** | Save configurations. |

## Example

**(1)VLAN translation function**

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)# vlan-mapping 100 1 200 2 one-tagged

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

**(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)# vlan-mapping 300 3 400 4 db-tagged

gpon-olt (config)#show vlan vlan-mapping interface gigabitethernet 0/2

# ARP Proxy

In order to achieve interconnection between ONU in the same PON, the devices added the ARP Proxy function.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **interface vlan** *vlan\_id* | Create vlan and enter to vlan interface |
| **Step 3a** | **ip proxy-arp** | Enable ARP Proxy |
| **Step 3b** | **no ip proxy-arp** | Disable ARP Proxy |

# MAC Address Configuration



## 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.

## Configure MAC Address

MAC address management includes:

* Configure MAC address table
* Configure MAC address aging time

### Configure MAC address Table

You can add static MAC address entries, delete MAC address entries or clean MAC address table.

Begin at 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** *interface\_type slot/port* | Add static MAC address entry. |
| **Step 2b** | **no mac address-table vlan** *vlan\_id xxxx:xxxx:xxxx* | Delete MAC address entry. |
| **Step 2c** | **mac address-table clean** | Clean MAC address table. |
| **Step 3** | **show mac address-table** | Show MAC address table. |
| **Step 4** | **write** | Save configurations. |

### 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.

Begin at 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 agingtime** *value* | Configure MAC address aging time, range is 10-1000000s.  0s means don’t aging.  Default is 300s. |
| **Step 3** | **show mac address-table agingtime** | Show aging time. |
| **Step 4** | **write** | Save configurations. |

### Clean MAC Address Table

Begin at privileged configuration mode, clean MAC address table as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **mac address-table clean** | Clean MAC address table. |

### Configure Maximum Learnt MAC Enties of Port

Begin at 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. |

## Show MAC Address Table

### Show MAC Address Table

Begin at 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 basedon 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. |

### Show MAC Address Aging Time

Begin at 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 agingtime** | Show MAC address aging time. |

# 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.

## Configure Mirroring Destination Port

Begin at 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** *interface\_type**interface\_num* | Confire mirroring destination port.  Session number is 1~4. |
| **Step 3** | **show monitor session all** | Show mirroring configurations. |
| **Step 4** | **write** | Save configurations. |

## 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.

Begin at 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** *session\_number* **source interface** *interface\_type**start\_interface\_num* [ **-** *end\_interface\_num* **]** {**both|rx|tx**} | Configure mirroring source port.  session\_number is 1-4.  **Both** means received data and transmitted data.  **rx** means received data.  **tx** means transmitted data. |
| **Step 3** | **show monitor session all** | Show mirroring configurations. |
| **Step 4** | **write** | Save configurations. |

## Delete Port Mirroring

Begin at 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** *session\_number* **{[destination | source] interface** *interface\_type**slot/port***}** | Delete port mirroring. session\_number is 1-4 |
| **Step 3** | **show monitor session all** | 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

# IGMP Configuration



## IGMP Snooping

### Enable/Disable IGMP Snooping

IGMP snooping is disabled by default. You should enable by the following command.

Begin at 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. |

### Configure Multicast Data Forwarding Mode

Begin at 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** *vlan-id* **mode { flood ｜ forward ｜ strict-forward}** | Configure multicast data forwarding mode. |
| **Step 3** | **write** | Save configurations. |

### Configure Port Multicast VLAN

After add VLAN to the port, you should also configure multicast VLAN for multicast service. Begin at 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** *{interface\_type slot/port}* | Enter interface configuration mode. | |
| **Step 3a** | **ip igmp snooping user-vlan vlan\_id group-vlan vlan\_id { tagged | untagged }** | Configure port multicast VLAN.  VLAN range is 1-4094. |
| **Step 3b** | **no ip igmp snooping group-vlan** *vlan\_id* | 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. |

### Configure Multicast Router Port

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

Begin at 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** *vlan-id* **interface** *{interface\_type slot/port}* | Configure multicast router port. |
| **Step 2b** | **no ip igmp snooping mrouter vlan** *vlan-id* **interface** *{interface\_type slot/port}* | Delete multicast router port. |
| **Step 3** | **show ip igmp-snooping mrouter vlan all** | Show multicast router mode configuration. |
| **Step 4** | **write** | Save configurations. |

### Configure Static Multicast

Begin at 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** *vlan-id**<A.B.C.D>* **interface** *interface-id* | Configure static multicast. |
| **Step 2b** | **no ip igmp snooping static vlan** *vlan-id <A.B.C.D>* **interface** *interface-id* | Delete static multicast. |
| **Step 3** | **show ip igmp-snooping configuration** | Show IGMP configurations. |
| **Step 4** | **write** | Save configurations. |

### Configure Fast Leave

Begin at privileged configuration mode, configure fast leave 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** | **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. |

### Configure Multicast Group Limit

Begin at 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** *{interface\_type 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. |

### Configure Parameters of Special Query

Begin at 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** *<1-255>* | Configure specific query response time. Default is 1s. |
| **Step 3** | **show ip igmp snooping configuration** | Show IGMP configurations. |
| **Step 4** | **write** | Save configurations. |

### Configure Parameters of General Query

Begin at 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. |

### Configure Source IP of Query

Begin at 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. |

### 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.

Begin at 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 host-aging-time** *seconds* | 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. |

### 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** *[vlan-id |* **all***]* | Show multicast group information. |
| **Step 2b** | **show ip igmp snooping statistic** | Show multicast statistic. |

### Configure Multcast on PON

Include the way to process unknown-mcast and igmp

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode |
| **Step 2a** | **ip igmp snooping mvlan** *<1-4094>* **unknown-mcast** *[forward|drop]* **igmp** *[forward|trap-to-cpu]* | Configurate the way to process mvlan and unknown multcast. |

## 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.

* + - 1. **Framework**



* + - 1. **Steps**

(1)Create VLAN

gpon-olt (config)# vlan 100

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

(2)Configure multcast VLAN100

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

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

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

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

gpon-olt (config-pon-0/1)# switchport hybrid vlan 100 tagged

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 multcast and igmp rule

gpon-olt(config)# ip igmp snooping mvlan 100 unknown-mcast drop igmp trap-to-cpu

(6)Configure the onu

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

gpon-olt(config-pon-0/1)# onu add 1 profile 1GE sn GPON00000031

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

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

gpon-olt(config-pon-0/1)# onu 1 service 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 hybrid def\_vlan 100

gpon-olt(config)#ip igmp snooping mvlan 100

gpon-olt(config)#ip igmp snooping mvlan 100 receive-port gpon-onu\_1/1/2:1 vport 1

gpon-olt(config)#ip igmp snooping mvlan 100 group 224.1.1.1 to 224.1.1.10 static-port gpon-onu\_1/1/2:1 vport 1

# ACL Configuration



## 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 | Maxium 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 |
| ACL based on QoS | 6000-6999 | 1000 |

## ACL Confiuration

ACL configuration mainly includes:

* IP Standard ACL.
* IP Extended ACL.
* ACL based on MAC address
* ACL based on port binding.
* ACL based on QoS.
* ACL rule apply to port.

### IP Standard ACL

Begin at 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>* [*net-mask*]  **subset ip (permit|deny) host** *<A.B.C.D>*  **subset ip [permit|deny] 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 [***access-list-number |* **all]** | Show ACL configurations. |
| **Step 6** | **write** | Save configurations. |

### IP Extended ACL

Begin at 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> net-mask* {*<A.B.C.D> net-mask* | **host** *<A.B.C.D>**|* **any** }[**match** {**dscp** *priority*| **precedence** *priority* | **tos** *priority*}] [**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** | **no access-list** *access-list-index* | Delete ACL |
| **Step 4** | **exit** | Exit global configuration mode. |
| **Step 5** | **show access-list [***access-list-number |* **all** ] | Show ACL configurations. |
| **Step 6** | **write** | Save configurations. |

### ACL Based on MAC Address

Begin at privileged configuration mode, configure ACL based on MAC address 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>}\*1 {[vlan] <1-4094>}\*1 {[cos] <0-7>}\*1 {[ethernet-type] <XXXX> <XXXX> | Configure IP extended ACL rule. |
| **Step 3b** | **no access-list** *access-list-index* | Delete ACL |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show access-list [***access-list-number |* **all]** | Show ACL configurations. |
| **Step 6** | **write** | Save configurations. |

### ACL Based on Port Binding

This type of ACL includes the other types.

Begin at privileged configuration mode, configure ACL based on port binding 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:5000-5999; |
| **Step 3a** | **subset port-business [permit|deny] {src-ip |dest-ip | protocol | tos-dscp | src-mac | dest-mac | vlan | cos | ethernet-type | src-port | dest-port}** | Permit:Permit data stream which match the rule passing through.  Deny:Do not permit data stream which match the rule passing through.  src-ip : source IP address  dest-ip:destination IP address  protocol:IP protocol type  tos-dscp:IP priority  src-mac:source MAC address  dest-mac:destination MAC address  vlan:VLAN IAD  cos:802.1p priority  ethernet-type:ethernet type  src-port:Layer 4 source port  dest-port:Layer 4 destination port |
| **Step 3b** | **no access-list** *access-list-index* | Delete ACL |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show access-list** *access-list-number* | Show ACL configurations. |
| **Step 6** | **write** | Save configurations. |

### ACL Based on QoS

Begin at privileged configuration mode, configure ACL based on QoS 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:6000-6999. |
| **Step 3a** | **subset qos <0-8> <0-7> <1-12>** | <0-8>: output priority  <0-7>: output queue  <1-12>: rule priority |
| **Step 3b** | **subset qos {src-ip |dest-ip | protocol | tos-dscp | src-mac | dest-mac | vlan | cos | ethernet-type | src-port | dest-port}** | src-ip : source IP address  dest-ip: destination IP address  protocol: IP protocol type  tos-dscp: IP priority  src-mac: source MAC address  dest-mac: destination MAC address  vlan: VLAN ID  cos:802.1p priority  ethernet-type: Ethernet type  src-port:Layer 4 source port  dest-port:Layer 4 destination port |
| **Step 3c** | **no access-list** *access-list-number* | Deleting ACL rule. Only the ACL that have not been applied can be deleted. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show access-list** *access-list-number* | Show ACL configurations. |
| **Step 6** | **write** | Save configurations. |

### ACL Rule Apply to Port

Begin at privileged configuration mode, apply ACL rule to port as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter globle configuration mode. |
| **Step 2** | **interface** *{interface\_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **ip access-group** *access-list-number* **in** | Apply ACL rule to port. |
| **Step 3b** | **no ip access-group** *access-list-number*  **in** | Delete ACL rule from port. |
| **Step 4** | **exit** | Exit to glogbal configuration mode. |
| **Step 5** | **show access-list** *access-list-number* | Show ACL configurations. |
| **Step 6** | **write** | Save configurations. |

## Example

**(1)Deny specific IP address packets passing through**

PON1 denies packets which source IP is 192.168.100.10 passing through.

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)Permit specific MAC address packets passing through**

PON1 permits IP packets which source MAC is b8:97:5a:72:37:8d passing through.

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

# QoS Configuration



## Configure Queue Scheduling Mode

Queue scheduling mode contains strict priority, weighted round robin and hybrid mode. This device supports 8 queues altogether.

Begin at privileged configuration mode, configure queue scheduling mode as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **queue-scheduler strict-priority** | Configure strict priority scheduling mode. |
| **Step 2b** | **queue-scheduler wrr** [*queue0 queue1 queue2 queue3 queue4 queue5 queue6 queue7*] | Configure weighted round robin scheduling mode.  *Queue*x is weight of queue x, range is 1-127.  By default, weights of queue 0~7 are 1, 1, 2, 2, 4, 4, 8, 8. |
| **Step 2c** | **queue-scheduler sp-wrr [***queue0 queue1 queue2 queue3 queue4 queue5 queue6 queue7***]** | Configure hybrid scheduling mode.  *Queue*x is weight of queue x, range is 0-127. If it is set to be 0, the queue is strict priority queue.  By default, weights of queue 0~7 are 1, 1, 2, 2, 4, 4, 8, 8. |
| **Step 3** | **show queue-scheduler** | Show queue scheduling configurations. |
| **Step 4** | **write** | Save configurations. |

## Configure Queue Mapping

Begin at privileged configuration mode, configure queue mapping as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **queue-scheduler tc** *priority* **queue** *queue* | Configure mapping relation between queues and priority.  By default, priority 0~7 maps to queue 0~7 respectively. |
| **Step 3** | **show queue-scheduler priority mapping** | Show queue mapping. |
| **Step 4** | **write** | Save configurations. |

# STP Configuration



## 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 |

## Cofigure STP

STP configurations mainly contain:

* Enable device’s STP function.
* Enable port’s STP function.
* Configure STP mode.
* Configure bridge priority of device.
* Configure forward delay of device.
* Configure hello time of device.
* Configure max age of designated device.
* Configure priority of designated port.
* Configure path cost of designated port.

### Enable STP Function

Begin at privileged configuration mode, enable device’s STP function as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **spanning-tree on** | Enable device’s STP function.  By default, STP function is disabled. |
| **Step 2b** | **no spanning-tree** | Disable device’s STP function. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | Save configurations. |

### Enable Port STP

In order to work flexibly, you can disable some specific ports’ STP function.

Begin at privileged configuration mode, enable port’s STP function 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** | **spanning-tree on** | Enable port’s STP function. |
| **Step 3b** | **no spanning-tree on** | Disable port’s STP function. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show spanning-tree interface** *{interface\_type slot/port}* | Show port’s STP configurations. |
| **Step 6** | **write** | Save configurations. |

### Configure Bridge Priority

Device’s bridge priority decides if it will be selected as root of spanning tree.

Begin at privileged configuration mode, configure device’s bridge prority as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree priority** *bridge-priority* | Configure device’s bridge priority.  Priority range is 0~65535, default is 32768. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | Save configurations. |

### Configure Forward Delay

Network will recompute spanning tree when there is link down in network. Construction of spanning tree will be changed too. But the new STP PDU can’t go the rounds of network. In this case, a temporary loop will come out if the new root port and designated port forward data immediately. So, STP adopts state transition mechanism. Before re-forwarding data, root port and designated port will undergo an intermediate state. After forward delay time out in the intermediate state, the new STP PDU have gone the rounds of network, then root port and designated port begin to forward data.

Begin at privileged configuration mode, configure device’s forward delay as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree forward-time** *seconds* | Configure device’s forward delay.  bridge-priority range is 4~30, default is 15. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | Save configurations. |

Forward Delay has something to do with that how big the network is. Generally, the bigger the network, the longer forward delay should be configured. If forward delay is too small, there may be temporary redundant path; while it is too big, network will take more time to resume connectivity. We suggest using default value if you have no idea about this.

|  |
| --- |
| **Notice:**  Hello time, forward delay and maximum age are time parameters of root device. These three parameters should meet the following formula, otherwise, the network will not stable.  2 × (forward-delay －1) >= maximum-agemaximum-age >= 2 × (hello + 1)  The unit of “1” in formula is second. |

### Configure Hello Time

Network Bridge will send hello message to other surrounding network bridge at regular intervals for verifying link connectivity. A suitable hello time can ensure a device find link failure in time and not occupy more network resource. If hello time is too big, device will be in mistake for link failure when loss packets. Then network device recomputes spanning tree. While if too small, network device sends repeated STP PDU frequently. This will increase device’s load and waste network resource.

Begin at privileged configuration mode, configure device’s hello time as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree hellotime** *seconds* | Configure device’s hello time.  Hello time range is 1~10, default is 2. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | Save configurations. |

### Configure Max Aging Time

Max age time is maximum life time of configuration message. When message age is biger than maximum age, configuration message will be discarded.

Begin at privileged configuration mode, configure maximum age as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree max-age** *seconds* | Configure maximum age of device.  max age range is 6-40, default is 20. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | Save configurations. |

### Configure Priority of Designated Port

Port priority decides whether it can be selected as root port or not. On equal conditions, the higher priority port will be selected as root port. Generally, the priority value is smaller, the port has higher priority. If all ports’ priority value are the same, their priority decided by their port index.

Begin at privileged configuration mode, configure priority of designated 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** | **spanning-tree port-priority** *priority* | Configure priority of designated port.  priority range is 1-255, default is 128. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show spanning-tree interface** *{interface\_type slot/port}* | Show port STP configurations. |
| **Step 6** | **write** | Save configurations. |

### Configure Path Cost of Designated Port

Path Cost is related to the speed of the link connected to the port. On the STP switch, a port can be configured with different path costs.

Begin at privileged configuration mode, configure path cost of designated 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** | **spanning-tree cost** *value* | Configure path cost of designated port.  Path cost range is 1-65535, default is auto. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show spanning-tree interface** *{interface\_type slot/port}* | Show port STP configurations. |
| **Step 6** | **write** | Save configurations. |

### Configure Edge Port

The port which connects with terminal host is Edge Port. In process of spanning tree recomputation, edge port can transfer to forwarding status derectly so that it can reduce transfer time. Because RSTP can’t detect whether the port is edge port or not, if the port doesn’t connect with switch, you’d better configure it as edge port. But when the port connects with a switch, RSTP can detect and configure it as non-edge port. By default, all ports are configured as non-edged port.

Begin at privileged configuration mode, configure edge 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 3a** | **spanning-tree operedge** | Configure port as an edge port. |
| **Step 3b** | **no spanning-tree operedge** | Reset spanning tree port to default. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show spanning-tree interface** *{interface\_type slot/port}* | Show port STP configurations. |
| **Step 6** | **write** | Save configurations. |

### Configure Point to Point Mode

Point to point mode is usually the link which connects with switches. For the ports connected with the point-to-point link, upon some port role conditions met, they can transit to forwarding state fast through transmitting synchronization packet, thereby reducing the unnecessary forwarding delay.

Begin at privileged configuration mode, configure port to connect with point to point link 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** | **spanning-tree point-to-point** | Configure a port as point to point port.  By default, all ports are configured as point to point ports. |
| **Step 3b** | **no spanning-tree point-to-point** | Not to configure a port as point to point port. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show spanning-tree interface** *{interface\_type slot/port}* | Show port STP configurations. |
| **Step 6** | **write** | Save configurations. |

## Show STP Information

After configuring, use the following commands to show STP information.

|  |  |
| --- | --- |
| **Command** | **Function** |
| **show spanning-tree** | Show STP configurations and running status. |
| **show spanning-tree interface** *{interface\_type slot/port}* | Show STP configurations and running status of a port. |

# DHCP Management Configuration

## Configure DHCP Server

Now, larger and larger number of IP address are needed to allocate .DHCP (Dynamic Host configuration Protocol) is created to solve this problem .It concludes DHCP Server and DHCP Client.Requested by client, IP address are allocated by the server.Configure DHCP Server as the following table show:

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2a** | **dhcp-server [enable | disable]** | Disable the DHCP server function |
| **Step 2b** | **dhcp-server [ dns1 | dns2 | dns3 | wins]** <A.B.C.D> | Configure DHCP's DNS and WINS Server |
| **Step 2c** | **dhcp-server startip A.B.C.D endip A.B.C.D** | Configure DHCP IP address pool |
| **Step 2d** | **dhcp-server subnet A.B.C.D** | Configure DHCP mask |
| **Step 2e** | **dhcp-server gateway A.B.C.D** | Configure DHCP gateway |
| **Step 2f** | **dhcp-server interface vlan <1-4095>** | Add the VLAN to the DHCP Server（If want DHCP server successful，need to configure the vlan interface IP address） |
| **Step 2g** | **dhcp-server leasetime** *leasetime* | Configure IP address leasetime |
| **Step 3a** | **show dhcp-server** | Show DHCP server configuration |
| **Step 3d** | **show dhcp-server lease** | Show DHCP Server allocate IP address |
| **Step 4** | **copy running-config startup-config** | Save the configuration |

## 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** *vlan\_id* | 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 5** | **show dhcp-relay configure** | Show the DHCP relay configuration。 |
| **Step 6** | **copy running-config startup-config** | Save the configuration |

2. Multiple DHCP relay configuration：

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **dhcp-server group <groupname>** | Add a DHCP server group，and enter group configuration mode. |
| **Step 3a** | **dhcp-server A.B.C.D** | Add the DHCP server to the group. |
| **Step 3b** | **no dhcp-server A.B.C.D** | Delete DHCP server |
| **Step 4** | **exit** | Exit to the global configuration mode |
| **Step 5** | **interface vlan** *vlan\_id* | Add a VLAN and enter to VLAN interface configuration  *vlan\_id(*1－4094)； |
| **Step 6a** | **dhcp relay server-select <groupname>** | Select DHCP server group 。 |
| **Step 6b** | **no dhcp relay server-select <groupname>** | Delete the DHCP server group。 |
| **Step 7** | **exit** | Exit to global configuration mode |
| **Step 8** | **show dhcp-relay configure** | Sow DHCP relay configuration. |
| **Step 9** | **copy running-config startup-config** | Save the configuration. |

## 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 2** | **dhcp-snooping （enable|disable）** | Enable/disable DHCP Snoopin.（DHCP Snooping enable，can not open dhcp server and dhcp relay） |
| **Step 3a** | **dhcp-snooping vlan <1-4095> …** | Configure DHCP Snooping vlan list |
| **Step3b** | **no dhcp-snooping vlan <1-4095>…** | 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** | **copy running-config startup-config** | 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）** | Deil with 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** | **copy running-config startup-config** | 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 vlan <1-4095> A.B.C.D interface {***interface\_type slot/port}* **lease <60-1000000>** | Add the static DHCP binding list. |
|  | **no dhcp-snooping binding 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 configuration** | Show DHCP Snooping configuration. |
| **Step 6** | **copy running-config startup-config** | 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|untrust)** | Configure the trust/untrust port. All the port are untrust in default. |
| **Step 3b** | **dhcp-snooping information circuit-id string <string>** | Configure the option82的circuit-id value. |
| **Step 3c** | **no dhcp-snooping information circuit-id string <string>** | Delete the option82 circuit-id value ，and load default. |
| **Step 3d** | **dhcp-snooping information remote-id string <string>** | Configure option82remote-id value. |
| **Step 3e** | **no dhcp-snooping information remote-idstring <string>** | Delete option82 remote-id value，load default value. |
| **Step 3f** | **dhcp-snooping limit rate <0-4096>** | Configure the port max speed of receiving the DHCP packet. It doesn't limit by default. |
| **Step 3e** | **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）** | Configure 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** | **copy running-config startup-config** | Save configuration. |

# L3 Route Configuration

## L3 Route Configuration

### Hardware Router Table

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2a | **show l3 defip route** | Show hardware subnet routing information. |
| Step 2b | **show l3 hostroute** | Show hardware host routing information. |
| Step 2c | **show l3 interface** | Show interface information |

### 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 2a** | **ip route** *A.B.C.D A.B.C.D A.B.C.D* | | Add static route rule. |
| **Step 2b** | | **ip route** *A.B.C.D/M A.B.C.D* | Add static route rule. | |
| **Step 3a** | | **no ip route** *A.B.C.D A.B.C.D A.B.C.D* | Delete static route rule. | |
| **Setp 3b** | | **no ip route** *A.B.C.D/M A.B.C.D* | Delete static route rule. | |
| **Step 4** | | **show ip route** | Show route rules. | |

### 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**.

## RIP

### 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.

### RIP Configuration

RIP configuration includes:

* Configure RIP basic parameters
* Configure RIP authentication
* Configure RIP Split Horizon

#### 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** ip-address/masklen | 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** rip-address | (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**) **metric**<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** update timeout garbage | (Optional) Adjust routing protocol timers. Valid ranges for all timers are 0 to 4294967295 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.

#### 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** vlan\_id | 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.

#### 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** vlan\_id | 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.

#### RIP v1/2 Compatible Configuration

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **Interface vlan** vlan\_id | 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. |

### RIP Configuration Example

#### RIP General Configuration

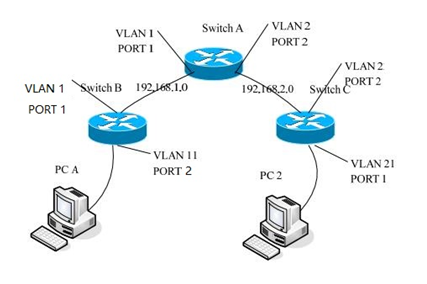
1. Networking requirements

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

#### 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.

#### 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.

## OSPF

### 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.

### OSPF Configuration

#### 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.

#### Configure OSPF Interface

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface vlan** vlan\_id | 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** seconds | (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** seconds | (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** number | (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-interva**l seconds | (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** seconds | (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 **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. |

#### 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. |
| **Step 4** | **area** area-id **authentication** **message-digest** | (Optional) Enable MD5 authentication on the area. |
| **Step 5** | **area** area-id **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** area-id **nssa**[no-summary] | (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** area-id **range**  address/masklen | (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. |

#### 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 OSPFconfigure mode. |
| **Step 3** | **default-information originate** **{[always]}\*1 {[metric]** <0-16777214>}\*1 {[**metric-type**] (1|2)}\*1 {[**route-map**] <WORD>}\***1** | Configure default route |
| **Step 4** | **exit** | Returen global configuration mode. |

#### Show OSPF Configurate Information

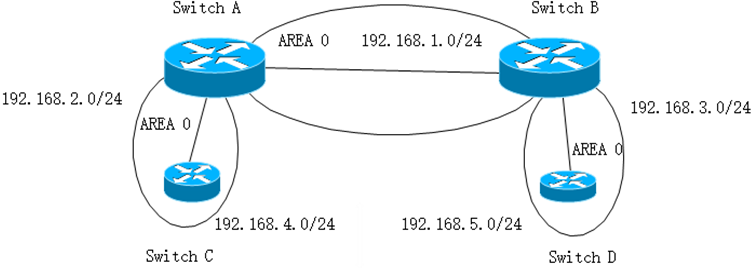
|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show ip ospf database** [router] [self-originate]  **show ip ospf database**[router] [adv-router [ip-address]]  **show ip ospf database** [network] [self-originate]  **show ip ospf database**[network] [adv-router [ip-address]]  **show ip ospf database**[summary] [self-originate]  **show ip ospf database**[summary] [adv-router [ip-address]]  **show ip ospf database**[asbr-summary] [self-originate]  **show ip ospf database**[asbr-summary] [adv-router [ip-address]]  **show ip ospf database**[external] [self-originate]  **show ip ospf database**[external] [adv-router [ip-address]] | Display lists of information related to the OSPF database. |
| **Step 3** | **show ip ospf route** | Display lists of information related to the OSPF route. |
| **Step 4** | **show ip ospf interface**[interface-name] | Display OSPF-related interface information. |
| **Step 5** | **show ip ospf neighbor** | Display OSPF interface neighbor information. |

### OSPF Configuration Example

#### 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

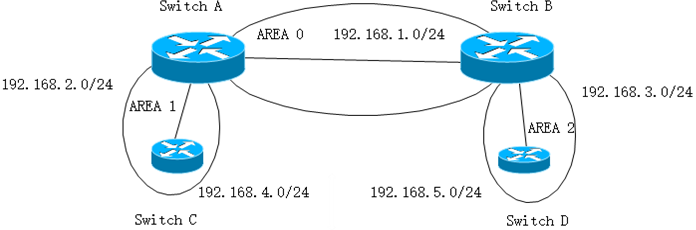
Switch C route table:192.168.1.0 and 192.168.5.0

Switch D route table:192.168.1.0 and 192.168.4.0

#### 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.

#### 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

1. intra-area route are converged. Refer to the OSPF intra-area route test to disconnect 192.168.4.0/24 of Switch C.
2. intra-area route are converged. Refer to the OSPF intra-area route test to reconnect 192.168.4.0/24 of Switch C.
3. inter-area route are converged. Refer to the OSPF inter-area route test to disconnect 192.168.4.0/24 of Switch C.
4. inter-area route are converged. Refer to the OSPF inter-area route test to reconnect 192.168.4.0/24 of Switch C

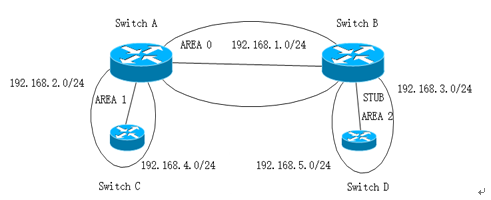
Test result:

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.

#### 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

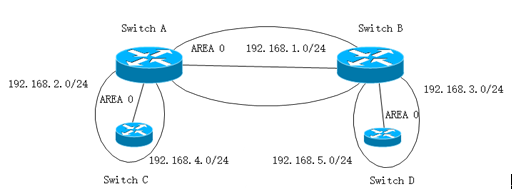
Test result:

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.

#### 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 |

## 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

### Route IP List

#### 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. Access-List lists are available in standard and extended formats:

1. The standard index has a value range of 1-99, 1300-1999, and only controls the source ip;

2. Extended index value range: 100-199, 2000-2699, control source ip and destination ip

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **ip access-list** access\_list\_index {**permit**|**deny**} <A.B.C.D> <wildcard\_mask>  **ip** **access-list** access\_list\_index {**permit**|**deny**} host <A.B.C.D>  **ip access-list** access\_list\_index {**permit**|**deny**} **any** | Define a standard access-list, access\_list\_index ranges from 1-99 to 1300-1999,  < A.B.C.D. > < wildcard\_mask > defines standard IP access based on the source IP address or mask;  Host defines standard IP access based on a single source IP address;  Any standard IP access based on any source IP address; |
| **Step 2b** | **ip access-list** access\_list\_index {**permit**|**deny**} <A.B.C.D> <wildcard\_mask> {<A.B.C.D> < wildcard\_mask> | host <A.B.C.D> | any}  **ip access-list** access\_list\_index {**permit**|**deny**} host <A.B.C.D> {<A.B.C.D> <wildcard\_mask> | host <A.B.C.D> | any}  **ip access-list** access\_list\_index {**permit**|**deny**} any {<A.B.C.D> <wildcard\_mask> | host <A.B.C.D> | any} | Define an extended access-list, access\_list\_index ranges from 100-199 to 2000-2699,  < A.B.C.D. > < wildcard\_mask > defines extended IP access based on the source IP address or mask;  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\_index | Delete access-list |
| **Step 3** | **exit** | Return to privileged EXEC mode. |
| **Step 4** | **show ip access-list** | Show access-list information |
| **Step 5** | **write** | Save configurations. |

To delete access list, command：**no ip access-list** access\_list\_index

#### 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\_name [seq sequence\_num] {permit|deny} <A.B.C.D/M>  [ge ge\_value] [le le\_value]  ip prefix-list prefix\_list\_name [seq sequence\_num] {permit|deny} 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** [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)

### 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.

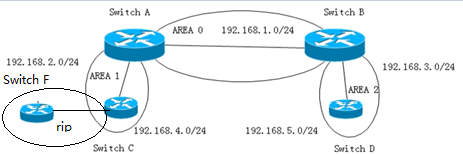
#### RIP Route Redistribution

|  |  |  |
| --- | --- | --- |
|  | **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) {**metric** <0-16>}\***1** {route-map <map-tag>}\***1** | Inter-protocol routing redistribution, including direct connection, kernel, ospf protocol, static routing information to rip protocol.Let rip be published. |
| **Step 6** | **passive-interface** <IFNAME> {A.B.C.D}\*1 | Configure the passive interface |
| **Step 7** | **offset-list** (<access-list>) (**in**|**out**) <0-16> {vlan <1-4094>}\***1** | Used to adjust measurements |
| **Step 8** | **show running-config** | Show running-config information |

#### 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|ospf|static) {**metric** <0-16>} {route-map <map-tag>}\***1** | Inter-protocol routing redistribution, including redistribution of direct connection, kernel, ospf protocol, static routing information to rip protocol.Get the ospf protocol out there. |
| **Step 6** | **passive-interface** <IFNAME> {A.B.C.D}\*1 | Configure the passive interface |
| **Step 7** | **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 |

### 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.

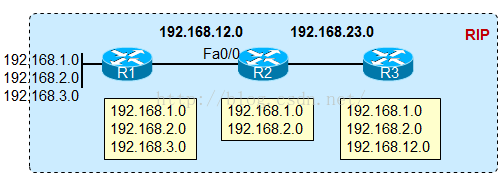
#### Distance Vector Routing Protocol RIP

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> **(in|out) {<ifname>}\*1** | Filter routing using the access control list |
| **Step 4** | **distribute-list prefix** <prefix-list> **(in|out) {**<WORD>**}\*1** | Filter routing using prefix lists |
| **Step 5** | **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

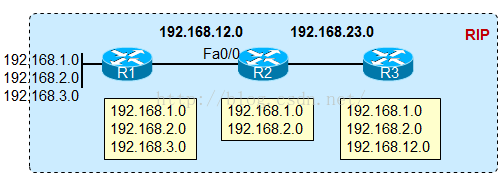
R2(config)# access-list 1 permit any

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

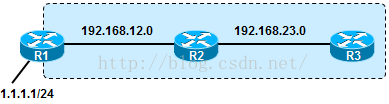
So, first of all, R2's own routing table will change, and 3.0's routing will be filtered out, and R3, the downstream RIP router, won't learn 3.0.

#### 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> **out** **(kernel|connected|static|rip)** | Use the access control list for redistribution |
| **Step 4** | **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

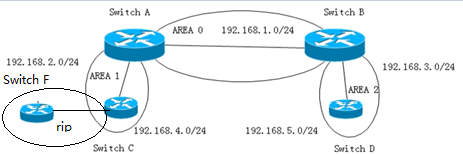
Redistribute rip metric 10 subnets

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; |

### Routing Maps to Control Routing Updates

#### 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.

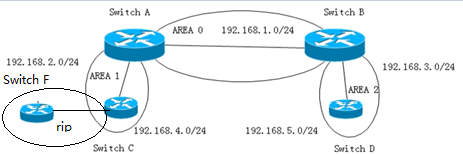
|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **route-map** map\_name **[permit|deny]** sequence\_number | Configure a route-map and enter the route-map configuration mode. |
| **Step 3** | **match 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 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 6** | **match ip next-hop prefix-list** prefix\_list\_name | Match the next hop routing address through the specified prefix-list. |
| **Step 7** | **match interface** interface\_name | Matches the routing of the next outgoing interface that is one of the specified interfaces |
| **Step 8** | **match metric** metric\_value | Matching the specified routing metrics, metric\_value ranges from 0-4294967295. |
| **Step 9** | **match tag** tag\_value | Matches the specified routing tag, and the tag\_value range is 1-4294967295. |
| **Step 10** | **set metric** metric\_value | Set the metrics for the reroute routing, and metric\_value ranges from 0-4294967295. |
| **Step 11** | **set metric-type** metric\_type | Sets the measurement value type for the redistributed routing. |
| **Step 12** | **set tag** tag\_value | Sets the tag for the redistributed routing. |
| **Step 13** | **set ip next-hop** metric\_value | Specifies the measure of the next hop of forwarding. |
| **Step 14** | **exit** | Return to privileged EXEC mode. |
| **Step 15** | **show route-map** | Show route-map information |
| **Step 16** | **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**.

#### 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|ospf|static)** {metric <0-16777214>} {metric-type (1|2)} {route-map <WORD>} | Redistribute direct connection, kernel, ospf protocol, static routing information to rip protocol.Get the ospf protocol out there. |
| **Step 4** | **show running-config** | Show running-config information |

For example



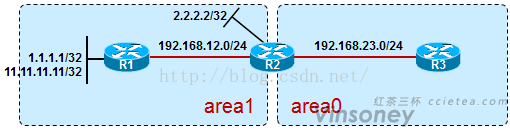
|  |  |
| --- | --- |
| Configuration | Result |
| switch c:  ip access-list 1 permit 192.168.6.0 0.0.0.255  ip access-list 2 permit 192.168.7.0 0.0.0.255  ip prefix-list 1 seq 5 permit 192.168.6.0/24  ip prefix-list 2 seq 5 permit 192.168.7.0/24  route-map test1 permit 10  match ip address 1  set metric 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  ! | 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 192.168.1.1, 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 |

### 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** area-id **filter-list** prefix <prefix> (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.

# IPv6

## VLAN IPv6 Address

Begin at 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** *vlan\_id* | enter VLAN interface configuration  *vlan\_id* range:1~4094 |
| **Step 3a** | **ipv6 address** *<X:X::X:X/M> [eui-64]*  **ipv6 address** *<X:X::X:X>* ***link-local*** | 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.  Configure the IPv6 link-local address of the vlan interface. |
| **Step 3b** | **no ipv6 address** *<X:X::X:X/M>*  **no ipv6 address**  **no ipv6 address** *<X:X::X:X>* ***link-local*** | Delete specified IPv6 address of VLAN interface.  Delete all IPv6 addresses of the VLAN interface.  Restore the default link-local address of VLAN interface. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface vlan** *vlan\_id* | Verify the configuration information. |
| **Step 6** | **write** | Save configurations. |

## 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** *vlan\_id <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** *vlan\_id* | Delete the specified item of the neighbor discovery table. | |
| **Step 4** | **show ipv6 neighbors** | Show the neighbor items in the current neighbor discovery table. | |

## 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 autoconfiguration 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.

### 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.

### IPv6 SLAAC Configuration

Begin at 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***vlan\_id* | Enter VLAN interface configuration. *vlan\_id* range: 1-4094. |
| **Step 3** | **no ipv6 nd suppress-ra**  **ipv6 nd suppress-ra** | Disable RA message suppression. The interface sends RA messages periodically (default 600S). By default, RA message suppression is enabled.  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>*  **[valid-lifetime][** **preferred-lifetime]**  **[off-link]**  **[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. | |

### Example(pending)

## DHCPv6

### 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.

#### DHCPv6 Network Composition

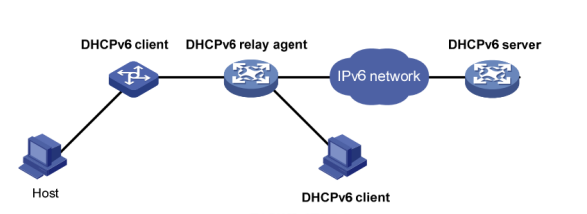


Figure 1：DHCPv6 network Composition

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.

#### 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** *<1-4294967295>* **|duid-uuid** *<word>*} | Configure DUID. |
| **Step 3** | **show ipv6 dhcp duid** | Display DUID configuration. |
| **Setp 4** | **write** | Save configuration. | |

### DHCPv6 Server

#### 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.

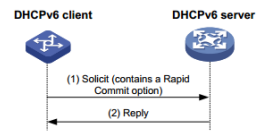


Figure 2：Quickly allocation process with two messages exchanging

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.

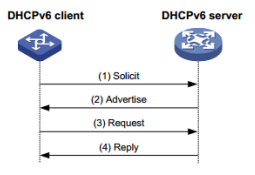


Figure 3：Allocation process with four messages exchanging

|  |  |  |
| --- | --- | --- |
| **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. |

#### 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.

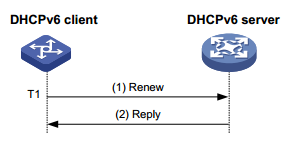


Figure 4：Update address/prefix lease by renew

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.

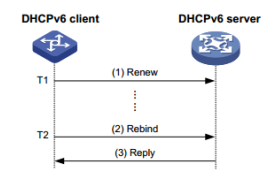


Figure 5：Update address/prefix lease by rebind

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.

#### 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.

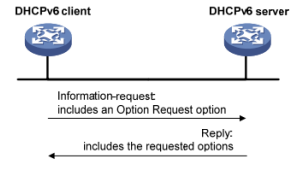


Figure 6：DHCPv6 stateless configuration process

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.

#### DHCPv6 Server Configurations

Begin at 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** *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 prefix**  *<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** *<WORD>* | Configure domain name. | |
| **Step 7** | **nis address** *<X:X::X:X>* | Configuring the NIS server IPv6 address. | |
| **Step 8** | **nis domain-name** *<WORD>* | Configuring the NIS server domain name. | |
| **Step 9** | **nisp address** *<X:X::X:X>* | Configure the NISP server IPv6 address. | |
| **Step 10** | **nisp domain-name** *<WORD>* | Configure the NISP server domain name. | |
| **Step 11** | **ntp address** *<X:X::X:X>* | Configure the NTP server IPv6 address. | |
| **Step 12** | **sip address** *<X:X::X:X>* | Configure the SIP server IPv6 address. | |
| **Step 13** | **sip domain-name** *<WORD>* | Configure the SIP server domain name. | |
| **Step 14** | **bcmcs address** *<X:X::X:X>* | Configuring the BCMCS server IPv6 address. | |
| **Step 15** | **bcmcs domain-name** *<WORD>* | Configure the BCMCS server domain name. | |
| **Step 16** | **exit** | Exit to global configuration mode. | |
| **Step 17** | **interface vlan** *vlan\_id* | Add VLAN and enter VLAN interface configuration.  vlan\_id(1－4094)； | |
| **Step 18** | **ipv6 dhcp server** *pool\_name* **[preference** *<0-255 >***] [allow-hint] [rapid-commit]** | Configure and enable the DHCPv6 server address of the network segment on the interface. | |
| **Step 19** | **exit** | Exit to global configuration mode. | |
| **Step 20** | **show ipv6 dhcp pool** | View DHCPv6 address pool information.. | |
| **Step 21** | **show ipv6 dhcp interface [vlan** *<1-4094>***]** | Show information about the device DHCPv6 interface | |
| **Step 22** | **show ipv6 dhcp binding** | View the address binding information of the DHCPv6 address pool. | |
| **Step 23** | **write** | Save configurations. | |

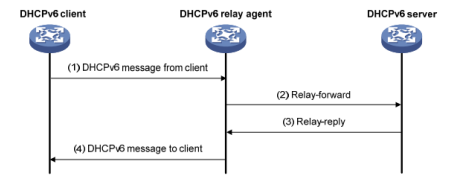
#### Example(pending)

### DHCPv6 Relay

#### 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.

#### DHCPv6 Relay Configuration

Begin at 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** *vlan\_id* | 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. | |

#### DHCPv6 Relay Option 37 Configuration

Begin at 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** *vlan\_id* | Add VLAN and enter VLAN interface configuration.vlan\_id(1-4094)； |
| **Step 3** | **ipv6 dhcp relay remote-id** *<WORD>* | Configure the remote-id value of the custom option37. |
|  | **show ipv6 dhcp relay option** | Display configuration information about trunk related options. | |
| **Setp 4** | **exit** | Exit to global configuration mode. | |
| **Step 5** | **write** | Save configurations. | |

#### DHCPv6 Relay Option 38 Configuration

Begin at 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** *vlan\_id* | Add VLAN and enter VLAN interface configuration.vlan\_id(1-4094)； |
| **Step 3** | **ipv6 dhcp relay subscriber-id** *<WORD>* | Configure the custom subscriber-id value of option38. |
|  | **show ipv6 dhcp relay option** | Display configuration information about trunk related options. | |
| **Setp 4** | **exit** | Exit to global configuration mode. | |
| **Step 5** | **write** | Save configurations. | |

#### Example(pending)

## IPv6 Route

### 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. |
| **Setp 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 | |

### View IPv6 Hardware Routing Information

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **show ipv6 l3 defip route** | View IPv6 hardware subnet routing information. |
| **Step 2b** | **show ipv6 l3 hostroute** | View IPv6 hardware host routing information. |
| **Step 2c** | **show l3 interface** | View interface information. |

## IPv6 Connectivity Test

Ping6 is mainly used to check network connectivity and host reachability for IPv6.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **ping6** *<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. |

# PON Management



## Show PON Port Info and Optical Power

### Show Pon Port Statistics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **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** | Show PON port statistics. | |

### 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.

Begin at 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. | |

### 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 pon onu [<1-128>|all] rx-power** | Show ONU optical transceiver | |

## PON Port Configuration

### Enable/Disable PON

Begin at 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 | |
| **Step 4** | | **show pon info** | Show pon info | |
| ONU auto-learn configuration 打开或者关闭PON口的ONU自动授权功能。   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | | **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** *{default-onu-profile <profile\_name>}\*1* | 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 | |   Note: After the ONU is auto-learned, there will be ONU connected to this PON port. The OLT will check whether there is equipment ID in the auto-binding list. If the equipment ID of this ONU is in the auto-binding list, the ONU uses the information of auto-binding list to register. | | | | |

# ONU Management



## ONU Basic Configuration

### Show 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** | Show auto-find ONU | |
|  | | **show onu auto-find** *{[detail-info]}\*1* | Show auto-find ONU detail info | |

### ONU Automatic Authorize

OLT can enable/disable automatic authorized mode. ONU will authorized automatically when ONU online

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | | Enter PON interface configuration mode. |
| **Step 3** | | **onu auto-learn** *{default-onu-profile <profile\_name>}\*1* | Enable/disable auto-auth | |
| **Step 4** | | **Show onu auto-learn** | Show auto-learn | |

### Show ONU Authorized 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 onuinfo [<1-128>]\*1** | Show ONU authorized info | |

### Show ONU Authorized Detail-info

It can show ONU Vendor ID, Version, SN, 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 {<1-128>}\*1** | Show a onu detail-info or can select a range | |

### Activate|Deactivate ONU

ONU will online/offline when you activate/deactivate 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|<1-128] [activate|deactivate]* | Activate/deactivate ONU on pon port | |

### 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 <1-128> profile <onu\_profile\_name> [hpw|loid+hpw|loid+pw|loid|pw|sn+hpw|sn+pw|sn]** | Authorize ONU | |

### Configure ONU Description String

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | | Enter PON interface configuration mode. |
| **Step 3** | | **onu** *<onuid>* **description** *<string>* | Add description string to ONU. | |
| **Step 4** | | **show onu** *<onuid>* **description** | Show ONU description. | |

## ONU Remote Configuration

### Show ONU SFP 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 onu** *<1-128>* **optical-info** | Show onu SFP info | |

### Upgrade ONU

Only ONU had authorized on OLT, ONU can upgrade.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **upgrade load image** *<filename> <A.B.C.D>* | Configure ONU firmware name and TFTP server. |
| **Step 3** | **upgrade select pon** *<pon\_num> {<onuid\_list>}\*1* | Select ONU. ONU ID format is 1-2. |
| **Step 4** | **upgrade start** *[download|active|commit|mix]* | Download ONU firmware and save in memory, and then update ONU. |
| **Step 5** | **upgrade stop** | Delete the firmware in memory,and detele the upgrader info |
| **Step 6** | **show****upgrade** *[status|info|* *onu-version] {pon <1-8> <onu\_list>}\*1* | Show the upgrade status,upgrade info and firmware info |

**Notice:**

1. DO NOT turn power off when updating. After finishing update, OLT will inform ONU if updated successfully and reset ONU with the new firmware.

2. After ONU updated and restarted, OLT will send commit command to confirm the new version.

3. Please delete the firmware and upgrade settings by command **upgrade onu stop**.

4. Display ONU upgrade progress by command **show upgrade onu status**.

5. Display ONU upgrade settings by command **show upgrade onu info**.

6. Stop upgrading ONU by command **upgrade onu stop**.

### Auto-upgrade ONU

OLT will compared equipment id with onu info, if they are consistent, will start to upgrade

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **auto-upgrade onu equipment\_id** *<string>* **version** *<string>* **image** *<filename> <A.B.C.D>* | Configure the onu equipment, id , version ,file name ,file address |
| **Step 3** | **no auto-upgrade onu equipment\_id** *<string>* | Delete the onu equipment |
| **Step 4** | **show auto-upgrade** *[status|config]* | Show the auto-upgrade |

### Reboot ONU

Reboot the ONU which had authorized

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **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|<1-128>* **reboot** | Reboot one of ONU or all of onu on PON | |

### TCONT Configuration

Create/modify a TCONT, and bind to DBA profile.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | | Enter PON interface configuration mode. |
| **Step 3a** | | **onu** *<1-128>* **tcont** *<1-255> {[name] <string>}\*1 {[dba] <string>}\*1* | Configure ONU TCONT and dba you had created. | |
| **Step 3b** | | **no onu** *<1-128>* **tcont** *<1-255>* | Delete TCONT | |
| **Step 4** | | **show onu** *<onuid>* **tcont** | Show ONU TCONT | |

### 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** *<1-128>* **gemport** *<1-255> [tcont]**<1-255> {[gemport\_name] <gemport\_name>}\*1 {[portid] <129-4095>}\*1 {[queue] <0-7>}\*1* | Configure GEMPORT to bind a TCONT. And can select portid and queue id | |
| **Step 3b** | | **onu** *<1-128>* **gemport** *<1-255> [traffic-limit]* **upstream** *<dba\_name>* **downstream** *<dba\_name>* | Configure GEMPORT to bind a traffic limit profile | |
| **Step 3c** | | **onu** *<1-128>* **gemport** *<1-255> [state] [enable|disable]* | Enable/disable gemport。 | |
| **Step 3d** | | **onu** *<1-128>* **gemport** *<1-255> [down-queue-map-id] <0-7>* **up-queue-map-id** *<0-3>* | Configure GEMPORT up/down queue | |
| **Step 3e** | | **onu** *<1-128>* **gemport** *<1-255>* **encrypt** *[disable|enable]**{[downstream|bidirection]}\*1* | Configure GEMPORT encrypt | |
| **Step 4** | | **no onu** *<1-128>* **gemport** *<1-255>* | Delete ONU GEMPORT | |
| **Step 5** | | **show onu** *<onuid>* **gemport** | Show ONU GEMPORT configuration | |

### 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** *<1-128>* **service** *<service\_name>* **gemport** *<1-255> [vlan] <vlan\_list> {[iphost] <1-255>}\*1 {[ethuni] lan <1-32>}\*1 {[cos] <cos\_list>}\*1* | Configure ONU service with vlan | |
| **Step 3b** | | **onu** *<1-128>* **service** *<service\_name>* **gemport** *<1-255> [untag] {[ethuni]* **lan** *<1-32>}\*1 {[iphost] <1-255>}\*1* | Configure ONU service without vlan | |
| **Step 4** | | **no onu** *<1-128>* **service** *<service\_name>* | Delete ONU service | |

### Service-port Configuration

Configure the service-port .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | | Enter PON interface configuration mode. |
| **Step 3a** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> {[to] <1-4094>}\*1 transparent* | Configure the vlan transparent mode | |
| **Step 3b** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094>* *[user\_priority] <0-7> [vlan] <1-4094> {[new\_cos] <0-7>}\*1* | Configure the vlan translate mode | |
| **Step 3c** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | Configure the vlan translate mode and QinQ | |
| **Step 3d** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> [user\_etype] [pppoe|ipoe] [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | Configure the vlan translate mode and QinQ.can select the type of packets | |
| **Step 3e** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> [user\_etype] [user\_define] <eth\_type> [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | Configure the vlan translate mode and QinQ.can select the type that user define. | |
| **Step 3f** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan untag** *[user\_etype] [user\_define] <eth\_type> [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | Configure the vlan untagged mode, can configure QinQ and type that user define. | |
| **Step 3g** | | **onu** *<1-128>* **service-port** *<1-128>* **gemport** *<1-128>* **uservlan untag** *[vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | Configure the vlan untagged mode,can configure QinQ | |
| **Step 4** | | **onu** *<1-128>* **service-port** *<1-128>* **admin-status** *[enable|disable]* | Enable/disable service-port | |
| **Step 5** | | **onu** *<1-128>* **service-port** *<1-128>* **description** *<desc>* | Configure the service-port description | |
| **Step 6** | | **no onu** *<1-128>* **service-port** *<1-128>* | Delete the service-port | |

### ONU UNI Configuration

Include 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** *<1-128>* **portvlan** *[eth|wifi|veip] <1-32> [mode] [transparent]* | Configure the UNI mode is transparent | |
| **Step 3b** | | **onu** *<1-128>* **portvlan** *[eth|wifi|veip] <1-32> [mode] [trunk]* | Configure the UNI mode is trunk | |
| **Step 3c** | | **onu** *<1-128>* **portvlan** *[eth|wifi|veip] <1-32> [mode] [tag]* **vlan** *<1-4094> {pri <0-7>}\*1* | Configure the UNI mode is access and bind a vlan | |
| **Step 3d** | | **onu** *<1-128>* **portvlan** *[eth|wifi|veip] <1-32> [mode] [hybrid]* **def\_vlan** *<1-4094> {def\_pri <0-7>}\*1* | Configure the UNI mode is hybrid and bind a vlan | |
| **Step 3e** | | **onu** *<1-128>* **portvlan** *[eth|wifi|veip] <1-32> [vlan] <vlan\_list>* | Configure the list of UNI vlan | |
| **Step 3f** | | **onu** *<1-128>* **portvlan** *[eth|wifi|veip] <1-32> [translate] [vlan] <1-4094> [cvlan] <1-4094> {[cvlan\_pri] <0-7>}\*1 [svlan] <1-4094> {[svlan\_pri] <0-7>}\*1* | Configure the UNI mode is translate | |

### ONU FEC Configuration

Enable/disable ONU FEC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **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>* **fec** *[enable|disable]* | Enable/disable ONU FEC | |

### Show 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** *{<1-128>} \*1* | Show ONU Service | |

### Show 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** *[<1-128>|all]* **capability** | Show ONU capability | |

## ONU Remote Port Configuration

### ONU Port Enable|Disable

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **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]}\*1* | Disable/enable port | |

### ONU Port Autonegotiation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **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>**{[speed] [auto|full-10|full-100|full-1000|half-10|half-100]}\*1* | ONU port autonegotiation | |

### ONU Port Flow Control Configuration

Begin at privileged configuration mode, configure ONU port flow control 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** | | **onu** *<onuid>* **eth** *<port-num>**{[pause-time] <0-65535>}\*1* | Configure flow control | |

### 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** *<1-128>* **mvlan** *<vlanList>* | Add a multicast vlan | |
| **Step 3b** | | **no onu** *<1-128>* **mvlan** *[all|<vlanList>]* | Delete multicast vlan | |

### Configure 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** *<1-128>* **iphost** *<1-255> [id] <desc>* | Configure iphost descible | |
| **Step 3b** | | **onu** *<1-128>* **iphost** *<1-255> [dhcp]* | Configure to dhcp mode | |
| **Step 3c** | | **onu** *<1-128>* **iphost** *<1-255> [static-ip] <A.B.C.D> <A.B.C.D> {<A.B.C.D>}\*1* | Configure to static mode,and subnet,GW | |
| **Step 3d** | | **onu** *<1-128>* **iphost** *<1-255> [primary-dns] <A.B.C.D> {second-dns <A.B.C.D>}\*1* | Configure the dns | |
| **Step 3e** | | **no onu** *<1-128>* **iphost** *<1-255>* | Delte the iphost configuration | |

### ONU Port Multicast Tag-strip 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 *<1-128>* mvlan *[tag-strip]* eth *<1-32>*** | Configure the multicast tag-strip | |
| **Step 3b** | | **no onu** *<1-128>* **mvlan** *[tag-strip]* **eth** *<1-32>* | Delete the configuration | |

### Example for SFU

1GE ONU with vlan 100. Uplink DBA mode: assured 10M, maximum 20M. Gemport 1 with downlink 20M.

1. Create a onu profile with 1 eth port

Profile onu name 1GE\_SFU

Port eth 1

Commit

Exit

1. Create a dba profile with assured 10M max 20M

Profile dba name 20M

Type 3 assured 10240 maximum 20480

Exit

1. Create a traffic profile to limit the downlink speed

Profile traffic name DN\_20M

Sir 20480 pir 20480

Exit

1. Register 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 gemport 1 traffic-limit upstream default downstream DN\_20M

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

1. Create vlan 100

Vlan 100

Exit

1. Bind the vlan to uplink port

Interface gigabitethernet 0/10

Switchport hybrid pvid vlan 100

### Example for HGU

4FE ONU with vlan 41 and vlan 46. Uplink DBA mode: assured 10M, maximum 20M. Gemport 1 with downlink 20M. vlan 46 is for tr069 , DBA mode: fixed 2M

1. Create a onu profile with 1 veip port

Profile onu name HGU

Port veip 1

Commit

Exit

1. Create a dba profile

Profile dba name 20M

Type 3 assured 10240 maximum 20480

Exit

Profile dba name 2M

Type 1 fixed 2048

Exit

1. Create a traffic profile to limit the downlink speed

Profile traffic name DN\_20M

Sir 20480 pir 20480

Exit

1. register 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 gemport 1 traffic-limit upstream default downstream DN\_20M

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

1. Create vlan 41 and 46, bind to uplink port

Vlan 41

Exit

Vlan 46

Exit

Interface gigabitethernet 0/10

Switchport mode trunk

Switchport trunk vlan 41

Switchport trunk vlan 46

1. Login to onu webinterface, create two WAN connection,one is internet with vlan41; another one is tr069 with vlan46

## Rogue-onu Configuration

We called this rogue ONT which does not follow the assigned timestamp to send up the optical signal.

Rogue ONT mainly divided into the following two types:

1) The long Lighting rogue ont: ONT is lighting (glowing at any moment).

2) Luminous rogue ont: Lighting in OLT non allocation of the timestamp, may be light in advance, or delay to turn off and so on.

### Rogue-onu-detect

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **rogue-onu-detect** *[enable|disable]* **locate** *[enable|disable]* **auto-shutdown** *[enable|disable]* | | Enable/disable detect/locate/auto-shudown function |
| **Step 3** | | **show rogue-onu-detect config** | Show the configuration | |
| **Step 4** | | **show rogue-onu-detect info pon** *<1-8>* | Show the result | |

### Rogue-onu status

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **rogue-onu-state pon** *<1-8>* **onu** *<1-128> [on|off|shutdown]* **duration** *[forever|<1-255>]* | | Configure the rogue-onu online/offline/shutdown and duration time |
| **Step 3** | | **show rogue-onu-detect config** | Show the configuration | |

# ONU Template Management



## Summary of ONU Template

Template under “config” node, the operation steps are as follows:

1.Create a template

profile [onu|dba|traffic|line|srv|voip|alarm] {id <1-32767>}\*1 {name <string>}\*1

2.Through profile\_id into the corresponding template node

profile [onu|dba|traffic|line|srv|voip|alarm] {id <1-32767>}\*1 {name <string>}\*1

3.Modify the template parameters

modify …

4.Exit template node

exit

5.Binding template to an onu equipment

Interface gpon *slot/port*

*onu add 1 profile <string>*

onu <onuid> profile [line|srv] <string>

6.Query onu equipment binding template

Interface gpon slot/port

show profile [onu|dba|traffic|line|srv|voip|alarm] {id <1-32767>}\*1 {name <string>}\*1

7. query template configuration information

Show profile [onu|dba|traffic|line|srv|voip|alarm] {id <1-32767>}\*1 {name <string>}\*1 used-info

## ONU Template Configuration

The ONU template is used for onu authorization, and each ONU must specify only one ONU template when authorizated. The ONU template specifies the capability of this ONU.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | **Command** | **Function** | |
| **Step 1** | | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **profile onu** *{id <1-32767>}\*1 {name <string>}\*1* | | | Create or enter the onu profile you had created before. |
| **Step 3a** | | **tcont-num** *<1-255>* **gemport-num** *<1-255>* | | Configure the onu support max tcont and gemport. | |
| **Step 3b** | | **switch-num** *<1-255>* **flow-num** *<1-255>* | | Configure the onu support max switch and flow | |
| **Step 3c** | | **port-num** *{[eth] <0-64>}\*1 {[pots] <0-64>}\*1 {[iphost] <0-255>}\*1 {[ipv6host] <0-255>}\*1 {[veip] <0-127>}\*1* | | Configure the onu support eth/pots/iphost/ipv6host/veip | |
| **Step 3d** | | **service-ability n:1** *[yes|no]* **1:p** *[yes|no]* **1:m** *[yes|no]* | | Capability profile | |
| **Step 4** | | **commit** | | Commit the profile.only enter “commit”can submit the setting | |
| **Step 5** | | **exit** | |  | |

## DBA Template Configuation

The default system will have an id 0 dba template, this template parameters cannot be modified, all onu when create the default binding in the template.Each ONU must bind a dba template.

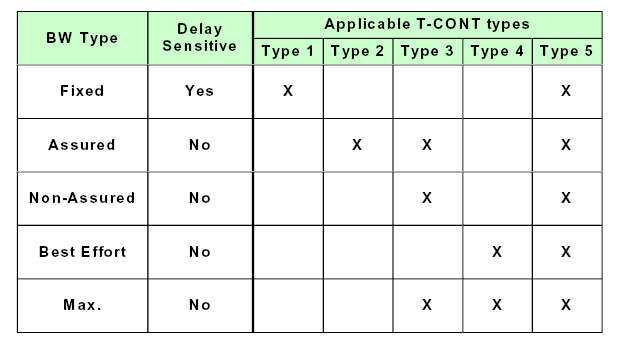
It have 5 dba filre:

Typr1: fix, integral

Type2: assure, integral

Type5: fix, assure, max, integral

Fix<=assure<=max.



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | **Command** | **Function** | |
| **Step 1** | | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **profile dba** *{id <1-32767>}\*1 {name <string>}\*1* | | | Create/modify a dba profile |
| **Step 3a** | | **type** *[1]* **fixed** *<64-2488320>* | | Configure type 1 with fixed | |
| **Step 3b** | | **type** *[2]* **assured** *<64-2488320>* | | Configure type 2 with assured | |
| **Step 3c** | | **type** *[3]* **assured** *<64-2488320>* **maximum** *<64-2488320>* | | Configure type 3 with assured and maximum | |
| **Step 3d** | | **type** *[4]* **maximum** *<64-2488320> {[priority] <1-4>}\*1 {[weight] <1-1000>}\*1* | | Configure type 4 with maximum | |
| **Step 3e** | | **type** *[5]* **fixed** *<64-2488320>* **assured** *<64-2488320>* **maximum** *<64-2488320> {[priority] <1-4>}\*1 {[weight] <1-1000>}\*1* | | Configure type 5 with fixed, assured, maximum. | |

## Traffic Template Configuation

The default system will have an id 0 traffic template, this template parameters cannot be modified, all GEMPORT when create the default binding in the template.Each GEMPORT must bind a traffic template.。

|  |  |  |
| --- | --- | --- |
| parameter | Detail | Range |
| Sir | sustained information rate | 0-10000000kbps |
| Pir | Peak information rate | 64-10000000kbps |
| Cbs | Committed Burst Size | 0-1023kbytes |
| pbs | Peak Burst Size | 0-1023kbytes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | **Command** | **Function** | |
| **Step 1** | | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **profile traffic** *{id <1-32767>}\*1 {name <string>}\*1* | | | Creat/modify a traffic profile |
| **Step 3** | | **sir** *<0-10000000>* **pir** *<64-10000000>**{cbs <0-1023> pbs <0-1023>}\*1* | | Configure the sir and pri, cbs and pbs is selectable. | |
| **Step 4** | | **Exit** | | Exit | |

## Line Template Configuation

The default system will have an id 0 LINE template, this template parameters cannot be modified,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | **Command** | **Function** | |
| **Step 1** | | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **profile line** *{id <1-32767>}\*1 {name <string>}\*1* | | | Create/modify a line profile |
| **Step 3a** | | **tcont** *<1-255> {[name] <string>}\*1 {[dba] <string>}\*1* | | Bind a tcont profile | |
| **Step 4a** | | **gemport** *<1-255> [tcont] <1-255> {[gemport\_name] <gemport\_name>}\*1 {[portid] <129-4095>}\*1 {[queue] <0-7>}\*1* | | Bind a gemport profile | |
| **Step 4b** | | **gemport** *<1-255> [encrypt] [enable|disable]* | | Enable/disable the gemport encrypt.by default, is enable | |
| **Step 4c** | | **gemport** *<1-255> [state] [enable|disable]* | | Enable/disable the gemport state | |
| **Step 4d** | | **gemport** *<1-255>**[traffic-limit]* **upstream** *<dba\_name>* **downstream** *<dba\_name>* | | Bind a up/downstream limit to gemport | |
| **Step 5a** | | **service** *<service\_name>* **gemport** *<1-255> [vlan] <vlan\_list> {[iphost] <1-255>}\*1 {[ethuni] lan <1-32>}\*1 {[cos] <cos\_list>}\*1* | | Bind a gemport which with vlan to service | |
| **Step 5b** | | **service** *<service\_name>* **gemport** *<1-255> [untag] {[ethuni] lan <1-32>}\*1 {[iphost] <1-255>}\*1* | | Bind a gemport without vlan to service | |
| **Step 5c** | | **mvlan** *<vlanlist>* | | Create the multicast vlan | |
| **Step 6a** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> {[to] <1-4094>}\*1 transparent* | | Configure the vlan mode to transparent | |
| **Step 6b** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094>* *[user\_priority] <0-7> [vlan] <1-4094> {[new\_cos] <0-7>}\*1* | | Configure the vlan mode to translate | |
| **Step 6c** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | | Configure the vlan mode to translate,QinQ | |
| **Step 6d** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> [user\_etype] [pppoe|ipoe] [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | | Configure the vlan mode to translate,QinQ,can select the type of data | |
| **Step 6e** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan** *<1-4094> [user\_etype] [user\_define] <eth\_type> [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | | Configure the vlan mode to translate,QinQ,can select the type that user define | |
| **Step 6f** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan untag** *[user\_etype] [user\_define] <eth\_type> [vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | | Configure the vlan mode to untag,QinQ,can select the type that user define | |
| **Step 6g** | | **service-port** *<1-128>* **gemport** *<1-128>* **uservlan untag** *[vlan] <1-4094> {[new\_cos] <0-7>}\*1 {[svlan] <1-4094>}\*1 {[new\_scos] <0-7>}\*1* | | Configure the vlan mode to untag,QinQ | |
| **Step 6h** | | **service-port** *<1-128>* **admin-status** *[enable|disable]* | | Enable/disable service-port | |
| **Step 6I** | | **service-port** *<1-128>* **description** *<desc>* | | Add the service-port description | |
| **Step 7** | | **no onu** *<1-128>* **service-port** *<1-128>* | | Delete the service-port | |
| **Step 8** | | **no mvlan** *[all|<vlanlist>]* | | Delete the multicast vlan | |
| **Step 9** | | **no tcont** *<1-255>* | | Delete the tcont | |
| **Step 10** | | **no gemport** *<1-255>* | | Delete the gemport | |
| **Step 11** | | **no service** *<service\_name>* | | Delete the service | |
| **Step 12** | | **commit** | | Commit the configuration | |
| **Step 13** | | **Exit** | | Exit | |

## Service Template Configuation

The default system will have an id 0 SRV template, this template parameters cannot be modified

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **profile srv** *{id <1-32767>}\*1 {name <string>}\*1* | | Create/modify sre 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] [trunk]* | Configure portvlan mode to trunk | |
|  | | **portvlan** *[eth|wifi|veip] <1-32> [mode] [tag] vlan <1-4094> {pri <0-7>}\*1* | Configure portvlan mode to tag,and configure pri | |
|  | | **portvlan** *[eth|wifi|veip] <1-32> [mode] [hybrid] def\_vlan <1-4094> {def\_pri <0-7>}\*1* | Configure portvlan mode to hybrid | |
|  | | **portvlan** *[eth|wifi|veip] <1-32> [translate] [vlan] <1-4094> [cvlan] <1-4094> {[cvlan\_pri] <0-7>}\*1 [svlan] <1-4094> {[svlan\_pri] <0-7>}\*1* | Configure portvlan mode to translate | |
| **Step 4a** | | **mvlan** *[tag-strip]* **eth** *<1-32>* | Configure the lan port to untag mode | |
| **Step 4b** | | **no mvlan** *[tag-strip]* **eth** *<1-32>* | Delete the the lan port to untag mode | |
| **Step 5a** | | **iphost** *<1-255> [id] <desc>* | Configure the iphost description | |
| **Step 5b** | | **iphost** *<1-255> [dhcp]* | Configure the iphost to dhcp mode | |
| **Step 5c** | | **iphost** *<1-255> [static-ip] <A.B.C.D> <A.B.C.D> {<A.B.C.D>}\*1* | Configure the iphost to static mode. | |
| **Step 5d** | | **iphost** *<1-255> [primary-dns] <A.B.C.D> {second-dns <A.B.C.D>}\*1* | Configure the DNS | |
| **Step 5e** | | **no iphost** *<1-255>* | Delete the iphost setting | |
| **Step 6** | | **Commit** | Commit the configuration | |
| **Step 7** | | **Exit** | Exit | |

## Alarm Threshold Template Configuration

Alarm threshold only can be configured by template. Begin at privileged configuration mode, configure alarm threshold template as the following table shows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **profile alarm** *{id <1-32767>}\*1 {name <string>}\*1* | | Create or enter a profile |
| **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>* **upper** *<-27~-8>* | Configure the range of rx-optical | |
| **Step 3c** | | **Tx-optical low <0-5> upper <0-5>** | Configure the range of tx-optical | |
| **Step 4** | | **Commit** | Commit the configuration | |
| **Step 5** | | **Exit** | Exit | |

## Show/Delete Profile Configuration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **no profile {dba|srv|voip|alarm}****id** *<1-32767>* | | Delete profile |
| **Step 3a** | | **show profile****{dba|srv|voip|alarm} all|id** *<0-65535>* **}** | Show profile | |
| **Step 3b** | | **show profile {dba|srv|voip|alarm} id** *<0-65535>*  **bind** | Show the onu which binding profile | |



# ONU Auto-learn Configuration



## ONU Auto-learn

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **onu auto-learn bind onu-profile** *<equipid> <onu\_profile>* | | Bind the equipment id with onu profile |
| **Step 3** | | **onu auto-learn bind** *(line-profile|srv-profile|alarm-profile) <equipid> <profile\_name>* | Bind the onu equipment with line/srv/alarm profile | |
| **Step 4** | | **no onu auto-learn bind onu-profile** *<equipid>* | Delete the binding setting | |
| **Step 5** | | **no onu auto-learn bind** *(line-profile|srv-profile|alarm-profile) <equipid>* | Delete the binding setting | |
| **Step 6** | | **show onu auto-learn bind** *{[ onu-profile|line-profile|srv-profile|alarm-profile]}\*1* | Show the equipment and profile | |

## Enable Auto-learn

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | | Enter Gpon interface |
| **Step 3a** | | **onu auto-learn** *{default-onu-profile <profile\_name>}\*1* | Enable auto-learn and select a profile. | |
| **Step 3b** | | **no onu auto-learn** | Disable auto-learn | |
| **Step 4** | | **show onu auto-learn** | Show auto-learn configuration | |

# System Management



## Configuration Management

### Save Configurations

After modified the configurations, you should same them so that these configurations can take effect next time it restarts. Use the following commands to save configurations.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **write** | Save configurations. | |

### Erase Configurations

If you need to reset to factory default, you can use the following commands to erase all configurations. After erased, the device will reboot automatically.

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

### Show Startup Configurations

Use the following command to display the configurations you have saved.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show startup-config** | Show configuration | |

### Show Running Configurations

Use the following commands to display running configurations. These running configurations may not be saved in flash.

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

### Upload/Download Configuration File

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node |
| **Step 3a** | **upload tftp configuration**  *<filename> <A.B.C.D>* | filename is Upgrade file  A.B.C.D is TFTP server IP |
| **Step 3b** | **download tftp configuration** *<filename> <A.B.C.D>* | filename is Upgrade file  A.B.C.D is TFTP server IP |

## Check System Information

### Check System Running Information

Use the following commands to view system information.

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

### Check Version Information

Use the following commands to check version information which includes hardware version, software version, software created time and so on.

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

### Check System Running Time

Use the following command to show system running time after turned power on.

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

## System Basic Configurations

### Configure System Name

Use the following command to modify system name. This modification will take effect immediately. You will see it in command prompt prefix.

Begin at privileged configuration mode,configure system name as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **hostname** *<name>* | Configure system name. It must start with alphabet. |
| **Step 3** | **hostname default** | Restore default |

### Configure Terminal Display Attribute

This command is used to configure display line number when access by console port or telnet.

Begin at privileged configuration mode, configure terminal display attribure as the followingtable shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **terminal length** *value* | Configure display line number.  Value range is 0-512. |

### Configure Terminal Time-out Value

Use the following commands to configure terminal time-out value. Default value is 10 minutes.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **line vty** | Enter line node |
| **Step 3a** | **exec-timeout** *<min> [<second>]* | Set the command-line timeout |
| **Step 3b** | **no exec-timeout** | Set the command-line timeout to default |
| **Step 4** | **show exec-timeout** | Show the command-line timeout |

## System Basic Operations

### Upgrade System

Use the following command to upgrade the equipment.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2b** | **download tftp image** *<filename> <A.B.C.D>* | Update firmware with header. |

### Network Connectivity Test

Use **ping** command to check network connectivity.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **ping** [**-s** *<packetsize>*] *<A.B.C.D>* | *Packetsize* is test packet length, unit is byte. | |

### Reboot System

Use the following command to reboot system.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **reboot** | Reboot system. | |

### Telnet

You can telent to system via outband or inband management IP. The default outband management IP is 192.168.8.100.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
|  | **telnet 192.168.200** | Telnet to application layer of system. Login name and passwork both are **admin**. |
|  | **telnet 192.168.200 2223** | Telnet to kernel of system. Login name is **default**. |
|  | gpon-olt(config)#**switch** | Telnet to kernel of system. Login name is **default**. |

### Configure RTC System Time

Use the following command to configure RTC system time.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter 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 |

### NTP Client

Device will update the time auto when you enable the NTP

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **ntp server <ip\_or\_domain>** | Configure the NTP server and enable it |
| **Step 3** | **no ntp server** | Disable the NTP server |
| **Step 4** | **show time** | Show the system time |

### Timezone Configuration

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **time zone <-12-12>** | Configure the timezone |
| **Step 3** | **show sys timezone** | Show the timezone |

### Fan Control

Use the following command to control fan running attribute.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **fan temperature** *<20-80>* | Configure Temperature of the fan |
| **Step 3** | **fan mode [open|close|auto]** | Configure the fan open mode |
| **Step 4** | **show fan** | Show the fan configuration and current  equipment temperature |

## Debug Information

### Enable/Disable CPU Debug Information

Use the following commands to enable or disable CPU debug information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **debug mode** | | Enter debug node. |
| **Step 3** | | **system debug {rx|tx} {on|off}** | On|off : enable or disable CPU debug.  Rx: CPU receives packets.  Tx: CPU transmits packets. | |

### Enable/Disable Functional Module Debug Information

Use the following commands to enable or disable function module debug information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **debug mode** | | Enter debug node. |
| **Step 3** | | **system debug {acl|timer|port|mac|vlan|vt| igmp|cfp|qos} {on|off}** | On|off : enable or disable function module debug information. | |

# User Management



## User Privilege

There are two privileges for user, administrator user and normal user.

Normal user is a read-only user, only can view system information but not user information, configurations. Administrator user can view all information and configure all parameters.

## Default User

By default, there is a administrator user **admin**, and password is **admin** too. Default user can’t be deleted, modified, but you can modify its password.

## Add User Account

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user add** *user-name* **login-password** *login-password* | Add new user account. |
| **Step 3** | **user role** *user-name* **{admin | normal enable-password** *enable-password***}** | Specify user role. New user is a normal privilege user. |

## Show User Account List

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user list** | Show user account list. |

## Delete User Account

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user delete** *username* | Delete user account. |

## Modify Password

Every user can modify its own password while administrator user can modify other users’ password. Modify password as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user login-password** *user-name*<CR>  Input new login password for user abc please.  New Password:  Confirm Password: | Configure user’s login password. |
| **Step 3** | **user enable-password** *user-name*<CR>  Input new enable password for user abc please.  New Password:  Confirm Password: | Configure user’s configuration mode password. |

# SNMP Configuration

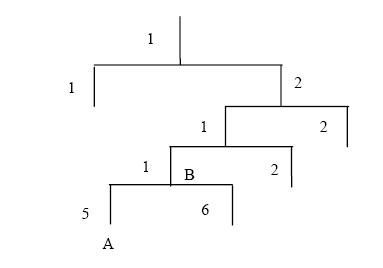
## SNMP Introduction

SNMP (Simple Network Management Protocol) is an extensive network management protocol at the moment. It is an industrial standard which is adopted and come into use for transmitting management information between two devices. Network administrator can search information, modify information, troubleshoot, diagnose fault, plan capacity and generate resports. SNMP adopts polling mechanism and provides basic functions, especially fits small, fast and low cost conditions. It is based on transport layer protocol UDP.

There are two parts of SNMP, NMS (Network Management Station) and agent. NMS is a station that runs client program, and agent is a server program that runs in device. NMS can send GetRequest, GetNextRequest and SetRequest messages to agent. Then agent will execute read or write command and respond to NMS. Agent also sends trap messages to NMS when device is abnormal.

## SNMP Version and MIB

In order to mark device’s management variable uniquely, SNMP identifies management object by hierarchical structure name scheme. The set of objects is like a tree, which the node stands for management object, shown as the following picture.



MIB(Management Information Base), a set of device’s variable definition, is used to describe the tree’s hierarchical structure. For the management object B in above picture, we can use a string of numbers {1.2.1.1} to describe it uniquely. This string of numbers is Object Identifier.

GPON OLT supports SNMP V1, V2C and V3. Common MIB shows in the following table.

|  |  |  |
| --- | --- | --- |
| **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 |  |

## SNMP Configuration

### Configure Community

Begin at privileged configuration mode, configure community as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **snmp-server community** *<word>*  **[ro| rw ]** | Configure SNMP community strings; |
| **Step 3** | **show snmp-server community** | Show the SNMP community configuration |
| **Step 4** | **exit** | From the global configuration mode to return to the privileged user configuration mode |
| **Step 5** | **write** | Save the configuration |

### Configure Trap Server Address

Use the following command to configure or remove the Trap messages of the target host IP address. Begin at privileged configuration mode, Configure Trap the target host address as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2a** | **snmp-server host <***A.B.C.D* **>{udp-port** *<1-65535>***}\*1 {version [1|2c]}\*1 {community** *<WORD>***}\***1 | Configure the Trap the target host address.  Configure the community string value |
| **Step 2b** | **no snmp-server host** *< A.B.C.D >* **version 1|2c|3** *community* | Delete trap target host address. |
| **Step 3a** | **snmp-server enable traps snmp** | Enable SNMP traps function |
| **Step 3b** | **no snmp-server enable traps snmp** | Delete SNMP traps function |
| **Step 4** | **show snmp-server targetaddress** | Check the SNMP trap configuration |
| **Step 5** | **write** | Save the configuration |

### Configure Contact Information

Begin at privileged configuration mode, Configure contact infromation as the following table shows.

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

### Configure Location Information

Begin at privileged configuration mode, Configure location information as the following table shows.

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

# Alarm and Event Management



## Alarm and Event Introduction

If you enable alarm report, it will trigger alarm events when system occured error or did some important operations. The alarm information will be saved in a buffer; you can execute some commands such as show syslog to display. All the alarms can be sent to specific servier.

Alarms include fault alarm and recovery alarm. Fault alarm will not disappear until the fault is repaired and the alarm is cleared.

Events include running envents and secury events, are notifications which generate and inform administrators under a normal condition. The difference between event and alarm is that event generates under a normal condition while alarm generates under an abnormal condition.

Command “show alarm-event information” is used to show description, level, type and class of all alarms and events.

## Alarm Management

Alarm severity level includes critical, major, minor and warning. Corresponding level in system log are alerts, critical, major and warnings. Alarm type includes device alarm, communication alarm and disposing alarm.

* Device alarm contains low temperature, high temperature, CPU usage, memory usage, fan, PON, optical power and so on.
* Communication alarm contains port up/down, loopback, PON deregister, PON register failed, PON los, ONU deregister, illegal ONU register, ONU authorized failed, ONU MAC conflication, ONU LOID conflication, ONU link los, ONU dying gasp, ONU link fault, ONU link events, ONU extended OAM notification and so on.
* Dispoing alarm contains upgrade failed, upload configuration file failed, download configuration file failed and so on.

### System Alarms

System alarms show the performance and security of system. The following table shows the system alarm list.

|  |  |  |
| --- | --- | --- |
| **System alarm** | **Reason** | **Default** |
| temp-high | Device temperature higher than threshold. | disable |
| temp-low | Device temperature lower than threshold. | disable |
| cpu-usage-high | CPU usage higher than threshold. | disable |
| mem-usage-high | Memory usage higher than threshold. | disable |
| fan | Fan switch. | disable |
| download-file-failed | Download file failed | enable |
| upload-file-failed | Upload file failed. | enable |
| upgrade-file-failed | Upgrade firmware failed. | enable |
| port-updown | Port link up and link down. | enable |
| port-loopback | Port loopback. | disable |

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **alarm {temp-high|temp-low| cpu-usage-high|mem-usage-high} disable** | Disable system alarm report. |
| **Step 2b** | **alarm {temp-high|temp-low| cpu-usage-high| mem-usage-high} enable** *<alarm-value> <clear-value>* | Enable system alarm report and configure system alarm threshold.  alarm-value: alarm threshold.  clear-value: clear threshold. |
| **Step 2c** | **alarm {fan|port-updown|port-loopback| register-failed|deregister}{enable|disable}** | Enable or disable system alarm report. |
| **Step 3** | **show alarm configuration** | Show system alarm configurations. |

### PON Alarms

Get rid of the issue caused by PON port or fiber by monitoring PON alarms, ensure PON works well. The following table shows PON alarm list.

|  |  |  |
| --- | --- | --- |
| **PON alarm** | **Reason** | **Default** |
| pon-txpower-high | PON port transmitting power higher than threshold. | enable |
| pon-txpower-low | PON port transmitting power lower than threshold. | enable |
| pon-txbias-high | PON port bias current higher than threshold. | enable |
| pon-txbias-low | PON port bias current lower than threshold. | enable |
| pon-vcc-high | PON port voltage higher than threshold. | enable |
| pon-vcc-low | PON port voltage lower than threshold. | enable |
| pon-temp-high | PON port temperature higher than threshold. | enable |
| pon-temp-low | PON port temperature lower than threshold. | enable |
| pon-los | Fiber unconnected or link fault. | enable |
| deregister | PON deregister. | disable |
| register-failed | PON register failed. | enable |

Configure global PON alarm as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **alarm {pon-register-failed|pon-deregister} {enable|disable}** | Enable or disable PON alarm report. |
| **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} {enable|disable}** | Enable or disable PON port alarm report. |
| **Step 3** | **show alarm configuration** | Show alarm configurations. |

Configure PON port alarm as the following table shows. Before this, you must enable global PON alarm. By default, global PON alarm is enabled, the alarms will be record in system log.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Command** | **Function** | |
| **Step 1** | | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | | Enter PON interface configuration mode. |
| **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 report. | |
| **Step 3b** | | **alarm pon optica {tx\_power\_high| tx\_power\_low |tx\_bias\_high |tx\_bias\_low| vcc\_high |vcc\_low | temp\_high|temp\_low} enable** *<alarm-value> <clear-value>* | Enable PON port alarm report and configure alarm parameters.  alarm-value: alarm threshold.  clear-value: clear threshold. | |
| **Step 4** | | **show alarm pon optical configuration** | Show PON port alarm configurations. | |

### ONU Alarms

ONU alarms also can help administrator to get rid of some ONU fault. The following table shows ONU alarm list.

|  |  |  |
| --- | --- | --- |
| **ONU alarm** | **Reason** | **Default** |
| onu-deregister | ONU deregister | enable |
| onu-link-lost | ONU fiber unconnected or link fault. | disable |
| onu-illegal-register | Illegal ONU register. | enable |
| onu-auth-failed | ONU LOID authorized failed in auto authorization mode or failed caused by packets loss. | enable |
| onu-mac-conflict | Current PON port exist MAC conflict with authorized ONU in the system. | enable |
| onu-loid-conflict | Current PON port exist LOID conflict with authorized ONU in the system. | enable |
| onu-critical-event | ONU critical link event. | enable |
| onu-dying-gasp | ONU power down. | enable |
| onu-link-fault | ONU link fault. | enable |
| onu-link-event | ONU link event | disable |
| onu-event-notific | ONU extended OAM notification | enable |

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **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} {enable|disable}** | Enable or disable ONU alarm report. |
| **Step 3** | **show alarm configuration** | Show system alarm configurations. |

## Event Management

Event severity level includes critical, major, minor and warning. Corresponding level in system log are alerts, critical, major, warnings. Event type includes device event, communication event and diposing event.

* Device event contains device reboot, PON event and so on.
* Communication event contains PON register, PON los recovery, ONU register, ONU find, ONU authorized successful, ONU deregister successful and so on.
* Disposing event contains save configuration event, erase configuration event, download configuration file successful, upload configuration file successful, ungrade successful and so on.

### System Events

System events are mainly used to monitor performation and security of system, ensure system works well.

|  |  |  |
| --- | --- | --- |
| **System event** | **Reason** | **Default** |
| reset | Device reset. | disable |
| config-save | Save configuration. | enable |
| config-erase | Erase configuration. | enable |
| download-file-success | Download file successful. | enable |
| upload-file-success | Upload file successful. | enable |
| upgrade-file-success | Upgrade firmware successful. | enable |

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **event reset {enable|disable}** | Enable or disable system event report. |
| **Step 3** | **show event configuration** | Show system event configurations. |

### PON Events

Get rid of the issue caused by PON port or fiber by monitoring PON events, ensure PON works well. The following table shows PON event list.

|  |  |  |
| --- | --- | --- |
| **PON event** | **Reason** | **Default** |
| pon-register | PON register. | disable |
| pon-los-recovery | PON los recovery. | enable |

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **event {pon-register|pon-los-recovery}****{enable|disable}** | Enble or disable PON event report. |
| **Step 3** | **show event configuration** | Show system event configurations. |

### ONU Events

ONU events also can help administrator to get rid of some ONU fault. The following table shows ONU event list.

|  |  |  |
| --- | --- | --- |
| **ONU event** | **Reason** | **Default** |
| onu-register | ONU register. | enable |
| onu-link-discover | ONU discover. | disable |
| onu-auth-success | OLT authorizes ONU successful. | enable |
| onu-deauth-success | OLT deauthorizes ONU successful. | disable |

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2b** | **event {onu-register|onu-link-discover|**  **onu-auth-success|onu-deauth-success} {enable|disable}** | Enable or disable ONU event report. |
| **Step 3** | **show event configuration** | Show system event configuration. |

# System Log



## System Log Introduction

System log is mainly used to record running condition and user operant behavior of the whole system. It is helpful for administrator to know and monitor system working condition, record abnormal information. System log comes from all the running module of system. Log system gather, manage, save and display the information. It can be shown in the deivce when you need to debug or check system status, and also can be sent to a server for long-term running status and operation tracking.

### 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.

### 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 |

## Configure System Log

### Show System Log

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **Show syslog** **[level {debug|info|notice| warning|major|critical|alert|emerg}]** | Show all system log or log of specific level. |

### Clear System Log

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **Clear syslog [level {debug|info|notice| warning|major|critical|alert|emerg}]** | Clear all system log or log of specific level. |

### Configure System Log Server

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **syslog server ip** *<A.B.C.D>* **port** *<1-65535>* | Configure system log server IP and port. |
| **Step 2b** | **no syslog server** | Delete system log server configuration. |
| **Step 3** | **show syslog server** | Show system log server configuration. |

### Configure Save Level of System Log

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter 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. |

### Save System Log to Flash

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

### Clear System Log in Flash

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

### Upload System Log

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **upload tftp syslog** *<filename> <A.B.C.D>* | Upload system log to local host byTFTP. |