**GPON OLT (Single PON) CLI**

**USER MANUAL**

**Version V1.0**

**Release Date 2024-11-12**

**Command line format conventions**

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

**Example:**

**Bold type:** gpon-olt(config)# **show running-config**

*italic type:* gpon-olt(config-aux)# **ip address** *A.B.C.D net-mask*

[ ]: gpon-olt(config)#**show pon statistics** [brief]

( x - y ): gpon-olt(config)#**show vlan** (1-4094)

< x | y | ... >:

gpon-olt(config)#**erase** <web-logo|web-logo1|web-logo2|web-logo3>

[ x | y | ... ]:

gpon-olt(config)#**show idprom interface gpon** *<S/P>* [<vendor|manufacture>]

{ x | y | ... } \*1:

gpon-olt(config)#**clear syslog** {[level] [debug|info|notice|warning|major|critical|alert|emerg]}

**CONTENTS**

[1. Access OLT 1](#_Toc13641)

[2. Command Line Interface 2](#_Toc20249)

[2.1 Abstract 2](#_Toc4052)

[2.2 CLI Configuration Mode 2](#_Toc8588)

[2.3 CLI Characteristic 3](#_Toc13656)

[2.3.1 Online Help 3](#_Toc4360)

[2.3.2 Display Characteristic 6](#_Toc8938)

[2.3.3 History Commands 6](#_Toc32736)

[2.3.4 Error Messages 7](#_Toc27868)

[2.3.5 Edit Characteristic 7](#_Toc10044)

[3. OLT Management Configuration 8](#_Toc3408)

[3.1 Configure Inband Management 8](#_Toc4078)

[3.1.1 In-band Management IPv4 Address 8](#_Toc19513)

[3.1.2 In-band Management IPv6 Address 8](#_Toc25303)

[3.2 Configure Gateway 9](#_Toc13484)

[3.2.1 Configure IPv4 Gateway 9](#_Toc21904)

[3.2.2 Configure IPv6 Gateway 9](#_Toc26989)

[3.3 Configure DNS 10](#_Toc23854)

[3.3.1 Configure IPv4 DNS 10](#_Toc31506)

[4. Port Configuration 11](#_Toc24669)

[4.1 Port Configuration 11](#_Toc13380)

[4.1.1 Enter Port Configuration Mode 11](#_Toc11050)

[4.1.2 Enable/Disable Port 11](#_Toc13526)

[4.1.3 Configure Port Description 11](#_Toc14891)

[4.1.4 Configure Port Speed 12](#_Toc15055)

[4.1.5 Configure Port Rate Limitation 12](#_Toc24558)

[4.1.6 Configure Port VLAN Mode 13](#_Toc12447)

[4.1.7 Configure Hybrid Port VLAN 14](#_Toc7890)

[4.1.8 Configure Trunk Port VLAN 14](#_Toc4626)

[4.1.9 Configure Port PVID 15](#_Toc8889)

[4.1.10 Configure Access Port VLAN 15](#_Toc1469)

[4.1.11 Configure Port Flow Control 16](#_Toc24883)

[4.1.12 Configure Port Broadcast Suppression 16](#_Toc14077)

[4.1.13 Configure Port Unknown Unicast Suppression 17](#_Toc23566)

[4.1.14 Configure Port Isolation 17](#_Toc7357)

[4.1.15 Configure Port Loopback 18](#_Toc8569)

[4.1.16 Show Port Statistics 18](#_Toc31646)

[4.1.17 Clean Port Statistics 19](#_Toc15891)

[4.1.18 Show Interface Configurations 19](#_Toc9786)

[4.1.19 Show Optical Module Parameters 20](#_Toc14495)

[4.2 Example 21](#_Toc21652)

[5. VLAN Configuration 22](#_Toc11320)

[5.1 VLAN Configuration 22](#_Toc29686)

[5.1.1 Create/Delete VLAN 22](#_Toc32051)

[5.1.2 Configure/Delete VLAN Description 22](#_Toc6855)

[5.1.3 Configure/Delete IP Address And Mask of VLAN 23](#_Toc17944)

[5.2 Show VLAN Information 23](#_Toc26665)

[6. VLAN Translation/QinQ 25](#_Toc17753)

[6.1 Configure VLAN Translation/QinQ 25](#_Toc5462)

[6.2 Example 25](#_Toc6564)

[7. MAC Address Configuration 27](#_Toc28440)

[7.1 Overview 27](#_Toc18962)

[7.2 Configure MAC Address 27](#_Toc24529)

[7.2.1 Configure MAC Address Table 27](#_Toc16510)

[7.2.2 Configure MAC Address Aging Time 28](#_Toc14058)

[7.2.3 Clean MAC Address Table 28](#_Toc20414)

[7.2.4 Configure Maximum Learnt MAC Enties of Port 28](#_Toc169)

[7.3 Show MAC Address Table 29](#_Toc27811)

[7.3.1 Show MAC Address Table 29](#_Toc6583)

[7.3.2 Show MAC Address Aging Time 29](#_Toc14304)

[8. Configure Port Mirroring 30](#_Toc17380)

[8.1 Configure Mirroring Destination Port 30](#_Toc10317)

[8.2 Configure Mirroring Source Port 30](#_Toc28131)

[8.3 Delete Port Mirroring 31](#_Toc24610)

[9. IGMP Configuration 32](#_Toc11797)

[9.1 IGMP Snooping 32](#_Toc19736)

[9.1.1 Enable/Disable IGMP Snooping 32](#_Toc12458)

[9.1.2 Configure Multicast Data Forwarding Mode 32](#_Toc29337)

[9.1.3 Configure Port Multicast VLAN 32](#_Toc7052)

[9.1.4 Configure Multicast Router Port 33](#_Toc30307)

[9.1.5 Configure Static Multicast 33](#_Toc16123)

[9.1.6 Configure Fast Leave 34](#_Toc2889)

[9.1.7 Configure Multicast Group Limit 34](#_Toc24522)

[9.1.8 Configure Parameters of Special Query 35](#_Toc29433)

[9.1.9 Configure Parameters of General Query 35](#_Toc4234)

[9.1.10 Configure Source IP of Query 36](#_Toc22252)

[9.1.11 Configure Multicast Member Aging Time 36](#_Toc31032)

[9.1.12 Show Multicast Group Information 36](#_Toc31217)

[9.2 Example 37](#_Toc10529)

[10. IPv6 MLD Configuration 39](#_Toc3823)

[10.1 MLD Snooping 39](#_Toc11544)

[10.1.1 Enable/Disable IGMP Snooping 39](#_Toc9938)

[10.1.2 Configure Port Multicast VLAN 39](#_Toc13366)

[10.1.3 Configure Multicast Router Port 40](#_Toc8123)

[10.1.4 Configure Static Multicast 40](#_Toc251)

[10.1.5 Configure Fast Leave 41](#_Toc32451)

[10.1.6 Configure Multicast Group Limit 41](#_Toc15937)

[10.1.7 Configure Parameters of Special Query 41](#_Toc15604)

[10.1.8 Configure Parameters of General Query 42](#_Toc4674)

[10.1.9 Configure Source IP of Query 42](#_Toc17234)

[10.1.10 Configure Multicast Member Aging Time 43](#_Toc28070)

[10.1.11 Show Multicast Group Information 43](#_Toc1230)

[10.2 Example 43](#_Toc20700)

[10.2.1 Requirement 43](#_Toc31831)

[10.2.2 Framework 44](#_Toc15970)

[10.2.3 Steps 44](#_Toc4218)

[11. ACL Configuration 46](#_Toc24701)

[11.1 Overview 46](#_Toc12483)

[11.2 ACL Configuration 46](#_Toc1394)

[11.2.1 Configure IP Standard ACL 46](#_Toc25483)

[11.2.2 Configure IP Extended ACL 47](#_Toc28351)

[11.2.3 Configure ACL Based on IP Address 48](#_Toc28374)

[11.2.4 Configure ACL Based on MAC Address 48](#_Toc4839)

[11.2.5 Configure ACL Based on MAC And IP Address 49](#_Toc23910)

[11.2.6 Configure ACL Based on Ports 49](#_Toc11976)

[11.2.7 Configure IPv6 Standard ACL 50](#_Toc26933)

[11.2.8 Configure IPv6 Extended ACL 51](#_Toc10913)

[11.2.9 Configure ACL Based on IPv6 Addresses 51](#_Toc24307)

[11.2.10 Configure ACL Based on IPv6 And MAC Addresses 52](#_Toc14375)

[11.3 Examples 53](#_Toc27196)

[12. QoS Configuration 54](#_Toc31323)

[12.1 Configure Queue Scheduling Mode 54](#_Toc30873)

[13. STP Configuration(Not Supported Yet) 55](#_Toc19712)

[13.1 STP Default Settings 55](#_Toc4501)

[13.2 STP Configure 55](#_Toc12520)

[13.2.1 Enable STP Function 55](#_Toc13418)

[13.2.2 Enable STP on Port 56](#_Toc19305)

[13.2.3 Configure Bridge Priority 56](#_Toc4106)

[13.2.4 Configure Forwarding Latency 57](#_Toc6843)

[13.2.5 Configure Hello Time 58](#_Toc20634)

[13.2.6 Configure Maximum Aging Time 58](#_Toc19987)

[13.2.7 Configure Priority of Port 59](#_Toc21911)

[13.2.8 Configure Path Cost of Port 59](#_Toc26541)

[13.2.9 Configure Edge Ports 60](#_Toc32310)

[13.2.10 Configure The Point-to-Point Mode 60](#_Toc16429)

[13.3 Display STP Information 61](#_Toc26052)

[14. Loop Detection Configuration 62](#_Toc32251)

[14.1 Configure Loop Detection 62](#_Toc30738)

[14.1.1 Enable/Disable Loop Detection Function 62](#_Toc26757)

[14.1.2 Configure Loop Detection Mode 62](#_Toc17970)

[14.1.3 Configure Aging Time of Loop Detection Information 63](#_Toc32398)

[14.1.4 Configure loop Detection Packet Send Method 63](#_Toc1540)

[14.1.5 Configure Time For Sending Data Packets 63](#_Toc12273)

[14.2 Configure Loop Detection Port 64](#_Toc15219)

[14.3 Display Loop Detection Information 64](#_Toc24192)

[15. DHCP Management Configuration 65](#_Toc16463)

[15.1 Configure DHCP Server 65](#_Toc9965)

[15.2 Configure DHCP Relay 65](#_Toc18462)

[15.3 Configure DHCP Snooping 66](#_Toc14811)

[16. L3 Route Configuration 69](#_Toc10082)

[16.1 Configure Static Route 69](#_Toc3717)

[17. IPv6 70](#_Toc8739)

[17.1 Configure VLAN IPv6 Address 70](#_Toc17316)

[17.2 IPv6 SLAAC 71](#_Toc25539)

[17.2.1 IPv6 SLAAC Work Processes 71](#_Toc26742)

[17.2.2 Configure IPv6 SLAAC 71](#_Toc4701)

[17.3 DHCPv6 74](#_Toc30488)

[17.3.1 DHCPv6 Overview 74](#_Toc16966)

[17.3.2 DHCPv6 Server 75](#_Toc21136)

[17.3.3 DHCPv6 Relay 79](#_Toc29286)

[17.4 IPv6 Route 82](#_Toc28213)

[17.4.1 Configure IPv6 Static Route 82](#_Toc16514)

[17.5 IPv6 Connectivity Test 83](#_Toc12638)

[18. WAN Function 84](#_Toc15535)

[18.1 WAN Configuration 84](#_Toc380)

[18.2 LAN Configuration 85](#_Toc15749)

[18.3 NAT Configuration 85](#_Toc28169)

[19. PON Management 86](#_Toc25296)

[19.1 Show PON Port Info 86](#_Toc5366)

[19.1.1 Show PON Port Info And Optical Power 86](#_Toc8903)

[19.1.2 Show PON Port Optical Power 86](#_Toc19322)

[19.1.3 Show ONU Optical Transceiver 86](#_Toc24092)

[19.2 PON Port Configuration 87](#_Toc13941)

[19.2.1 Enable/Disable PON 87](#_Toc6493)

[19.2.2 Configure P2P Function On The PON Port 87](#_Toc5823)

[19.2.3 Configure PON Port Range Function 87](#_Toc11897)

[20. ONU Management 89](#_Toc28956)

[20.1 ONU Basic Configuration 89](#_Toc8047)

[20.1.1 Display Auto-find ONU 89](#_Toc14000)

[20.1.2 Display ONU Automatic Authorization 89](#_Toc15215)

[20.1.3 Display ONU Authorization Information 89](#_Toc31265)

[20.1.4 Display ONU Authorization Details 90](#_Toc4588)

[20.1.5 Activate/Deactivate The ONU 90](#_Toc24274)

[20.1.6 ONU Authorization 90](#_Toc19326)

[20.1.7 Configure ONU Description 90](#_Toc6866)

[20.1.8 Configure ONU Whitelist 91](#_Toc32380)

[20.1.9 Display ONU Statistics 91](#_Toc27003)

[20.1.10 Configure Plug and Play 92](#_Toc1461)

[20.1.11 Configure ONU Delete Automatically 92](#_Toc31702)

[20.2 ONU Remote Configuration 92](#_Toc20919)

[20.2.1 Display ONU SFP Information 92](#_Toc7479)

[20.2.2 Upgrade ONU 93](#_Toc12672)

[20.2.3 ONU Automatic Upgrade 93](#_Toc13750)

[20.2.4 Restart ONU 94](#_Toc13716)

[20.2.5 T-cont Configuration 94](#_Toc24939)

[20.2.6 GEMPORT Configuration 94](#_Toc10434)

[20.2.7 ONU Service Configuration 95](#_Toc19100)

[20.2.8 ONU UNI Configuration 95](#_Toc13348)

[20.2.9 Display ONU Service 96](#_Toc9784)

[20.2.10 Display The ONU Capability 96](#_Toc12323)

[20.3 ONU Remote Port Configuration 96](#_Toc27994)

[20.3.1 Enable/Disable ONU Port 96](#_Toc29312)

[20.3.2 Configure ONU Port Auto-negotiation 97](#_Toc930)

[20.3.3 Configure Port Flow Control Of ONU 97](#_Toc10668)

[20.3.4 Configure Multicast VLAN 97](#_Toc14765)

[20.3.5 Configure ONU Iphost 98](#_Toc6144)

[20.3.6 Configure Port Multicast Label Of ONU 98](#_Toc21490)

[20.3.7 SFU Example 98](#_Toc21905)

[20.3.8 HGU Example 99](#_Toc16835)

[20.4 Private Configuration 100](#_Toc13741)

[20.4.1 Configure ONU ACL Rules 100](#_Toc19800)

[20.4.2 Configure ONU CATV Status 100](#_Toc5453)

[20.4.3 Configure ONU Dhcp Server 101](#_Toc5372)

[20.4.4 Configure ONU DHCPv6 Server 101](#_Toc16889)

[20.4.5 Configure ONU Equid Server 102](#_Toc24277)

[20.4.6 Restore ONU To Factory Defaults 102](#_Toc25844)

[20.4.7 Configure ONU Firewall 102](#_Toc9198)

[20.4.8 Configure ONU IGMP Mode 102](#_Toc31918)

[20.4.9 Configure ONU LAN Binding Mode 103](#_Toc21592)

[20.4.10 Configure ONU Loopback 103](#_Toc32453)

[20.4.11 Configure ONU MAC Connection 103](#_Toc9643)

[20.4.12 Configure ONU Port Isolation 104](#_Toc20261)

[20.4.13 Configure ONU Voice Port 104](#_Toc1576)

[20.4.14 Configure ONU Voice SIP Service 105](#_Toc23807)

[20.4.15 Save ONU Configuration 105](#_Toc25158)

[20.4.16 Configure ONU RSTP 105](#_Toc31928)

[20.4.17 Configure ONU Uplink Upstream Speed Limit 106](#_Toc6017)

[20.4.18 Configure ONU TR069 Management Information 106](#_Toc3575)

[20.4.19 Configure ONU UPnP 106](#_Toc1683)

[20.4.20 Configure ONU WAN Information 107](#_Toc14201)

[20.4.21 Configure ONU WIFI SSID 107](#_Toc2178)

[20.5 Rogue ONU Configuration 108](#_Toc3686)

[20.5.1 Configure Rogue ONU Detection 108](#_Toc25903)

[20.5.2 Display Rogue ONU Status 108](#_Toc27941)

[21. ONU Profile Management 109](#_Toc8007)

[21.1 Summary 109](#_Toc7687)

[21.2 ONU Profile Configuration 109](#_Toc18624)

[21.3 DBA Profile Configuration 110](#_Toc24659)

[21.4 Line Profile Configuration 111](#_Toc27730)

[21.5 Service Profile Configuration 111](#_Toc16994)

[21.6 Alarm Threshold Profile Configuration 112](#_Toc15230)

[21.7 Private Profile Configuration 113](#_Toc25073)

[21.8 IGMP Profile Configuration 117](#_Toc28207)

[21.9 Format Profile Configuration 118](#_Toc27618)

[21.10 ONU Binding Profile Configuration 118](#_Toc26611)

[21.11 Show/Delete The Profile 119](#_Toc16113)

[22. ONU Auto-learn Configuration 120](#_Toc6231)

[22.1 Enable Automatic Learn 120](#_Toc28974)

[23. System Management 121](#_Toc30462)

[23.1 Configure Management 121](#_Toc13888)

[23.1.1 Save Configuration 121](#_Toc16726)

[23.1.2 Erase Configuration 121](#_Toc21686)

[23.1.3 Show The Boot Configuration 121](#_Toc3870)

[23.1.4 Show The Running Configuration 121](#_Toc2808)

[23.1.5 Upload/Download The Configuration File 122](#_Toc15401)

[23.2 Display System Information 122](#_Toc2188)

[23.2.1 Display System Operation Information 122](#_Toc22765)

[23.2.2 Display Version Information 122](#_Toc1750)

[23.3 System Basic Configuration 123](#_Toc8426)

[23.3.1 Configure The System Name 123](#_Toc9334)

[23.3.2 Configure The Terminal Timeout Value 123](#_Toc11499)

[23.4 System Basic Operations 123](#_Toc238)

[23.4.1 Upgrade The System 123](#_Toc2223)

[23.4.2 Restart The System 124](#_Toc16961)

[23.4.3 Telnet 124](#_Toc20093)

[23.4.4 Configure The RTC System Time 124](#_Toc15517)

[23.4.5 NTP Client 124](#_Toc16559)

[23.4.6 Configure Time Zone 125](#_Toc29784)

[23.4.7 Fan Control 125](#_Toc22582)

[24. User Management 126](#_Toc13504)

[24.1 User Privilege 126](#_Toc14502)

[24.2 Default User 126](#_Toc2709)

[24.3 Add User Account 126](#_Toc15700)

[24.4 Display List of User Accounts 126](#_Toc10019)

[24.5 Delete User Account 127](#_Toc12411)

[24.6 Change Password 127](#_Toc6486)

[25. Login Management 128](#_Toc29757)

[25.1 Overview 128](#_Toc26912)

[25.2 Login Access List Configuration 128](#_Toc30420)

[25.3 Service Port Configuration 128](#_Toc8205)

[25.4 Login Configuration 129](#_Toc10010)

[25.5 Language Configuration 129](#_Toc23739)

[26. SNMP Configuration 131](#_Toc8880)

[26.1 Overview 131](#_Toc1720)

[26.2 SNMP Version And MIB 131](#_Toc14744)

[26.3 SNMP Configuration 132](#_Toc16899)

[26.3.1 Configure The Group Name 132](#_Toc19407)

[26.3.2 Configure The Trap Server Address 132](#_Toc29364)

[26.3.3 Configure Association Information 133](#_Toc26838)

[26.3.4 Configure Location Information 133](#_Toc24300)

[27. Alarm And Event Management 134](#_Toc26728)

[27.1 Description Of Alarms And Events 134](#_Toc26923)

[27.2 Alarm Management 134](#_Toc11754)

[27.2.1 System Alarm 134](#_Toc28294)

[27.2.2 PON Alarm 135](#_Toc5211)

[27.2.3 ONU Alarm 136](#_Toc28493)

[27.3 Event Management 137](#_Toc11986)

[27.3.1 System Event 138](#_Toc7714)

[27.3.2 PON Event 138](#_Toc10693)

[27.3.3 ONU Event 139](#_Toc4245)

[28. System Log 140](#_Toc15277)

[28.1 Introduction 140](#_Toc26040)

[28.1.1 Log Type 140](#_Toc18385)

[28.1.2 System Log Level 140](#_Toc6734)

[28.2 Configure System Log 141](#_Toc11308)

[28.2.1 Display System Log 141](#_Toc16261)

[28.2.2 Clear System Log 141](#_Toc15313)

[28.2.3 Configure System Log Server 141](#_Toc12373)

[28.2.4 Configure Storage Level 142](#_Toc12611)

[28.2.5 Save System Logs To The Flash 142](#_Toc760)

[28.2.6 Clear System Logs In The Flash 142](#_Toc141)

[28.2.7 Upload System Log 142](#_Toc7968)

[29. SSH Function 143](#_Toc28452)

[29.1 SSH Configuration 143](#_Toc26319)

[29.1.1 Enable The SSH Server 143](#_Toc18394)

[29.1.2 Configure Maximum Authentication Times of SSH 143](#_Toc3839)

[29.1.3 Configure SSH Authentication Timeout Period 143](#_Toc29549)

[29.1.4 Configure Maximum Number Of SSH Connections 144](#_Toc28286)

[29.1.5 Configure Maximum Number Of SSH Sessions 144](#_Toc17007)

[29.2 Display SSH 144](#_Toc31906)

[29.2.1 Display the SSH Key 144](#_Toc23456)

[29.2.2 Display SSH Configuration 145](#_Toc18128)

[30. Diagnose Function 146](#_Toc6645)

[30.1 Diagnose Configuration 146](#_Toc6876)

[30.1.1 Network Connection Test 146](#_Toc16341)

[30.1.2 Network Tracking Test 146](#_Toc21968)

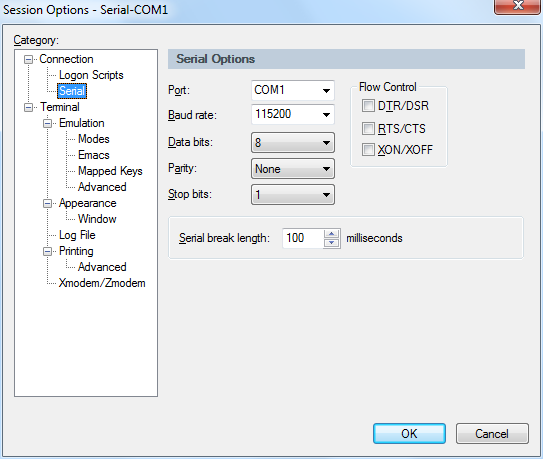
# 

# Access OLT

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

1. Connect PC serial port or USB-to-Serial port to OLT console port by console cable.
2. Run secureCRT or other simulation tools such as Putty in the PC, and set parameters as follows.

* Baudrate: 115200
* Data bits: 8
* Parity: none
* Stop bits: 1
* Flow control: none



COM port properties

After turned 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 Characteristic

### 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 Access list entry

acl Add an access list entry.

alarm Specify alarm.

alarm-event Specify alarm and event.

allow-external-route-update Allow FRR routes to be overwritten by external processes

arp Specify arp.

auto-copy Auto copy configuration

auto-upgrade Auto upgrade of ONU.

bfd Configure BFD peers

clean Clean system information.

clear Clear system information.

debug Debugging functions

dhcp-relay Dhcp relay configure.

dhcp-server Dhcp server group configuration

dhcp-snooping Dhcp snooping configure.

domainname Set system's domain name

download Download file for software upgrade or load user config.

dst Set DST(Before using DST, please configure commands to enable ntp server.)

duid DHCP Unique Identifier

enable Modify enable password parameters

end End current mode and change to enable mode

erase Erase info from flash.

event Specify event.

evpn EVPN

exec exec cmd

exit Exit current mode and down to previous mode

fan Specify olt fan management.

find Find CLI command matching a regular expression

fpm Forwarding Plane Manager configuration

frr FRRouting global parameters

gpon gpon.

hostname Set system's network name

interface Select an interface to configure

ip System ip configuration.

ip-dscp Configure egress ip dscp.

ipv6 IPv6 Information

key Authentication key management

line Configure a terminal line

list Print command list

log Logging control

log-filter Filter Logs

login-access-list Login-access list entry.

loopback Error detection on loopback

mac MAC address

monitor Configure SPAN mirroring.

mpls MPLS information

nexthop-group Nexthop Group configuration

no Negate a command or set its defaults

ntp Configure NTP

onu Specify onu information.

onu-schedule-reboot Schedule Reboot ONU task.

output Direct vtysh output to file

p2p Specify p2p feature.

password Modify the terminal connection password

ping Send echo messages

profile Select profile to configure.

pseudowire Static pseudowire configuration

queue-scheduler Configure qos functionality.

quit Exit current mode and down to previous mode

reboot Reboot the switch.

remote remote server config

remove Negate a command or set its defaults

rogue-onu-ctrl Rogue onu control.

rogue-onu-detect Config rogue onu detection

route-map Create route-map or enter route-map command mode

router Enable a routing process

router-id Manually set the router-id

save Save system information.

service Set up miscellaneous service

set Set system configuration.

show Show running system information

snmp Snmp server config

snmp-server Snmp server config

software Software information.

spanning-tree Config STPD information.

ssh ssh server config

sshd SSH Configuration interface

syslog Specific system log save level, which syslog level not less than level will save to flash.

telnet Telnet Configuration interface

terminal Set terminal line parameters

time Specify system time configuration.

timezone Set Time Zone.

upgrade Specify upgrade system.

upload Upload file for software or user config.

user User

vlan Vlan commands.Please input vlan ID you want to create.

vni VNI corresponding to the DEFAULT VRF

vrf Select a VRF to configure

web Specify web.

write Write running configuration to memory, network, or terminal

zebra Zebra information

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

gigabitEthernet GigabitEthernet IEEE 802.3z.

gpon Specify gpon module.

loopback Config loopback interface

vlan Config vlan information.

wan System wan configuration.

1. Input “?” behind a command, it will display description of parameters when this site should be a parameter.

gpon-olt(config)# acl

(1-7999) Rule index.

disable Don't activate the entry.

effective Effective period.

enable Make entry active.

ipv6 IPv6 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

end End current mode and change to enable mode

erase Erase info from flash.

event Specify event.

evpn EVPN

exec exec 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.

When the command is unique, the command is automatically fully completed:

gpon-olt(config)# g

gpon-olt(config)# gpon

If not unique, all commands that can be completed are displayed:

gpon-olt(config)# u

upgrade upload user

### Display Characteristic

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

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

### 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 Characteristic

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

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

# OLT Management Configuration



## Configure Inband Management

### In-band Management IPv4 Address

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 vlan** [*vlan\_id*] | Show VLAN information. |
| **Step 8** | **write** | Save configurations. |

### In-band Management IPv6 Address

|  |  |  |
| --- | --- | --- |
|  | **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** | **ipv6 address** *X:X::X:X/M* [eui-64] | Configure IPv6 address and prefix. |
| **Step 5b** | **no ipv6 address** [*X:X::X:X/M* [eui-64]] | Delete IPv6 address and mask. |
| **Step 6** | **exit** | Exit to global configuration mode. |
| **Step 7** | **show vlan** [*vlan\_id*] | Show VLAN information. |
| **Step 8** | **write** | Save configurations. |

## Configure Gateway

### Configure IPv4 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 IPv4 gateway as the following table shows.

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

### Configure IPv6 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 IPv6 gateway as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **ipv6 gateway** *X:X::X:X*[**vlan** *vlan\_id*] | Configure IPv6 gateway. |
| **Step 3** | **no ipv6 gateway** | Delete IPv6 gateway. |
| **Step 4** | **show ipv6 gateway** | Show IPv6 gateway configuration. |
| **Step 5** | **write** | Save configurations. |

## Configure DNS

### Configure IPv4 DNS

It can configure two IPv4 DNS servers.

|  |  |  |
| --- | --- | --- |
|  | **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 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 3** | **speed** < 10 | 100 | 1000 | 10000|auto > | Configure port speed. |
| **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** < access | trunk | hybrid> **vlan** *vlan\_id* | 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 4.1.9.

### 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** | **switchport** <hybrid|trunk> **pvid vlan 1** | Reset hybrid or trunk port PVID to default 1. |
| **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** *vlan\_id* | Delete access port VLAN |
| **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** | **flowcontrol off** | 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: 64-13000, 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 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 unknow bps** *value* | Configure unknown unicast suppression.  Value range: 64-1000000, it should be integral multiple of 64kbps. |
| **Step 3b** | **no storm-control unknow** | Remove unknown unicast suppression. |
| **Step 4** | **exit** | Exit global configuration mode. |
| **Step 5** | **show interface** *interface\_type slot/port* | Show interface configurations. |
| **Step 6** | **write** | Save configurations. |

### 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 5** | **show interface** *interface\_type slot/port* | Show interface configurations. |
| **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 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. |

### 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 statistics** | 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 stands for GPON port 1.For example, display configurations of uplink port 1.

gpon-olt(config)# show int gigabitethernet 0/1

Interface gigabitEthernet 0/1's information.

GigabitEthernet0/1 current state : up

Description:

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

Link speed type: autonegotiation, Link duplex type: autonegotiation

Current link state: Up

Current autonegotiation mode: enable

Current link speed: 100Mbps, Current link mode: full-duplex

Inter Packet Gap: 0 ns(null) Flow Control: disable

jumboframe :disable The Maximum Frame Length is 1536

Broadcast storm control: 1496 Kbps

Multicast storm control: disable

Unknow unicast storm control: 1496 Kbps

Ingress line rate control: no limit

Egress line rate control: no limit

mac address learn state : enable, no limit

Port priority: 0

Port combo mode: null

Isolate member : no

Port link-type: hybrid

PVID: 1

Untagged VLAN ID: 1

Tagged VLAN ID : 3000 100

Last 300 seconds input: 0 packets/sec Last 300 seconds output: 0 packet s/sec

Input(total): 27 packets, 1887 bytes

1 broadcasts, 0 multicast

Input(normal): 27 packets, 0 bytes

0 broadcasts, 0 multicast, 0 pauses

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

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

Output(total): 118 packets, 7691 bytes

20 broadcasts, 93 multicast

Output(normal): 118 packets, 0 bytes

20 broadcasts, 93 multicast, 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

### Show Optical Module Parameters

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **show gigabitethernet optical transceiver** | Show the information of the optical uplink port 3. |
| **Step 3** | **interface gpon 0/1** | Enter interface configuration mode. |
| **Step 4** | **show pon optical transceiver** | Show the information of the optical gpon port. |

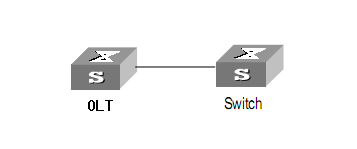
## Example

Configure VLAN and broadcast suppression of trunk mode port.

**1.Requirement**

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

**2.Framework**



**3.Steps**

(1)Enter interface configuration mode.

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

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

(2)Configure port mode and add VLAN

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

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

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

PS. The VLAN must be added first. Please refer to 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 bps 64

# 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* | Show VLAN configurations.  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** | **vlan** *vlan\_id* | Create VLAN or enter VLAN 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 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** | Delete IP address and mask of VLAN. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show 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 vlan** |
| Show VLAN port members | **show vlan** *vlan-id* |

**Example:**

Show VLAN 3000 port members

gpon-olt(config)# show vlan 3000

Vlan ID : 3000

Name : vlan\_3000

IPv6 Address :

Link-Local address:

fe80::6e68:a4ff:fe21:a68

Mac Address : 6c:68:a4:21:0a:68

Tagged Ports : ge0/1

Untagged Ports :

**Notice**:

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

Vlan ID : 1

Name : vlan\_1

IP Address : 192.168.1.1/24

IPv6 Address :

Link-Local address:

fe80::6e68:a4ff:fe21:a68

Mac Address : 6c:68:a4:21:0a:68

Tagged Ports :

Untagged Ports : ge0/1 ge0/2 ge0/3

# 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-mapping** (1-4094) *<*any|(0-7)*>* (1-4094) <any|(0-7)> <db-tagged|one-tagged> | Configure VLAN translation/QinQ.  db-tag means QinQ.  one-tag means translation. |
| S**tep 3b** | **no dot1q-tunnel vlan-mapping** (1-4094) (1-4094) | Delete VLAN translation/QinQ. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show vlan dot1q-tunnel vlan-mapping** | Show VLAN translation/QinQ configurations. |
| **Step 6** | **write** | Save configurations. |

## Example

**(1)VLAN Translation**

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

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

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

gpon-olt (config-if)#switchport hybrid vlan 200 tagged

gpon-olt(config-if)#dot1q-tunnel vlan-mapping 100 1 200 2 one-tagged

gpon-olt (config)#show vlan dot1q-tunnel vlan-mapping

**(2)QinQ function**

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

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

gpon-olt (config-if)#switchport hybrid vlan 300 tagged

gpon-olt (config-if)#switchport hybrid vlan 400 tagged

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

gpon-olt (config)#show vlan dot1q-tunnel vlan-mapping

# 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 process 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**xx:xx:xx:xx:xx:xx* **interface** *interface\_type slot/port* | Add static MAC address entry. |
| **Step 2b** | **no mac address-table vlan** *vlan\_id xx:xx:xx:xx:xx:xx* | Delete MAC address entry. |
| **Step 2c** | **clean mac address-table** | 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 aging-time** *value* | Configure MAC address aging time, range is 10-1000000s.  0s means don’t aging.  Default is 300s. |
| **Step 3** | **show mac address-table aging-time** | Show aging time. |
| **Step 4** | **write** | Save configurations. |

### 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** | **clean mac address-table** [interface *interface\_type slot/port* |pon] | 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 based on Ethernet port. |
| **Step 2b** | **show mac address-table vlan** *vlan\_id* | Show MAC address table based on VLAN ID. |
| **Step 2c** | **show mac address-table** | Show whole MAC address table. |

### 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 aging-time** | 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 slot/port* | Configure mirroring destination port.  Session number is 1. |
| **Step 3** | **show monitor session** *session\_number* | 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.  **Both** means received data and transmitted data.  **rx** means received data.  **tx** means transmitted data. |
| **Step 3** | **show monitor session** *session\_number* | 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* | Delete port mirroring. session\_number is 1 |
| **Step 3** | **show monitor session** *session\_number* | 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** (1-4094) **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** (1-4094) **group-vlan** (1-4094) [tagged | untagged ] | Configure port multicast VLAN.  VLAN range is 1-4094. |
| **Step 3b** | **no ip igmp snooping group-vlan** (1-4094) | Delete port multicast VLAN. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show ip igmp snooping user-vlan** | Show multicast VLAN. |
| **Step 6** | **write** | Save configurations. |

### 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** (1-4094)**interface** *interface\_type slot/port* | Configure multcast router port .  VLAN range is 1-4094. |
| **Step 2b** | **no ip igmp snooping mrouter vlan** (1-4094)**interface** *interface\_type slot/port* | Delete multicast router port. |
| **Step 3** | **show ip igmp snooping mrouter vlan** [all | *vlan\_id*] | 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** (1-4094) *A.B.C.D* **interface** [gigabitEthernet |gpon ] *slot:<0>/port:<1-x>* | Configure static multicast. |
| **Step 2b** | **no ip igmp snooping static vlan** (1-4094) *A.B.C.D* **interface** [gigabitEthernet |gpon ] *slot:<0>/port:<1-x>* | 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** (0-256) | 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 Group Information

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **show ip igmp snooping vlan** [(1-4096) | all] | Show multicast group information. |
| **Step 2b** | **show ip igmp snooping statistic** | Show multicast statistic. |

## 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 gigabitethernet 0/1

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

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

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

gpon-olt(config-pon-0/1)# ip igmp snooping user-vlan 100 group-vlan 100 tagged

gpon-olt(config-pon-0/1)# exit

(3)Enable IGMP Snooping

gpon-olt(config)# ip igmp snooping enable

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

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

(5)Configure the onu

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

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

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

gpon-olt(config-pon-0/1)# onu 1 gemport 1 tcont 1 gemport\_name gem\_1

gpon-olt(config-pon-0/1)#onu 1 service ser\_1 gemport 1 vlan 100

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

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

# IPv6 MLD Configuration

## MLD Snooping

### Enable/Disable IGMP Snooping

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

Begin at privileged configuration mode, enable/disable MLD snooping as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **ipv6 mld snooping** | Enable MLD Snooping. |
| **Step 2b** | **no ipv6 mld snooping** | Disable MLD snooping. |
| **Step 3** | **show ipv6 mld snooping** | Show MLD snooping configurations. |
| **Step 4** | **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** | **Ipv6 mld snooping user-vlan** (1-4094) **group-vlan** (1-4094) | Configure port multicast VLAN.  VLAN range is 1-4094. |
| **Step 3b** | **no ipv6 mld snooping user-vlan** (1-4094) **group-vlan** (1-4094) | Delete port multicast VLAN. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show ipv6 mld snooping user-vlan** | Show multicast VLAN. |
| **Step 6** | **write** | Save configurations. |

### Configure Multicast Router Port

Multicast router port is used to forward MLD 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** | **ipv6 mld snooping vlan** (1-4094) **mrouter interface gigabitethernet** *slot:<0>/port:<1-x>* | Configure multcast router port .  VLAN range is 1-4094. |
| **Step 2b** | **no ipv6 mld snooping vlan** (1-4094) **mrouter interface gigabitethernet** *slot:<0>/port:<1-x>* | Delete multicast router port. |
| **Step 3** | **show ipv6 mld snooping mroute** | 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** | **Ipv6 mld snooping vlan** (1-4094) **static** *X:X::X:X* **interface** <gigabitethernet *slot:<0>/port:<1-x>* | gpon *slot:<0>/port:<1-x>*> | Configure static multicast. |
| **Step 2b** | **no ipv6 mld snooping vlan** (1-4094) **static** *X:X::X:X* **interface** <gigabitethernet *slot:<0>/port:<1-x>* | gpon *slot:<0>/port:<1-x>*> | Delete static multicast. |
| **Step 3** | **show ipv6 mld snooping address** | Show static MLD 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** | **ipv6 mld snooping immediate-leave** | Enable fast leave. |
| **Step 3b** | **no ipv6 mld snooping immediate-leave** | Disable fast leave. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show ipv6 mld snooping interface** | Show port mld information. |
| **Step 6** | **write** | Save configurations. |

### 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** | **ipv6 mld snooping group-limit**  (0-256) | Configure port multicast group limitation. |
| **Step 3b** | **no ipv6 mld snooping group-limit** | Reset multicast group limitation to default. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show ipv6 mld snooping interface** | Show port multicast information. |
| **Step 6** | **write** | Save configurations. |

### 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** | **ipv6 mld snooping last-listener-query-count**  (1-7) | Configure specific query count. Default is 2. |
| **Step 2b** | **ipv6 mld snooping last-listener-query-interval** (1-255) | Configure specific query interval. Default is 1s. |
| **Step 2c** | **ipv6 mld snooping last-listener-query-response** (1-255) | Configure specific query response time. Default is 1s. |
| **Step 3** | **show ipv6 mld snooping** | Show 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** | **ipv6 mld snooping general-query-packet** | Enable general query function. Default is disable. |
| **Step 2b** | **no ipv6 mld snooping general-query-packet** | Disable general query function. Default is disable. |
| **Step 2b** | **ipv6 mld snooping general-query-interval**  (10-3600) | Configure general query interval. Default is 126s. |
| **Step 3** | **show ipv6 mld snooping** | 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** | **ipv6 mld snooping general-query-source-ip**  *X:X::X:X* | Configure source IP of query message. Default is fe80::1. |
| **Step 3** | **show ipv6 mld snooping** | Show MLD configurations. |
| **Step 4** | **write** | Save configurations. |

### 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 multicast member aging time as the following table shows.

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

### Show Multicast Group 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 ipv6 mld snooping address** | Show multicast group information. |
| **Step 2b** | **show ipv6 mld snooping statistics** | Show multicast statistic. |

## Example

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

### Requirement

In order to achieve multicast function, you should enable MLD 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.

### Framework



### Steps

(1)Create VLAN

gpon-olt (config)# vlan 100

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

(2)Configure multcast VLAN100

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

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

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

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

gpon-olt(config-pon-0/1)# ipv6 mld snooping user-vlan 100 group-vlan 100

gpon-olt(config-pon-0/1)# exit

(3)Enable MLD Snooping

gpon-olt(config)# ipv6 mld snooping

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

gpon-olt(config)# ipv6 mld snooping vlan 100 mroute interface gigabitethernet 0/1

(5)Configure the onu

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

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

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

gpon-olt(config-pon-0/1)# onu 1 gemport 1 tcont 1 gemport\_name gem\_1

gpon-olt(config-pon-0/1)#onu 1 service ser\_1 gemport 1 vlan 100

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

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

# 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 | Maximum rules |
| IP Standard ACL | 0-999 | 1000 |
| IP Extended ACL | 1000-1999 | 1000 |
| ACL based on MAC address | 2000-2999 | 1000 |
| ACL based on port binding | 5000-5999 | 1000 |
| ACL based on QoS | 6000-6999 | 1000 |

## ACL Configuration

### Configure 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** | **acl** *rule index.* | Enter ACL configuration mode.  rule index range:1-999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out >  **subset** < permit | deny > < both | in | out > < dest-ip | src-ip > *A.B.C.D net-mask* | Configure ACL rule.  define based on interface ACL rule.  A.B.C.D: define based on source/destination IP address and mask ACL rule. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl disable** | Disable ACL. |
| **Step 3d** | **no acl** *index* | Delete the acl |
| **Step 4** | **show acl** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure 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 configuration mode. |
| **Step 2** | **acl** *rule index.* | Enter ACL configuration mode.  rule index range:1000-1999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out > < dest-ip *A.B.C.D net-mask* | src-ip *A.B.C.D net-mask* dest-ip *A.B.C.D net-mask*| protocol < (0-255) | egp | gre | icmp | igmp | ipinip | ospf | pim | rsvp | tcp | udp > [ dest-ip *A.B.C.D net-mask* | src-ip [ dest-ip *A.B.C.D net-mask* ] > | Configure IP extended ACL rule.  Parameter *protocol* should be icmp, igmp, egp, ipinip, ospf, pim, tcp, or udp, etc. it also can be replaced by protocol code 0~255. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl disable** | Disable ACL. |
| **Step 3d** | **no acl** *index* | Delete the acl |
| **Step 4** | **show acl** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure ACL Based on IP Address

begin at the privilege configuration mode, apply the ACL rules to the IP as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **acl** (1000-1999) | Enter ACL configuration mode.  range:1000-1999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out > < dest-ip *A.B.C.D net-mask* | src-ip *A.B.C.D net-mask* dest-ip *A.B.C.D net-mask*| protocol < (0-255) | egp | gre | icmp | igmp | ipinip | ospf | pim | rsvp | tcp | udp > [ dest-ip *A.B.C.D net-mask* | src-ip [ dest-ip *A.B.C.D net-mask* ] ]> | Configure IP ACL rule. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl disable** | Disable ACL. |
| **Step 3d** | **no acl** *index* | Delete the acl |
| **Step 4** | **show acl** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure ACL Based on MAC Address

begin at the privilege configuration mode, apply the ACL rules to the MAC as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **acl** (2000-2999) | Enter ACL configuration mode.  range:2000-2999. |
| **Step 3a** | **subset** < permit | deny > **in src-mac** *X:X:X:X:X:X* | Configure IP extended ACL rule. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl disable** | Disable ACL. |
| **Step 3d** | **no acl** *index* | Delete the acl |
| **Step 4** | **show acl** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure ACL Based on MAC And IP Address

begin at the privilege configuration mode, apply the ACL rules to the MAC and IP as the following table shows.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **acl** (5000-5999) | Enter ACL configuration mode.  *access-list-number* is ACL index. range:5000-5999. |
| **Step 3a** | **subset** < permit | deny > **in src-mac** *X:X:X:X:X:X* < dest-ip *A.B.C.D net-mask* | src-ip *A.B.C.D net-mask* [ dest-ip *A.B.C.D net-mask* ] > | Permit:Permit data stream which match the rule passing through.  Deny:Do not permit data stream which match the rule passing through.  src-mac :source MAC address  *X:X:X:X:X:X*：MAC address mask |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl disable** | Disable ACL. |
| **Step 3d** | **no acl** *index* | Delete the acl |
| **Step 4** | **show acl** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure ACL Based on Ports

This type of ACL includes other types.

Start from the privilege configuration mode and configure ACLs based on port binding, as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **acl** (5000-5999) | Enter the ACL configuration mode.  The ID of the access list is an ACL index. The value ranges from 5000-5999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out > **protocol** < tcp | udp > { dest-port (0-65535) | src-port (0-65535) | src-ip *A.B.C.D net-mask* | src-ip *A.B.C.D net-mask* }\*1 | src ip: indicates the source ip address  dest ip: indicates the destination ip address  Protocol: IP protocol type  src-port: indicates the Layer 4 source port  dest-port: indicates the Layer 4 destination port |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl disable** | Disable ACL. |
| **Step 3d** | **no acl** *index* | Delete the acl |
| **Step 4** | **show acl** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure IPv6 Standard ACL

begin at the privileged configuration mode, configure the IPV6 standard ACL according to the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **acl ipv6** (1-999) | Enter the ACL configuration mode.  An access list is an ACL index. The value ranges from 1 to 999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out >  **subset** < permit | deny > < both | in | out > < dest-ipv6 | src-ipv6 > *X:X::X:X/M* | Configure ACL rule.  define based on interface ACL rule. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl ipv6 disable** | Disable ACL. |
| **Step 3d** | **no acl ipv6** *index* | Delete the acl |
| **Step 4** | **show acl ipv6** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure IPv6 Extended ACL

begin at the privileged configuration mode, configure the IPV6 extended ACL according to the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **acl ipv6** (1000-1999) | Enter the ACL configuration mode.  The ID of the access list is an ACL index. The value ranges from 1000 to 1999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out > < dest-ipv6  *X:X::X:X/M* | src-ipv6  *X:X::X:X/M* dest-ipv6  *X:X::X:X/M* | protocol < (0-255) | icmpv6 | ospf | tcp | udp > [ dest-ip *A.B.C.D net-mask* | src-ip [ dest-ip *A.B.C.D net-mask* ] > | Configure IP extended ACL rule.  Parameter *protocol* should be icmpv6,ospf, tcp, or udp. it also can be replaced by protocol code 0~255. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl ipv6 disable** | Disable ACL. |
| **Step 3d** | **no acl ipv6** *index* | Delete the acl |
| **Step 4** | **show acl ipv6** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure ACL Based on IPv6 Addresses

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **acl ipv6** (1000-1999) | Enter ACL configuration mode.  range:1000-1999. |
| **Step 3a** | **subset** < permit | deny > < both | in | out > < dest-ipv6 *X:X::X:X/M* | src-ipv6 *X:X::X:X/M* dest-ipv6 *X:X::X:X/M*| protocol < (0-255) | icmpv6 | ospf | tcp | udp > [ dest-ipv6 *X:X::X:X/M* | src-ipv6 [ dest-ipv6 *X:X::X:X/M* ] ] > | Configure IP ACL rule. |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl ipv6 disable** | Disable ACL. |
| **Step 3d** | **no acl ipv6** *index* | Delete the acl |
| **Step 4** | **show acl ipv6** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

### Configure ACL Based on IPv6 And MAC Addresses

begin at the privilege configuration mode, ACL rules are applied to both IP and MAC addresses, as shown in the following table

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **acl ipv6** (5000-5999) | Enter the ACL configuration mode.  The ID of the access list is an ACL index. The value ranges from 5000-5999. |
| **Step 3a** | **subset** < permit | deny > **in src-mac** *X:X:X:X:X:X* < dest-ipv6 *X:X::X:X/M* | src-ipv6 *X:X::X:X/M* [ dest-ipv6 *X:X::X:X/M* ] > | Permit:Permit data stream which match the rule passing through.  Deny:Do not permit data stream which match the rule passing through.  src-mac :source MAC address  *X:X:X:X:X:X*：MAC address mask |
| **Step 3b** | **exit** | Exit to global configuration mode. |
| **Step 3c** | **acl ipv6 disable** | Disable ACL. |
| **Step 3d** | **no acl ipv6** *index* | Delete the acl |
| **Step 4** | **show acl ipv6** < *rule index* | all > | Show ACL configurations. |
| **Step 5** | **write** | Save configurations. |

## Examples

**(1)Reject packets with specific IP addresses**

PON1 denies the packet whose source IP address is 192.168.100.10.

gpon-olt(config)# acl enable

gpon-olt(config)# acl 5000

gpon-olt(config-acl-5000)# subset deny both src-ip 192.168.100.10 255.255.255.255

gpon-olt(config-acl-5000)# exit

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

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

gpon-olt(config)# acl enable

gpon-olt(config)#acl 2000

gpon-olt(config-acl-2000)# subset deny in

gpon-olt(config-acl-2000)#exit

gpon-olt(config)# acl 2001

gpon-olt(config-acl-2001)# subset permit in src-mac b8:97:5a:72:37:8d ff:ff:ff:ff:ff:ff

gpon-olt(config-acl-2001) # exit

# QoS Configuration



## Configure Queue Scheduling Mode

Queue scheduling modes include strict priority, weighted cyclic scheduling and mixed scheduling. The device supports a total of eight queues.

begin at the privilege configuration mode, configure the queue scheduling mode as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2a** | **queue-scheduler sp** | Configure the strict priority scheduling mode |
| **Step 2b** | **queue-scheduler wrr** [*queue1*|*queue2*|*queue3*|*queue4*] | Set the weighted cyclic scheduling mode. Queuex is the weight of queue x. The value ranges from 1 to 100. |
| **Step 3** | **show queue-scheduler** | Displays the queue scheduling configuration. |
| **Step 4** | **write** | Save configuration |

# STP Configuration(Not Supported Yet)



## 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 :20000  Gigabit Ethernet :20000 |
| Hello time | 2s |
| Forward delay time | 15s |
| Maximum aging time | 20s |
| Mode | RSTP |

## STP Configure

STP configuration includes:

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

### Enable STP Function

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2a** | **spanning-tree on** | Enable the STP function on the device. By default, STP is disabled. |
| **Step 2b** | **no spanning-tree** | The STP function of the device is disabled |
| **Step 3a** | **interface vlan** *vlan\_id* | Enter VLAN interface configuration mode. |
| **Step 3b** | **show spanning-tree** | Show STP configuration |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **write** | Save configuration |

### Enable STP on Port

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

begin at the privileged configuration mode, enable the STP function on the port, as shown in the following table.

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

### Configure Bridge Priority

The bridge priority of the device determines whether it will be selected as the root of the tree.

begin at the privilege configuration mode, configure the bridge priority of the device as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **spanning-tree priority** *bridge-priority* | Configure the bridge priority of the device. The priority ranges from 0 to 61440. The default value is 32768. |
| **Step 3** | **show running-config** | Show STP configuration |
| **Step 4** | **write** | Save configuration |

### Configure Forwarding Latency

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

Begin at the privileged configuration mode, configure the forwarding delay of the device according to the following table.

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

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

|  |
| --- |
| **Attention:**  Hello Time, Forward Delay, and Max Age are the time parameters of the root device. These three parameters should meet the following formula, otherwise, the network will be unstable.  2 × (forward delay-1) >= maximum age  maximum age >= 2 × (hello + 1)  The unit of “1” in formula is second. |

### Configure Hello Time

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

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

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

### Configure Maximum Aging Time

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

begin at the privileged configuration mode, set the maximum aging time according to the following table.

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

### Configure Priority of Port

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

begin at privilege configuration mode, configure the priority of the specified port as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **interface** *interface\_type slot/port* | The port configuration mode is displayed |
| **Step 3** | **spanning-tree port-priority** *priority* | Configures the priority of a specified port. The priority ranges from 0 to 240. The default value is 128. |
| **Step 4** | **exit** | Exit the global configuration mode |
| **Step 5** | **show running-config** | The STP configuration of the port is displayed |
| **Step 6** | **write** | Save configure |

### Configure Path Cost of Port

The path cost is related to the speed of the link connected to the port. On an STP switch, different path costs can be configured for a port.

begin at privileged configuration mode, configure the path cost of the specified port, as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **interface** *interface\_type slot/port* | The port configuration mode is displayed |
| **Step 3** | **spanning-tree cost** [ *value* | auto ] | The path cost of a specified port is specified. The path cost ranges from 1 to 200000000. The default value is 200000. |
| **Step 4** | **exit** | Exit the global configuration mode |
| **Step 5** | **show running-config** | The STP configuration of the port is displayed |
| **Step 6** | **write** | Save configure |

### Configure Edge Ports

The port connected to the terminal host is an edge port. During the spanning tree recalculation, the edge port can be directly converted to the forward state, thus reducing the transmission time. Since RSTP cannot detect whether a port is an edge port, it is best to configure a port as an edge port if it is not connected to a switch. However, when a port is connected to a switch, RSTP can detect and configure it as a non-edge port. By default, all ports are configured as non-edge ports.

Starting in privileged configuration mode, configure the edge port as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **interface** *interface\_type slot/port* | The port configuration mode is displayed |
| **Step 3a** | **spanning-tree operEdge** | Configure the port as an edge port |
| **Step 3b** | **no spanning-tree operEdge** | Reset the spanning tree port to the default value |
| **Step 4** | **exit** | Exit the global configuration mode |
| **Step 5** | **show running-config** | The STP configuration of the port is displayed |
| **Step 6** | **write** | Save configure |

### Configure The Point-to-Point Mode

Point-to-point mode is usually a link to a switch. A port connected by a point-to-point link can quickly transition to the forwarding state by sending synchronous packets when certain port role conditions are met, thus reducing unnecessary forwarding delay.

begin at the privileged configuration mode, configure the port point-to-point link, as shown in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **interface** *interface\_type slot/port* | The port configuration mode is displayed |
| **Step 3a** | **spanning-tree point-to-point** [ auto ] | Configure the port as a point-to-point port. By default, all ports are configured as point-to-point ports. |
| **Step 3b** | **no spanning-tree point-to-point** | Example Delete the configuration of a point-to-point port |
| **Step 4** | **exit** | Exit the global configuration mode |
| **Step 5** | **show running-config** | The STP configuration of the port is displayed |
| **Step 6** | **write** | The STP configuration of the port is displayed |

## Display STP Information

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

|  |  |
| --- | --- |
| **Command** | **Function** |
| **show spanning-tree** | Displays the STP configuration and running status |
| **show running-config** | Displays the STP configuration and port running status |

# Loop Detection Configuration

## Configure Loop Detection

### Enable/Disable Loop Detection Function

Loopback Detect is disabled by default. You can enable it with the following command.

begin at the privileged configuration mode, enable/disable Loopback Detect listening, as shown in the following table.

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

### Configure Loop Detection Mode

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

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

### Configure Aging Time of Loop Detection Information

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

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

### Configure loop Detection Packet Send Method

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **loopback packet-send port-base** (1-720) | Set the packet sending mode to the port |
| **Step 3** | **loopback packet-send vlan-base** (1-720) | Set the packet sending mode to the vlan |
| **Step 4** | **write** | Save configure |

### Configure Time For Sending Data Packets

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **loopback packet-send <** port-base | vlan-base > (1-720) | Set the packet sending interval,range:1-720 |
| **Step 3** | **show loopback detect** | Display loop information |
| **Step 4** | **write** | Save configure |

## Configure Loop Detection Port

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **interface** *interface\_type slot/port* | The port configuration mode is displayed |
| **Step 3** | **loopback enable** | Loop detection is enabled for the port |
| **Step 4** | **loopback disable** | The loop detection function is disabled on the port |
| **Step 5** | **exit** | Exit the port configuration mode |
| **Step 6** | **show loopback detect port** | Displays loop detection configurations |
| **Step 7** | **write** | Save configure |

## Display Loop Detection Information

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

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

# DHCP Management Configuration

## Configure DHCP Server

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter the global configuration mode |
| **Step 2a** | **dhcp-server interface vlan** *vlan\_id* | Configure the vlan based on which the DHCP address pool is based |
| **Step 2b** | **dhcp-server address** *hostname* | Configure the hostname of the DHCP IP address pool |
| **Step 2c** | **dhcp-server startip** *A.B.C.D* **endip** *A.B.C.D* | Configure the range of the DHCP IP address pool |
| **Step 2d** | **dhcp-server subnet** *A.B.C.D* | Configure the DHCP mask |
| **Step 2e** | **dhcp-server wins** *A.B.C.D* | The DHCP WINS server is configured |
| **Step 2f** | **dhcp-server gateway** *A.B.C.D* | Configuring a DHCP Gateway |
| **Step 2g** | **dhcp-server dns1** *A.B.C.D*  **dhcp-server dns2** *A.B.C.D*  **dhcp-server dns3** *A.B.C.D* | Configure the dns of the DHCP IP address pool |
| **Step 2h** | **dhcp-server leasetime** *leasetime* | Configure the IP address lease time.range:60s-864000s.default lease time is 864000s. |
| **Step 3** | **dhcp-server enable** | Enable DHCP IP address pool |
| **Step 4** | **show dhcp-server** | The DHCP server configuration is displayed |
| **Step 5** | **write** | Save configure |

## Configure DHCP Relay

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

1.Single DHCP relay configuration：

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode |
| **Step 2** | **interface vlan** (1-4094) | Add VLAN and enter VLAN interface configuration  *vlan\_id(*1－4094) |
| **Step 3** | **dhcp relay** *A.B.C.D* | Configure the DHP relay server IP address ,and enable the DHCP relay |
| **Step 3b** | **no ip 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** | **write** | 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 2a** | **dhcp-snooping enable** | Enable DHCP Snooping.（DHCP Snooping enable，can not open dhcp server and dhcp relay） |
| **Step 2b** | **dhcp-snooping disable** | disable DHCP Snooping |
| **Step 3a** | **dhcp-snooping vlan** (1-4094)[to (1-4094)] | Configure DHCP Snooping vlan list |
| **Step3b** | **no dhcp-snooping vlan** (1-4094)[to (1-4094)] | Delete DHCP Snooping vlan list |
| **Step 4** | **show dhcp-snooping configuration** | Show DHCP Snooping configuration |
| **Step 5** | **write** | Save configuration |

B.Configure DHCP Snooping option82

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

C.Configure DHCP Snooping binding list

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode |
| **Step 2** | **dhcp-snooping binding** *X:X:X:X:X:X* **vlan** (1-4094)*A.B.C.D* **interface** *interface\_type slot/port* **lease** (60-1000000) | Add the static DHCP binding list |
|  | **no dhcp-snooping binding mac** *X:X:X:X:X:X* | 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** | **show dhcp-snooping configuration** | Show DHCP Snooping configuration |
| **Step 5** | **write** | Save configuration |

D.Configure DHCP Snooping port

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter global configuration mode |
| **Step 2** | **interface** *interface\_type slot/port* | Enter the interface configuration |
| **Step 3a** | **dhcp-snooping trust** | Configure the trust port. All the port are untrust in default |
| **Step 3b** | **dhcp-snooping untrust** | Delete trust port. |
| **Step 3c** | **dhcp-snooping information circuit-id string** *string* | Configure the option82 circuit-id value |
| **Step 3d** | **no dhcp-snooping information circuit-id string** | Delete option82 circuit-id value,load default value |
| **Step 3e** | **dhcp-snooping information remote-id string** *string* | Configure option82 remote-id value |
| **Step 3f** | **no dhcp-snooping information remote-id string** | Delete option82 remote-id value，load default value |
| **Step 3g** | **dhcp-snooping limit rate** (0-4096) | Configure the port max speed of receiving the DHCP packet. It doesn't limit by default |
| **Step 3h** | **no dhcp-snooping limit rate** | No limit speed |
| **Step 4** | **exit** | Exit to the global configuration mode |
| **Step 5a** | **dhcp-snooping errdisable recovery** <enable|disable> | CConfigure whether the port get down when the DHCP packetreceiving speed larger then the limit speed .The default is disable |
| **Step 5b** | **dhcp-snooping errdisable recovery interval** (3-3600) | Configure the time when the port recovery after getting down |
| **Step 6** | **show dhcp-snooping configure interface** <all |*interface\_type slot/port* > | Show DHCP Snooping configuration |
| **Step 7** | **write** | Save configuration |

# L3 Route Configuration

## Configure Static Route

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

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

# IPv6

## Configure 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** (1-4094) | 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 vlan** (1-4094) | Verify the configuration information. |
| **Step 6** | **write** | Save configurations. |

## 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.

### Configure IPv6 SLAAC

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** (1-4094) | 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*  [ { (0-4294967295) |  off-link | infinite | no-autoconfig | router-address } \*1] | 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. | |

## 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

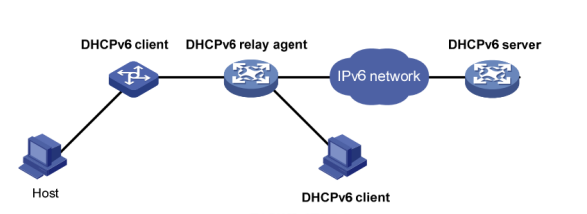


Figure 1：DHCPv6 network Composition

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.

#### Configure DHCPv6 DUID

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|duid-uuid> (1-4294967295)identifier *Identifier string* | 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.

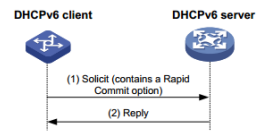


Figure 2：Quickly allocation process with two messages exchanging

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.

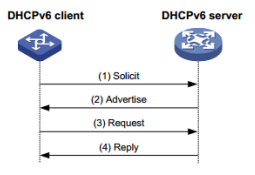


Figure 3：Allocation process with four messages exchanging

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

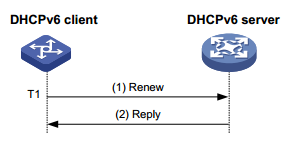


Figure 4：Update address/prefix lease by renew

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

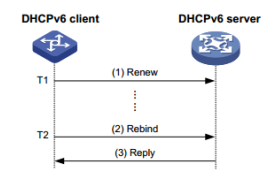


Figure 5：Update address/prefix lease by rebind

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.

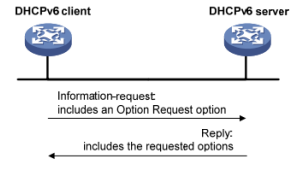


Figure 6：DHCPv6 stateless configuration process

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.

#### Configure DHCPv6 Server

Begin at privileged configuration mode, configure DHCPv6 server as the following table shows.

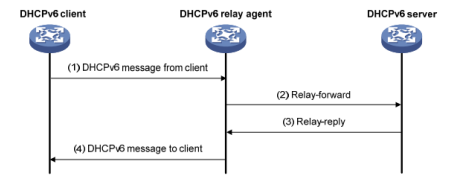
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Command** | **Function** | | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | | |
| **Step 2** | **ipv6 dhcp pool** *DHCP pool name* | Configure an IPv6 DHCP address pool. |  |
| **Step 3** | **prefix-delegation**  *X:X::X:X/M* *X:X::X:X/M* [lifetime  < (60-4294967295)|infinite>  < (60-4294967295)|infinite> ] | Configure prefix delegation and its lifetime. |  |
| **Setp 4** | **address** *X:X::X:X/M X:X::X:X/M* [ lifetime  < (60-4294967295)|infinite> < (60-4294967295)|infinite> ] | Configure IPv6 address prdfix and its lifetime. | | |
| **Step 5** | **dns-sever** *X:X::X:X* | Configure the DNS server IPv6 address. | | |
| **Step 6** | **domain-name** *A domain name* | Configure domain name. | | |
| **Step 7** | **interface vlan**(1-4094) | Add VLAN and enter VLAN interface configuration.  vlan\_id(1－4094)； | | |
| **Step 8** | **ipv6 dhcp server** *Name of IPv6 DHCP pool* [ preference (0-255)|allow-hint | rapid-commit ] | Configure and enable the DHCPv6 server address of the network segment on the interface. | | |
| **Step 9** | **exit** | Exit to global configuration mode. | | |
| **Step 10** | **show ipv6 dhcp pool** | View DHCPv6 address pool information.. | | |
| **Step 11** | **show ipv6 dhcp interface vlan** (1-4094) | Show information about the device DHCPv6 interface | | |
| **Step 12** | **write** | Add VLAN and enter VLAN interface configuration.  vlan\_id(1－4094)； | | |

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

#### Configure DHCPv6 Relay Option 37

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**(1-4094) | Add VLAN and enter VLAN interface configuration.vlan\_id(1-4094)； |
| **Step 3** | **ipv6 dhcp relay remote-id** *remote id* | Configure the remote-id value of the custom option37. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show ipv6 dhcp relay option** | Display configuration information about trunk related options. | |
| **Step 6** | **write** | Save configurations. | |

#### Configure DHCPv6 Relay Option 38

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**(1-4094) | Add VLAN and enter VLAN interface configuration.vlan\_id(1-4094)； |
| **Step 3** | **ipv6 dhcp relay subscriber-id** *subscriber id* | Configure the custom subscriber-id value of option38. |
| **Step 4** | **exit** | Exit to global configuration mode. | |
| **Step 5** | **show ipv6 dhcp relay option** | Display configuration information about trunk related options. | |
| **Step 6** | **write** | Save configurations. | |

## IPv6 Route

### Configure IPv6 Static Route

**IPv6 Static Routes Introduction**

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

**Default Routes Introduction**

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

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

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

## 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** | **ping ipv6** [ *X:X::X:X* |-c *count* |*ipv6 name*] | Packetize: The length of the packet to be sent, in bytes. Ping the link local address to specify the interface. |

# WAN Function

The OLT supports the 10 Gbit/s uplink port as the WAN port. Other ports are used only as the LAN port.This configuration enables the OLT to be used as a router/gateway.

## WAN Configuration

To configure the 10G upper interface as the WAN interface, perform the following steps.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface wan** | Enter wan interface configuration mode. |
| **Step 3a** | **wan ipversion** <both | ipv4 | ipv6> | Set the IP address type for the WAN connection. |
| **Step 3b** | **wan mode** <dhcp | pppoe | static> | Configure the WAN connection type. |
| **Step 4a** | **wan ip address** *A.B.C.D/M*  **wan ip gateway** *A.B.C.D*  **wan ipv6 address** *X:X::X:X/M*  **wan ipv6 gateway** *X:X::X:X* | Configure static WAN connections of IPv4 or IPv6 type. |
| **Step 5a** | **wan pppoe server** *PPPoE server ip or hostname* | Configure the IP address or name of the PPPoE server for the WAN connection. |
| **Step 5b** | **pppoe user name** *name* **password** *password* | Configure the PPPoE WAN account password. |
| **Step 6** | **wan mtu** (576-1500) | Configure MTU of the WAN connection. |
| **Step 7** | **wan vlan** <*vlan\_id* | default> | The VLAN ID configured for the WAN connection takes effect with the VLAN ID configured for the LAN. |
| **Step 8** | **wan startup** | Enable the WAN function and submit the WAN connection configuration. |
| **Step 9** | **wan stop** | Disable the WAN function. |
| **Step 10** | **show pppoe**  **show wan** <ip | mode | mtu | vlan> | Show WAN configuration. |
| **Step 11** | **multicast proxy** <enable | disable> | The multicast proxy for the WAN was enabled or disabled. |
| **Step 12** | **wan ipv6 dhcp prefix-delegation** <enable|disable> | Enable or disable obtaining IPv6 WAN prefixes. |
| **Step 13** | **exit** | Exit the global configuration mode |
| **Step 14** | **write** | Save configure |

## LAN Configuration

After setting the WAN function, you need to set the LAN interface address by using the following command.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface wan** | Enter wan interface configuration mode. |
| **Step 3** | **lan ip address** *A.B.C.D/M* | Configure the LAN IP address and mask. |

## NAT Configuration

After enabling the routing mode of OLT, NAT related parameters need to be set using the following command.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface wan** | Enter wan interface configuration mode. |
| **Step 3** | **nat type** < nat1 | nat2 | nat4> | The NAT type is specified. |
| **Step 4a** | **dmz enable ip address** *A.B.C.D* | Configure a host address for the DMZ.The DMZ must be enabled. |
| **Step 4b** | **dmz disable** | Disable DMZ. |
| **Step 5** | **show nat type** | Displays the configuration of the NAT type. |
| **Step 6** | **show dmz** | Show DMZ configuration. |
| **Step 7** | **exit** | Exit the global configuration mode |
| **Step 8** | **write** | Save configure |

# PON Management



## Show PON Port Info

### Show PON Port Info And Optical Power

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

### 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 rx-power onu** [(1-128)|all] | 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 | |

### Configure P2P Function On The PON Port

begin at the privilege configuration mode, enable or disable the PON port P2P function, as shown in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **show p2p** | Show PON port P2P configuration |
| **Step 3** | **show p2p info** | Show P2P configurations of interfaces in different PON modes | |
| **Step 4** | **p2p** <enable|disable> | Enable/disable P2P function | |

### Configure PON Port Range Function

begin at the privilege configuration mode, configure the PON port Range function, as shown in the following table.

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

# ONU Management



## ONU Basic Configuration

### Display Auto-find ONU

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

### Display ONU Automatic Authorization

OLT enables/disables automatic authorization mode. When the ONU is online, the ONU will automatically authorize the ONU.

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

### Display ONU Authorization Information

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

### Display ONU Authorization Details

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3** | **show onu** **info** | Displays onu details | |

### Activate/Deactivate The ONU

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3a** | **onu** [all|(1-128)][active|deactivate] | Activate/disable the ONU on the 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* [loid|sn+loid|sn] | Authorization ONU | |

### Configure ONU Description

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3** | **onu** *onuid* **desc** *string*(1-31) | ONU add description string | |
| **Step 4** | **show onu desc** | Display ONU description | |

### Configure ONU Whitelist

Whitelist To enable ONU authentication. Supports filtering based on the source SN and Vendor ID.

begin at the privilege configuration mode, configure the onu whitelist function of the device, as shown in the following table:

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| Step 1a | **onu** **allowlist sn-auth** *Vendor(4 chars)* | Whitelist based on Vendor ID. The value is a four-digit string |
| Step 1b | **no onu allowlist sn-auth** *Vendor(4 chars)* | Delete the whitelist based on the Vendor ID |
| Step 2a | **onu allowlist sn-auth**  *SN(12 chars)* [*END SN(12 chars)*] | Whitelist based on SN. The value is a 12-digit string. You can set only the start SN or the range SN (start SN and end SN). |
| Step 2b | **no onu allowlist sn-auth** *SN(12 chars)* [*END SN(12 chars)*] | Delete the SN whitelist |

### Display ONU Statistics

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

### Configure Plug and Play

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON port |
| **Step 3** | **onu plug-and-play** <enable|disable> *vlan*(1-4094) | Configure ONU plug and play and VLAN |

### Configure ONU Delete Automatically

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

## ONU Remote Configuration

### Display ONU SFP Information

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

### Upgrade ONU

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

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

**attention：**

1. Do not turn off the power when updating. When the update is complete, the OLT notifies the ONU that the update was successful and resets the ONU with the new firmware.

2. After the ONU update restarts, the OLT sends the commit command to confirm the new version.

3. Run the upgrade load image <filename> delete command to delete the firmware and upgrade Settings.

4. Run the show upgrade status command to display the upgrade progress of the ONU.

5. Run the show upgrade info command to display the ONU upgrade Settings.

6. Run the upgrade stop command to stop the ONU upgrade.

### ONU Automatic Upgrade

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

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

### Restart ONU

Restart the authorized ONU

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3a** | **onu** [all|(1-128)] **reboot** | Restart one of the ONUs or all ONUs on the PON | |

### T-cont Configuration

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3a** | **onu** (1-128) **tcont** (1-255) *{[name] string}\*1 {[dba] string}\*1* | Configure the created ONU TCONT, dba | |
| **Step 3b** | **no onu** (1-128) **tcont** (1-255) | 删除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 | Configure GEMPORT to bind TCONT. You can also select the port id | |
| **Step 4** | **no onu** (1-128) **gemport** (1-255) | Delete the ONU GEMPORT | |

### 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|eth] (1-255)}\*1 | Configure the ONU service using vlans | |
| **Step 3b** | **onu** (1-128) **service** *service\_name* **gemport** (1-255) [untag] {[eth] port\_id(1-32)}\*1 {[iphost] port\_id(1-255)}\*1 {[vlan]*vlan\_id* (1-4094)}\*1 | Configure the ONU service without vlan | |
| **Step 4** | **no onu**(1-128)**service** *service\_name* | Delete the ONU service | |

### ONU UNI Configuration

Including LAN, VEIP, IPHOST

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

### Display ONU Service

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3** | **show running-config onu** (1-128) | Display ONU service | |

### Display The ONU Capability

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3** | **show onu capability** *onu\_list* | Displays ONU capability values | |

## ONU Remote Port Configuration

### Enable/Disable ONU Port

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

### Configure ONU Port Auto-negotiation

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON Interface configuration mode |
| **Step 3** | **onu** (1-128) **eth** (1-32) **speed**  [auto|full-10|full-100|full-1000|half-10|half-100|half-1000] | ONU Port auto-negotiation | |

### Configure Port Flow Control Of ONU

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

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

### Configure Multicast VLAN

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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 a 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) **dhcp** | Set this parameter to dhcp mode | |
| **Step 3b** | **onu** (1-128) **iphost**  (1-255) **static-ip** *A.B.C.D A.B.C.D* [gateway] *A.B.C.D* | Set this parameter to static mode, subnet mask, and gateway | |
| **Step 3c** | **onu** (1-128) **iphost**  (1-255)**primary-dns** *A.B.C.D* {[second-dns] *A.B.C.D}\*1* | Configure DNS | |
| **Step 3d** | **no onu** (1-128) **iphost** (1-255) | Delete an iphost configuration | |

### Configure Port Multicast Label Of 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** (1-128) **mvlan** [tag-strip] **eth** (1-32) | Configure the multicast label | |
| **Step 3b** | **no onu** (1-128) **mvlan** [tag-strip] **eth** (1-32) | Delete configuration | |

### SFU Example

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

1. Create an onu configuration file with one eth port

profile onu name 1GE\_SFU

port eth 1

commit

exit

1. Create a dba configuration file. Ensure that a maximum of 10 MB is 20 MB

profile dba name 20M

type 3 assured 10240 maximum 20480

commit

exit

Register the onu and configure the service

interface gpon 0/1

show onu auto-find

onu add 1 profile 1GE\_SFU sn GPON00000031

onu 1 tcont 1 dba 20M

onu 1 gemport 1 tcont 1

onu 1 service 1 gemport 1 vlan 100

onu 1 portvlan eth 1 mode tag vlan 100

1. Create vlan 100

vlan 100

exit

1. Bind the vlan to the uplink port

interface gigabitethernet 0/1

switchport hybrid pvid vlan 100

### HGU Example

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

1. Create an onu profile with one veip port

profile onu name HGU

port veip 1

commit

exit

1. Create a dba configuration fileprofile dba name 20M

type 3 assured 10240 maximum 20480

commit

exit

profile dba name 2M

type 1 fixed 2048

commit

exit

3. Register the onu and configure the service

interface gpon 0/1

show onu auto-find

onu add 1 profile HGU sn GPON000000AB

onu 1 tcont 1 dba 20M

onu 1 tcont 2 dba 2M

onu 1 gemport 1 tcont 1

onu 1 service HSI gemport 1 vlan 41

onu 1 gemport 2 tcont 2

onu 1 service TR69 gemport 2 vlan 46

onu 1 portvlan veip 1 mode transparent

1. Create vlan41 and VLAN46 and bind them to uplink ports

vlan 41

exit

vlan 46

exit

interface gigabitethernet 0/10

switchport mode trunk

switchport trunk vlan 41

switchport trunk vlan 46

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

## Private Configuration

### Configure ONU ACL Rules

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri acl** [fttp|http|https|ping|ssh|telnet|tftp]  [disable|enable] | Configure the corresponding acl rules | |
| **Step 4** | **show onu** (1-128) **pri** | Show results | |

### Configure ONU CATV Status

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri catv <**disable|enable> | Configure the catv status | |
| **Step 4** | **show onu** (1-128) **pri catv\_status** | Show results | |

### Configure ONU Dhcp Server

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu**(1-128) **pri dhcp\_server** *A.B.C.D A.B.C.D <*enable|disable|relay> | Configure the dhcp server status |
| **Step 4** | **onu** *1* **pri dhcp\_server** *192.168.1.1 255.255.255.0* **enable** *10000 192.168.1.2 192.168.1.254* **stb** *8.8.8.8 114.114.114.114 192.168.1.1* | Example of configuring the dhcp server state: Create a dhcp server whose gateway is 192.168.1.1, address pool is 192.168.1.2 to 192.168.1.254, lease is 10000S, and DNS is 8.8.8.8 114.114.114.114 |
| **Step 5** | **show onu**  (1-128) **pri dhcp\_server** | Display result |

### Configure ONU DHCPv6 Server

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **Interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **Onu** (*1-128*) **pri dhcp\_server ipv6** *X:X::X:X* <enable|disable|relay> | Configure the dhcpv6 server status | |
| **Step 4** | **onu** *1* **pri dhcp\_server ipv6** *2550::11* **prefix\_mode auto server enable preference** *10000* **valid** *5000 2000::1 2000::10* stb dns *204f::1 204f::2* gw *2550::11* | Example: Create a gateway with 2550::1,PD mode is automatic, preference time is 10000s, live time is 5000s, address pool range is 2000::1 to 2000::10,dns  The dhcpv6 server is 204f::1 204f::2 | |
| **Step 5** | **show onu** (1-128) **pri dhcp\_server\_ipv6** | Display result | |

### Configure ONU Equid Server

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri equid**  *word* | Example Change the id of an ONU device | |
| **Step 4** | **show running-config onu** (1-128) | Display result | |

### Restore ONU To Factory Defaults

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri factory\_reset** | Restore the ONU to factory defaults | |

### Configure ONU Firewall

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128)**pri firewall level** {disable|low|middle|high}\*1 | Configure the ONU firewall | |

### Configure ONU IGMP Mode

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri igmp** [enable|disable] | Configure ONU igmp | |
| **Step 4** | **show onu** (1-128) **pri igmp\_status** | Display result | |

### Configure ONU LAN Binding Mode

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri lan\_bind\_mode port (**1-255) **mode vlan lanVlan0** (1-4094) **wanVlan0** (1-4094) | Set the ONU LAN binding mode to vlan | |
| **Step 4** | **onu** (1-128) **pri lan\_bind\_mode port** (1-255) **mode port** | Set the ONU LAN binding mode to vlan | |
| **Step 5** | **show onu** (1-128) **pri lan\_bind\_mode** | Display result | |

### Configure ONU Loopback

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri loopback\_detect**  **<**disable|enable> | Configure ONU loopback | |
| **Step 4** | **show onu** (1-128) **pri loopback** | Display result | |

### Configure ONU MAC Connection

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri mac\_aging\_time** (0-65535) | Set the ONU MAC aging time | |
| **Step 4** | **onu** (1-128) **pri mac\_clean** | Clear the ONU mac table | |
| **Step 5** | **onu** (1-128) **pri mac\_limit pon** (0-65535) | Example Set the aging time of an ONU mac address | |
|  | **show onu** (1-128) **pri mac\_addr\_table** | The ONU MAC table is displayed | |

### Configure ONU Port Isolation

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri port <**disable|enable> | Configure ONU port isolation | |

### Configure ONU Voice Port

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri pots** [all|(1-255)] **sip\_user\_config active enable acconut** *word max length 16* **name** *word max length 16* **pwd** *word max length 16* | Configure ONU voice port information | |
| **Step 4** | **show onu** (1-128) **pri pots** [all|(1-255)] | Display result | |

### Configure ONU Voice SIP Service

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri sip\_global\_param mg\_port** (0-65535) **proxy\_serv** word(0-65535) **backup\_proxy\_serv** *word* (0-65535) **reg\_serv** *word* (0-65535) | Configure ONU sip server information | |
| **Step 4** | **show onu** (1-128) **pri sip** | Display result | |

### Save ONU Configuration

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri save\_config** | Save The ONU configuration | |

### Configure ONU RSTP

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri spanning\_tree <**disable|enable> | Configure ONU RSTP | |

### Configure ONU Uplink Upstream Speed Limit

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri speed\_limit us** (1-1244000,kbps) | Configure ONU uplink limiting | |

### Configure ONU TR069 Management Information

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **Interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri tr069\_mng enable ace\_server url** *word* **username** *word* **password** *word* **certificate <**disable|enable> **inform <**disable|enable> **inform\_interval** (0-4294967295) | Configure ONU TR069 management information | |
| **Step 4** | **onu** (1-128) **pri tr069\_stun <**disable|enable> **server** *word* **port** (1-65535) **username** *word* **password** *word* | Configure the ONU TR069 Stun server | |
| **Step 5** | **show onu** (1-128) **pri tr069** | Display result | |

### Configure ONU UPnP

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri upnp status <**disable|enable> **wan\_index** (1-8) | Configure ONU UPNP | |

### Configure ONU WAN Information

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri wan\_adv index** (1-8) **route** [ipv4|ipv6|both][dhcp|pppoe|static][dns] primary *A.B.C.D* [nat]<disable|enable> | Example of configuring ONU route wan | |
| **Step 4** | **onu** (1-128) **pri wan\_adv index** (1-8) **bridge** [internet|other] [ipv4|ipv6|both|mtu] | Example of configuring ONU bridge wan | |
| **Step 5** | **onu** (1-128) **pri wan\_adv index** (1-8) **bind** [lan|ssid] | Configure WAN bond ports | |
| **Step 6** | **onu** (1-128) **pri wan\_adv index** (1-8) **delete** | Deleting a WAN | |
| **Step 7** | **onu** (1-128) **pri wan\_adv commit** | Commit WAN | |
| **Step 8** | **show onu** (1-128) **pri wan\_adv** | Display result | |

### Configure ONU WIFI SSID

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **interface gpon** *slot/port* | Enter the corresponding PON port |
| **Step 3** | **onu** (1-128) **pri wifi\_ssid** (1-8) **disable** | Turn off wifi | |
| **Step 4** | **onu** (1-128) **pri wifi\_ssid** (1-8) **name***word* **hide** <disable|enable> | Set whether the WIFI SSID is hidden | |
| **Step 5** | **onu** (1-128) **pri wifi\_ssid** (1-8) **name** *word*  **hide disable** | Configure WAN bond ports | |
| **Step 6** | **onu** (1-128) **pri wifi\_switch** (1-2) **enable**[fcc|etsi|ic|spain|france|mkk|isreal|mk k2|mkk3|russian|cn|global|world-wide|mkk1|ncc][auto|chl\_34|chl\_36|chl\_38|chl\_40|chl\_42|ch l\_44|chl\_46|chl\_48|chl\_52|chl\_56|chl\_60|chl\_64|chl\_100|chl\_104|chl\_108|chl\_112|chl\_116|ch l\_120|chl\_124|chl\_128|chl\_132|chl\_136|chl\_140|chl\_144|chl\_149|chl\_153|chl\_157|chl\_161|chl \_165]{80211ac0|80211acA|80211acN|80211acAN|80211acNAC|80211acANAC|80211acax|80211acanacax}\*(0-20) [cw20|cw40|cw80|cw20/40|cw20/40/80|cw160] [easy\_mesh] <enable|disable> | Configure WIFI channels, protocols, etc | |
| **Step 7** | **show onu** (1-128) **pri wifi\_ssid** (1-8) | The wifi ssid information is displayed | |
| **Step 8** | **show onu** (1-128) **pri wifi\_switch** | The wifi channel information is displayed | |

## Rogue ONU Configuration

An ONU that does not follow the specified timestamp to send an optical signal is called a rogue ONU.

There are two main types of rogue ONUs:

1) Long time Glowing rogue ONU: ONU is glowing (glowing at any time).

2) Luminous rogue ONU: The ONU is not assigned a timestamp in the OLT, which may be premature luminous, or delayed shutdown, and so on.

### Configure Rogue ONU Detection

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

### Display Rogue ONU Status

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **show rogue-onu-detect config** | Display configuration |

# ONU Profile Management



## Summary

The template is under the "config" node, and the operation steps are as follows:

1. Create the profile

**profile** {onu|dba|format|igmp|line|srv|pri} {id <1-32767>}\*1 {name <string>}\*1

2.Enter the corresponding profile node via profile\_id

**profile** {onu|dba|format|igmp|line|srv|pri} {id <1-32767>}\*1 {name <string>}\*1

3.Modifying profile parameters

**modify** …

4.Exit profile node

**exit**

5.Bind the profile to the onu device

**Interface gpon** *slot/port*

**onu add** *1* **profile** *<string>*

**onu** <onuid> **profile** {line|srv} *<string>*

6.Query the onu device binding profile

**Interface gpon** *slot/port*

**show profile {**onu|dba|format|igmp|line|srv|pri} *{id <1-32767>}\*1 {name <string>}\*1*

7.Query profile configuration information

**Show profile** {onu|dba|format|igmp|line|srv|pri} *{id <1-32767>}\*1 {name <string>}\*1 used-info*

## ONU Profile Configuration

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode | |
| **Step 2** | **profile onu** [id] (1-32767) [name] *string* | Create or enter the onu profile you created earlier. |
| **Step 3a** | **tcont-num** (1-255) **gemport-num** (1-255) | Configure the maximum tcont and gemport supported by the onu. | |
| **Step 3b** | **port-num** [eth](0-64) [pots](0-64) [iphost] (0-255) [ipv6host] (0-255) [veip] (0-127) | Configure onu  eth/pots/iphost/ipv6host/veip | |
| **Step 4** | **commit** | Commit the configuration file. The Settings can only be committed by typing "commit" | |
| **Step 5** | **exit** |  | |

## DBA Profile Configuration

The default system will have a DBA profile with id 0, this template parameter cannot be modified, and all ONUs will be in the template when the default binding is created. Each ONU must bind a dba template.

There are 5 DBA profiles:

Type1: Fixed

Type2:Assured

Type3:Assured,Maximum

Type4:Maximum

Type5: Fixed,Assured,Maximum

Fixed<=Assured<=Maximum

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Fixed | Assured | Maximum |
| Type\_1 | √ |  |  |
| Type\_2 |  | √ |  |
| Type\_3 |  | √ | √ |
| Type\_4 |  |  | √ |
| Type\_5 | √ | √ | √ |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode | |
| **Step 2** | **profile dba** [id] (1-32767) [name] *word* | Create/modify dba configuration files |
| **Step 3a** | **type** [1]**fixed** (128-9953280) | Configure type 1 to be fixed | |
| **Step 3b** | **type** [2] **assured** (128-9953280) | Configure type 2 to be guaranteed | |
| **Step 3c** | **type** [3] **assured** (128-9953280) **maximum** (128-9953280) | Configure type 3 with guaranteed and maximum values | |
| **Step 3d** | **type** [4] **maximum** (128-9953280) | Configures type 4 with the maximum value | |
| **Step 3e** | **type** [5] **fixed** (128-9953280) **assured** (128-9953280) **maximum** (128-9953280) | Configure type 5 with fixed, guaranteed, maximum values | |

## Line Profile Configuration

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode | |
| **Step 2** | **profile line** [id](1-32767) [name] *word* | Create a modified line profile |
| **Step 3** | **tcont** (1-255)[id](1-32767)[name] *word* | Bind the tcont configuration file | |
| **Step 4** | **gemport** (1-255) **tcont**(1-255) *gemport\_name* | Binding the gemport configuration file | |
| **Step 5a** | **service** *service\_name* **gemport** (1-255) **vlan** *VLAN\_LIST* **[ethuni]** (1-32)**[iphost]**(1-255) | Bind gemport with vlan to the service | |
| **Step 5b** | **service** *service\_name* **gemport** (1-255) [untag][ethuni] (1-32)[iphost] (1-255) [vlan](1-4094) | Bind gemport without vlan to the service | |
| **Step 5c** | **mvlan** *vlanlist* | Create a multicast vlan | |
| **Step 6** | **commit** | Submitting configuration | |
| **Step 7** | **no mvlan** [all|*vl*anlist] | Delete the multicast vlan | |
| **Step 8** | **no tcont** (1-255) | Delete tcont | |
| **Step 9** | **no gemport** (1-255) | Delete gemport | |
| **Step 10** | **no service** *service\_name* | Delete service | |
| **Step 11** | **exit** |  | |

## Service Profile Configuration

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode | |
| **Step 2** | **profile srv** *id* (1-32767) *name string* | Create/modify srv profile |
| **Step 3a** | **portvlan** {eth|wifi|veip}\*1(1-32)**mode**transparent | Configure portvlan mode to transparent | |
| **Step 3b** | **portvlan** {eth|wifi|veip}\*1(1-32) **mode**trunk | Configure the portvlan mode to trunk | |
| **Step 3c** | **portvlan** {eth|wifi|veip}\*1(1-32) **mode****tag** *vlan* (1-4094) **pri** (0-7*)* | Configure portvlan mode to tag, and configure pri | |
| **Step 3d** | **portvlan** {eth|wifi|veip}\*1(1-32)**mode****hybrid****def\_vlan**(1-4094)**def\_pri** (0-7) | Configure portvlan mode to hybird | |
| **Step 4a** | **mvla*n******tag-strip******eth***(1-32) | Configure the LAN port to untag mode | |
| **Step 4b** | **no mvlan** **tag-strip eth** (1-32) | Remove LAN port untag mode | |
| **Step 5a** | **iphost**(1-255) [desc] string | Configure the iphost description | |
| **Step 5b** | **iphost** (1-255) [dhcp] | Configure iphost to dhcp mode | |
| **Step 5c** | **iphost**(1-255) **static-ip** *A.B.C.D* *A.B.C.D* **gateway** *A.B.C.D* | Configure iphost to static mode | |
| **Step 5d** | **iphost** (1-255) **primary-dns** *A.B.C.D* **second-dns** *A.B.C.D* | Configuring DNS | |
| **Step 5e** | **no iphost** (1-255) | Delete the iphost configuration | |
| **Step 6** | **commit** | Submitting configuration | |
| **Step 7** | **exit** |  | |

## Alarm Threshold Profile Configuration

Alarm thresholds can only be configured via profile. begin at the privilege configuration mode, configure the alarm threshold profile as shown in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode | |
| **Step 2** | **profile alarm** [id](1-32767)[name] *string* | Create or enter a configuration file |
| **Step 3a** | **sf-sd-threshold sf** (3-8) **sd** (4-10) | Configure the range of sf and sd | |
| **Step 3b** | **rx-optical low** (-27~-8) **high** (-27~-8) | Configure rx optical range | |
| **Step 3c** | **tx-optical low** (1-5) **upper** (1-10) | Configure the range of tx optical | |
| **Step 4** | **commit** | Submitting configuration | |
| **Step 5** | **exit** |  | |

## Private Profile Configuration

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode | |
| **Step 2** | **profile pri** [id] (1-128) [name] *string* | Create/modify the pri profile |
| **Step 3** | **wan\_adv add** <bridge|route> | Add a route/bridge WAN | |
| **Step 4** | **wan\_adv index** (1-8) **bind** {lan1|lan2|lan3|lan4|lan5|lan6|lan7|lan8|ssid1|ssid2|ssid3|ssid4|ssid5|ssid6|ssid7|ssid8|ssid9|ssid10}\*1 | Binding port | |
| **Step 5** | **wan\_adv index** (1-8) **bridge** <internet|other> [mtu] (576-1500)[ipv4|ipv6|both] | Configuring Bridge WAN | |
| **Step 6a** | **wan\_adv index** (1-8) **route both pppoe proxy** <enable|disable> **user** *NAME* **pwd** *word*server *servername* **mode** <auto|payload> **nat** <enable|disable>**slaac**<enable|disable> | Configure pppoe mode routing WAN | |
| **Step 6b** | **wan\_adv index** (1-8) **route both static ipv4** *A.B.C.D* **mask** *A.B.C.D* **gw** *A.B.C.D* **dns** primary *A.B.C.D* secondary *A.B.C.D* **nat**<enable|disable> **ipv6** *X:X::X:X/M* **gw** *X:X::X:X* **dns** primary *X:X::X:X* secondary *X:X::X:X* | Configuring a routing WAN in static mode | |
| **Step 6c** | **wan\_adv index** (1-8) **route** <both|ipv6> **client\_address** <enable|disable> **client\_prifix** <enable|disable> | Configure the client\_address, client\_prifix, and aftr\_mode of the routing WAN | |
| **Step 6d** | **wan\_adv index** (1-8) **route both dhcp** [dns-v4] primary A.B.C.D secondary A.B.C.D[nat]<enable|disable>[dns-v6]primary *X:X::X:X* secondary *X:X::X:X* [slaac] *<*enable|disable*>* | Configure dhcp mode routing WAN | |
| **Step 7** | **wan\_adv index** (1-8) **route mode** [internet|multicast|tr069|tr069\_internet|tr069\_voip|voip\_internet|tr069\_voip\_internet|voip|other]  [mtu ](576-1500) | Configure the mode of routing WAN | |
| **Step 8a** | **wan\_adv index** (1-8) **vlan disable** [qos]*<enable|disable>* | VLAN to disenable WAN | |
| **Step 8b** | **wan\_adv index** (1-8) **vlan tag** [wan\_vlan] (1-4095) cos (0-7) [qinq] tpid (1-65534) vlan (1-4095) cos (0-7) [qos] <enable|disable> | Configure the VLAN mode to tag | |
| **Step 8c** | **wan\_adv index** (1-8) **vlan transparent** [wan\_vlan] (1-4095) (0-7)] [tranlation] (1-4095) (0-7) [qinq] tpid (1-65534) vlan (1-4095) cos (0-7) [qos] <enable|disable> | Configure VLAN mode to transparent | |
| **Step 9** | **wan\_adv index** (1-8) **bin*d* <**lan|ssid> | Bind lan port and ssid | |
| **Step 10** | **wan\_adv commit** | Submitting WAN | |
| **Step 11** | **wan\_adv index** (1-8) **delete** | Removing index | |
| **Step 12** | **dhcp\_server** *A.B.C.D**A.B.C.D* **disable** | disenable the dhcp server | |
| **Step 13a** | **dhcp\_server** *A.B.C.D**A.B.C.D* **enable** (0-4294967295)*A.B.C.D A.B.C.D* [pc|camera|stb|ip\_phone] *A.B.C.D**A.B.C.D**A.B.C.D* | Configure the dhcp server | |
| **Step 13b** | **dhcp\_server ipv6** *X:X::X:X* **prefix\_mode**{auto|static *X:X::X:X/M*|wan\_delegated (1-8)}\*1 **server enable preference** (0-4294967295) **valid** (0-4294967295)*HHHH:HHHH:HHHH:HHHH HHHH:HHHH:HHHH:HHHH* {pc|camera|stb|ip\_phone}\*1**dns** *X:X::X:X X:X::X:X* **gw** *X:X::X:X* [ra manage] <enable|disable> [other] <enable|disable> max\_interval (1-1800) min\_interval (1-1800) | Configure the dhcpv6 server | |
| **Step 13c** | **dhcp\_server ipv6** *X:X::X:X* **prefix\_mode**{auto|static *X:X::X:X/M*|wan\_delegated (1-8)}\*1 **server disable** [ra manage] <enable|disable>[other] <enable|disable> max\_interval (1-1800) min\_interval(1-1800) | To enable dhcpv6 server | |
| **Step 13d** | **dhcp\_server ipv6** *X:X::X:X*[prefix\_mode] static *X:X::X:X/M* | Configuring dhcpv6 in static mode server | |
| **Step 13e** | **dhcp\_server ipv6** *X:X::X:X*[prefix\_mode] *wan\_delegated* (1-8) | Configure the dhcpv6 server in wan\_delegated mode | |
| **Step 14a** | **wifi\_ssid** (1-8) **name** *WORD* **hide** <enable|disable> **auth\_mode** {open|shared|wepauto}\*1 **encrypt\_type** *wep* **encryptionlevel** <64|128> **keyindex** (1-4) **key1** *WORD* **key2** *WORD* **key3** *WORD* **key4** *WORD* | Configure the dhcpv6 server in wan\_delegated mode | |
| **Step 14b** | **wifi\_ssid** (1-8) **name** *WORD* **hide** <enable|disable> **auth\_mode** {wpapsk|wpa2psk|wpapsk\_wpa2psk|wpa3psk|wpa2psk\_wpa3psk}\*1  **encrypt\_type** {tkip|aes|tkipaes}\*1 **shared\_key** *WORD*[rekey\_interval] (0-4194303) | Configure the dhcpv6 server in wan\_delegated mode | |
| **Step 15** | **wifi\_ssid** (1-8) **disable name** *WORD* | To enable ssid | |
| **Step 16a** | **wifi\_switch** (1-2)**enable** {fcc|etsi|ic|spain|france|mkk|isreal|mkk2|mkk3|russian|cn|global|world-wide|mkk1|ncc}\* (0-14) {80211b|80211g|80211bg|80211n|80211bgn|80211ax|80211bgnax|80211gn}\* (0-20) <20|40|20/40> | Configure 2.4G wifi\_switch | |
| **Step 16b** | **wifi\_switch** (1-2)**enable** [fcc|etsi|ic|spain|france|mkk|isreal|mkk2|mkk3|russian|cn|global|world-wide|mkk1|ncc] [auto|chl\_34|chl\_36|chl\_38|chl\_40|chl\_42|chl\_44|chl\_46|chl\_48|chl\_52|chl\_56|chl\_60|chl\_64|chl\_100|chl\_104|chl\_108|chl\_112|chl\_116|chl\_120|chl\_124|chl\_128|chl\_132|chl\_136|chl\_140|chl\_144|chl\_149|chl\_153|chl\_157|chl\_161|chl\_165]  {80211ac0|80211acA|80211acN|80211acAN|80211acNAC|80211acANAC|80211acax|80211acanacax}\*(0-20) <20|40|80|20/40|20/40/80|160>[easy\_mesh] <*enable|disable>* | Config 5G wifi\_switch | |
| **Step 17** | **wifi\_switch** (1-2) **disable** | Disable the wifi | |
| **Step 18** | **no wifi\_ssid** (1-8) | Delete Wi-Fi ssid configuration | |
| **Step 19** | **no wifi\_switch** (1-2) | Delete Wi-Fi switch Configuration | |
| **Step 20a** | **sip\_global\_param mg\_port** (0-65535) **proxy\_serv** *WORD*(0-65535)[backup\_proxy\_serv WORD](0-65535)**reg\_serv** *WORD* (0-65535)[backup\_reg\_serv WORD](0-65535)**out\_bound\_serv WORD** (0-65535) **reg\_interval** (1-10000000) **heartbeat** <active|passive>(1-65535) (1-65535) | Configure SIP to enable heartbeat packets. | |
| **Step 20b** | **sip\_global\_param mg\_port** (0-65535) **proxy\_serv** *WORD* (0-65535)[backup\_proxy\_serv WORD ](0-65535) **reg\_serv** *WORD*(0-65535)[backup\_reg\_serv WORD](0-65535) **out\_bound\_serv** *WORD* (0-65535*)* **reg\_interval** (0-10000000) **heartbeat** disable | Configure SIP to close heartbeat packets | |
| **Step 21** | **no sip\_global\_param** | Delete SIP configuration | |
| **Step 22** | **pots** (1-255) **parameter vad** <enable|disable> **echo\_cancel** <enable|disable> **input\_gain** *WORD*(-32-32) **output\_gain** *WORD*(-32-32) **dtmf\_mode** <transparent|rfc2833|rfc2833\_redundancy|outband> | Configure pots advanced parameters | |
| **Step 23a** | **pots** (1-255) **sip\_user\_config active** *disable* | Disable pots | |
| **Step 23b** | **pots** (1-255) **sip\_user\_config active** enable **account** *WORD* **name** *WORD* **pwd** *WORD* | Configure the pots user parameters | |
| **Step 24** | **no pots** (1-255) **parameter** | Delete the pots’ configuration | |
| **Step 25a** | <port\_isolate|spanning\_tree|catv|igmp> <enable|disable> | Configure port isolation、stp、catv、igmp | |
| **Step 25b** | **speed\_limit us** (1-9953000) **ds** (1-9953000) | Configure rate limit | |
| **Step 25c** | **mac\_aging\_time** (0-65535) | Configure the mac aging time | |
| **Step 25d** | **mac\_limit pon** (0-65535) **lan** (0-65535) | Configure the mac aging time | |
| **Step 26a** | **nat\_type** <nat1|nat2|nat3|nat4-napt> | Configure the nat type | |
| **Step 26b** | **upnp status disable** | Disable the upnp | |
| **Step 26c** | **upnp status enable wan\_index** (1-8) | Configure upnp | |
| **Step 26d** | **no** <nat\_type|upnp> | Delete NAT/UPNP configuration | |
| **Step 27a** | **onu\_mode status** disable | Disable the onu mode state | |
| **Step 27b** | **onu\_mode status** enable **mode** <sfu|hgu|auto> | Configure the onu mode status | |
| **Step 28** | **username admin\_control enable** *WORD WORD* **user\_control enable** *WORD WORD* | Configure the account number and password of the admin users and user users | |
| **Step 29** | **firewall level** <disable|low|middle|high> | Configure firewall | |
| **Step 30** | **acl** <telnet|ftp|http|https|tftp|ping|ssh> **control enable lan** <enable|disable> **wan enable ipv4\_control enable** *A.B.C.D A.B.C.D* **ipv6\_control enable** *X:X::X:X/M* [port](0-65535) | Configure ACL | |
| **Step 31** | **loopback\_detect** <enable|disable>[loopcheck\_interval](1-60000) [recover\_interval](1-1800)[ethernet\_type]*WORD* [vlan](1-4094)[dest\_mac\_type]<broadcast\_address|bpdu\_address>[port\_closing\_time](1-1800)[alarm]<enable|disable> [portdislooped ]<enable|disable> | Configure loop detection | |
| **Step 32a** | **tr069\_mng** disable | Disable tr069 manage | |
| **Step 3b** | **tr069\_mng** enable **acs\_server url** *WORD* **username** *WORD* **password** *WORD* **certificate** <enable|disable> **inform** <disable|enable> *i*nform\_interval (0-4294967295) **reverse\_connection username** *WORD* **password** *WORD* | Disable tr069 manage | |
| **Step 32c** | **tr069\_stun** disable | Disable tr069 stun | |
| **Step 32d** | **tr069\_stun** enable **server** *WORD* **port** (1-65535)[username] *WORD* [password] *WORD* | Configure tr069 stun | |
| **Step 33** | **show profile pri** id(1-32767)name *string* | Show the private profile configuration | |
| **Step 34** | **exit** | Exit | |

## IGMP Profile Configuration

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **profile igmp** [id] (1-128)[name] *string* | Configure the igmp profile |
| **Step 3** | **igmp-mode** <snooping|spr|proxy> | Configure the igmp mode |
| **Step 4** | **igmp-rate-limit** (0-4294967294) | Configure the igmp rate limit | |
| **Step 5** | **igmp-version** <igmp-v1|igmp-v2|igmp-v3|mld-v1|mld-v2> | Configure the igmp version | |
| **Step 6** | **show profile igmp** [id] (1-32767)[name] *WORD* running-config | Show the igmp configuration | |

## Format Profile Configuration

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **profile format** [id] (1-128) [name] *string* | Configure the format profile |
| **Step 3** | **switch** [option82] <enable|disable> [option18] <enable|disable> [option37] <enable|disable> [pppoe-plus] <enable|disable> | Add exchange configuration |
| **Step 4** | **format type** <custom|ctc|unicom> | Configure the format type | |
| **Step 5** | <circuit-id|remote-id> **index** (1-22)<cvlan|devtype|acnoid|slotno|ponno|onuno|onutype|onusn> | Configure the circuit-id and remote-id parameters | |
| **Step 6** | **show profile format** [id] (1-32767)*[*name] *WORD* running-config | Show the format configuration | |

## ONU Binding Profile Configuration

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

## Show/Delete The Profile

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter the global configuration mode | |
| **Step 2** | **no profile** [onu|dba|format|igmp|line|srv|pri] **id**(1-32767) | Remove the profile |
| **Step 3a** | **show profile**[onu|dba|format|igmp|line|srv|pri] **id** (1-32767) | Show the profile | |

# ONU Auto-learn Configuration

## Enable Automatic Learn

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Command** | **Function** | |
| **Step 1** | **configure terminal** | Enter global configuration mode. | |
| **Step 2** | **interface gpon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **onu auto-learn** [alarm-profile|format-profile|line-profile|pri-profile|srv-profile][name] *string* [id] (1-32767) | 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 | |

# System Management



## Configure Management

### Save Configuration

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

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

### Erase Configuration

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

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

### Show The Boot Configuration

Use the following command to display the saved configuration.。

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

### Show The Running Configuration

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

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

### Upload/Download The Configuration File

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

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

## Display System Information

### Display System Operation Information

Use the following command to view the system information.

|  |  |
| --- | --- |
| **Command** | **Function** |
| **show sys arp** | Show the ARP table |
| **show top** | Show the CPU utilization rate |
| **show task** | Show the thread name |

### Display Version Information

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

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

## System Basic Configuration

### Configure The System Name

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

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

### Configure The Terminal Timeout Value

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **line vty** | Enter the line node |
| **Step 3a** | **exec-timeout** (0-35791) | Set the command-line timeout time |
| **Step 3b** | **no exec-timeout** | Set the command line timeout to the default value |
| **Step 4** | **show exec-timeout** | Show plays command line timeout |

## System Basic Operations

### Upgrade The System

Upgrade the device by using the following command.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **debug mode** | Enter the debug mode |
| **Step 3** | **download tftp image** *filename A.B.C.D* | Filename Is the upgrade file with a header h,A.B.C. D is the TFTP server IP |

### Restart The System

Restart the system by using the following command

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

### Telnet

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **telnet 192.168.8.100** | Telnet To the application layer of the system. Login name is admin and password is Xpon@Olt9417#. |

### Configure The RTC System Time

Use the following command to configure the RTC system time

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

### NTP Client

When you enable NTP, the device automatically updates the time

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ntp server** *HOSTNAME* | Configure the NTP server and enable it |
| **Step 3** | **ntp disable** | Disable the NTP server |
| **Step 4** | **show time** | Show the system time |

### Configure Time Zone

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

### Fan Control

Use the following command to control the fan running attributes.

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

# User Management



## User Privilege

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

## Default User

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

## Add User Account

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **user manager** | Enter the manager mode |
| **Step 3** | **user add** *user-name* **login-password** *login-password* | Add a new user account |
| **Step 4** | **user role** *user-name*[admin|normal|config]**enable-password** *enable-password* | Specify the user role, the new user is the normal privileged user |

## Display List of User Accounts

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **user manager** | Enter the manager mode |
| **Step 3** | **user list** | Show a list of user accounts |

## Delete User Account

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **user manager** | Enter the manager mode |
| **Step 3** | **user delete** *username* | Delete user account |

## Change Password

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **user manager** | Enter the manager mode |
| **Step 3** | **user login-password** *user-name**login\_password* | Configure the user's login password |
| **Step 4** | **user enable-password** *user-name* *enable\_password* | Configure the user's configuration mode password |

# Login Management

## Overview

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

## Login Access List Configuration

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

## Service Port Configuration

begin at the privileged configuration mode, configure the group name as shown in the table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter the global configuration mode |
| **Step 2** | **telnet** | Enter the telnet mode |
| **Step 3** | **telnet port** <(1-65535)|default> | Configure the service port for the telnet |
| **Step 4** | **exit** | Returns to the global configuration mode |
| **Step 5** | **sshd** | Enter the ssh mode |
| **Step 6** | **ip ssh port** <(1-65535)|default> | Configure the service port for the ssh |
| **Step 7** | **exit** | Returns to the global configuration mode |
| **Step 8** | **snmp-server agent port** (1-65535) | Configure the service port for the snmp |
| **Step 9** | **exit** | Returns to the global configuration mode |
| **Step 10** | **web port** <(1-65535)|default> | Configure the service port for the web |
| **Step 11** | **exit** | Returns to the global configuration mode |
| **Step 12** | **write** | Save configuration |

## Login Configuration

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter the global configuration mode |
| **Step 2** | **web login timeout**(1-30) | Configure the login time-out time for the web |
| **Step 3** | **show web login timeout** | Show the login timeout time of the web |
| **Step 4** | **web verification-code** <enable|disable> | Configure the login verification code for the web |
| **Step 5** | **show web verification-code** | Show the login verification code enabling status of the web |

## Language Configuration

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter the global configuration mode |
| **Step 2** | **web language** [english|chinese|portuguese] | Configure the web language |
| **Step 3** | **show web language** | Show the web-language configuration |
| **Step 4** | **exit** | Returns to the global configuration mode |

# SNMP Configuration

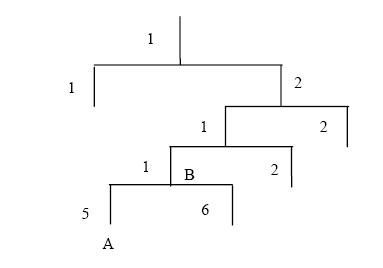
## Overview

SNMP(Simple Network Management Protocol)is a currently widely used network management protocol. It is an industry standard for transmitting management information between two devices. Network administrators can search for information, modify information, troubleshoot, diagnose faults, plan capacity, and generate responses. SNMP uses a polling mechanism that provides basic functions, especially suitable for small, fast, and low-cost situations. It is based on the transport layer protocol UDP.

SNMP has two parts, NMS (Network Management Station) and agent. The NMS is a workstation running a client program, while the agent is a server program running in the device. The NMS can send the GetRequest, GetNextRequest, and SetRequest messages to the agent. The agent will then execute the read or write commands and respond to the NMS. The agent also sends a trap message to the NMS when the device is abnormal.

## SNMP Version And MIB

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



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

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

## SNMP Configuration

### Configure The Group Name

begin at the privileged configuration mode, configure the group name as shown in the table.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter the global configuration mode |
| **Step 2** | **snmp-server community** *name*  [ro| rw ] | Configure the SNMP community string |
| **Step 3** | **show snmp-server community** | Show the SNMP community configuration |
| **Step 4** | **exit** | Returns the privileged user configuration mode from the global configuration mode |
| **Step5** | **write** | Save configuration |

### Configure The Trap Server Address

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **config terminal** | Enter the global configuration mode |
| **Step 2a** | **snmp-server host** *A.B.C.D* community *WORD* udp-port (1-65535) version <1|2c|3> | Configure the trap target host address. Configure the community string value |
| **Step 3b** | **no snmp-server host**  *A.B.C.D*  **version <**1|2c|3>*community\_string or user\_name* | Remove the trap target host address |
| **Step 3** | **write** | Save configuration |

### Configure Association Information

begin at the privileged configuration mode, configure the association information, as shown in the following table.

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

### Configure Location Information

begin at the privilege configuration mode, configure the location information, as shown in the following table.

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

# Alarm And Event Management



## Description Of Alarms And Events

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

## Alarm Management

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

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

### System Alarm

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

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

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

### PON Alarm

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

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

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2a** | **alarm** <pon-register-failed|pon-deregister> <enable|disable> | Enable or disable PON alarm reporting |
| **Step 2b** | **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 reporting |
| **Step 3** | **show alarm configuration** | Display alarm configuration |

### ONU Alarm

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

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **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 reporting |
| **Step 3** | **show alarm configuration** | Displays system alarm configuration |

## Event Management

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

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

### System Event

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

|  |  |  |
| --- | --- | --- |
| **System event** | **Reason** | **Default** |
| reset | Equipment reset | disable |
| config-save | Save configuration | enable |
| config-erase | Erase configuration | enable |
| download-file-success | Download file successfully | enable |
| upload-file-success | File uploaded successfully | enable |
| upgrade-file-success | Firmware upgrade successful | enable |

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

### PON Event

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

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

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

### ONU Event

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

|  |  |  |
| --- | --- | --- |
| **ONU event** | **Reason** | **Default** |
| onu-register | ONU Registration | enable |
| onu-link-discover | ONU discovery | disable |
| onu-auth-success | OLT authorizes ONU to succeed | enable |
| onu-deauth-success | OLT successfully deauthorized ONU | disable |

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

# System Log



## Introduction

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

### 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 information 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

### Display System Log

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

### Clear System Log

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

### Configure System Log Server

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2a** | **remote server** <address|ip *A.B.C.D*|ipv6 *X:X::X:X*> **[secondary-server|username]**username *username* password*password* | Configure the IP address and port number of the system log server. |
| **Step 2b** | **no remote server** <ipv4|ipv6> | Delete system log server configuration. |

### Configure Storage Level

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

### Save System Logs To The Flash

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

### Clear System Logs In The Flash

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

### Upload System Log

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

# SSH Function

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

## SSH Configuration

### Enable The SSH Server

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

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **sshd** <disable|enable|reload|status> | Shut down, start, and reload the server,and show status |

### Configure Maximum Authentication Times of SSH

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **ip ssh authentication-retries** <(0-6)|default> | Specifies the number of authentication retries |

### Configure SSH Authentication Timeout Period

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **ip ssh time-out** <(1-120)|default> | Authentication timeout times |

### Configure Maximum Number Of SSH Connections

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **ip ssh max-startups** <(1-5)|default> | Maximum connection number |

### Configure Maximum Number Of SSH Sessions

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **ip ssh max-sessions** <(1-12)|default> | Maximum sessions |

## Display SSH

### Display the SSH Key

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **show crypto key mypubkey** <rsa|ecdsa|ed25519|all> | The SSH key is displayed |

### Display SSH Configuration

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ssh** | The SSH configuration node is displayed |
| **Step 3** | **show ip ssh** | Show SSH configuration |

# Diagnose Function

## Diagnose Configuration

### Network Connection Test

Run the ping command to check the network connection.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **ping** <ip|ipv6|*WORD*> -i vlan (1-4094) -s (56-65535) | Network test  -s: indicates a port  -i: The vlan is used | |

### Network Tracking Test

Use the traceroute command to check the network connection.

|  |  |  |
| --- | --- | --- |
|  | **Command** | **Function** |
| **Step 1** | **configure terminal** | Enter the global configuration mode |
| **Step 2** | **traceroute** <ip|ipv6|*WORD*> | Network tracking | |

**Thank you!**