User Guide

Manage the OLT via the Omada Controller

About this Guide

Omada Controller offers centralized and efficient management for configuring enterprise networks comprised of gateways, switches, wireless access points (APs), optical line terminals (OLTs), and more. This guide provides information for centrally managing OLTs via the Omada Controller. Please read this guide carefully before operation.

For instructions about how to use the Omada Controller, refer to the Omada Controller User Guide.

For instructions about how to manage other types of devices via the Omada Controller, refer to the relevant user guides.

Intended Readers

This User Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that:

- Features available in the Omada Controller may vary due to your region, controller type and version, and device model. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- This guide uses the specific formats to highlight special messages. The following table lists the notice icons that are used throughout this guide.

In this guide, the following conventions are used:

Controller	Stands for the Omada On-Premises Controller and the Omada Cloud-Based Controller.
On-Premises Controller	Includes the Omada Software Controller (also referred to as the Omada Network Application), Omada Hardware Controller, and Omada Integrated Gateway (Controller).
Cloud-Based Controller/ Omada Central	The Omada Cloud-Based Controller is now referred to as the Omada Network system on the Omada Central. Note that the Omada Central integrates the Omada Network system and Omada Guard system. The Omada Network system works as an Omada Controller to manage network devices (gateways, switches, access points, OLTs, and more), while the Omada Guard system works as a VMS system to manage surveillance devices (security cameras, NVRs, and more). This guide involves instructions about the Omada Network system. For instructions about the Omada Guard system, refer to the Omada Guard User Guide.

OLT	Stands for the DeltaStream GPON Optical Line Terminal.
Note:	The note contains the helpful information for a better use of the controller.
Configuration Guidelines:	Provide guidelines for the feature and its configurations.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

For technical support, the latest software, and management app, visit https://support.omadanetworks.com/.

CONTENTS

About this Guide

1.Manage the OLT

2.Configure General Info and Interface

3.Configure PON

4.Configure L2 Features

5.Configure L3 Features

6.Configure Multicast

7.Configure QoS

8.Configure Security

9.Configure Device Maintenance

10.Manage System

Chapter 1

Manage the OLT

This chapter guides you on how to configure and monitor controller-managed OLT devices. You can configure the devices individually or in batches to modify device configurations. The chapter includes the following sections:

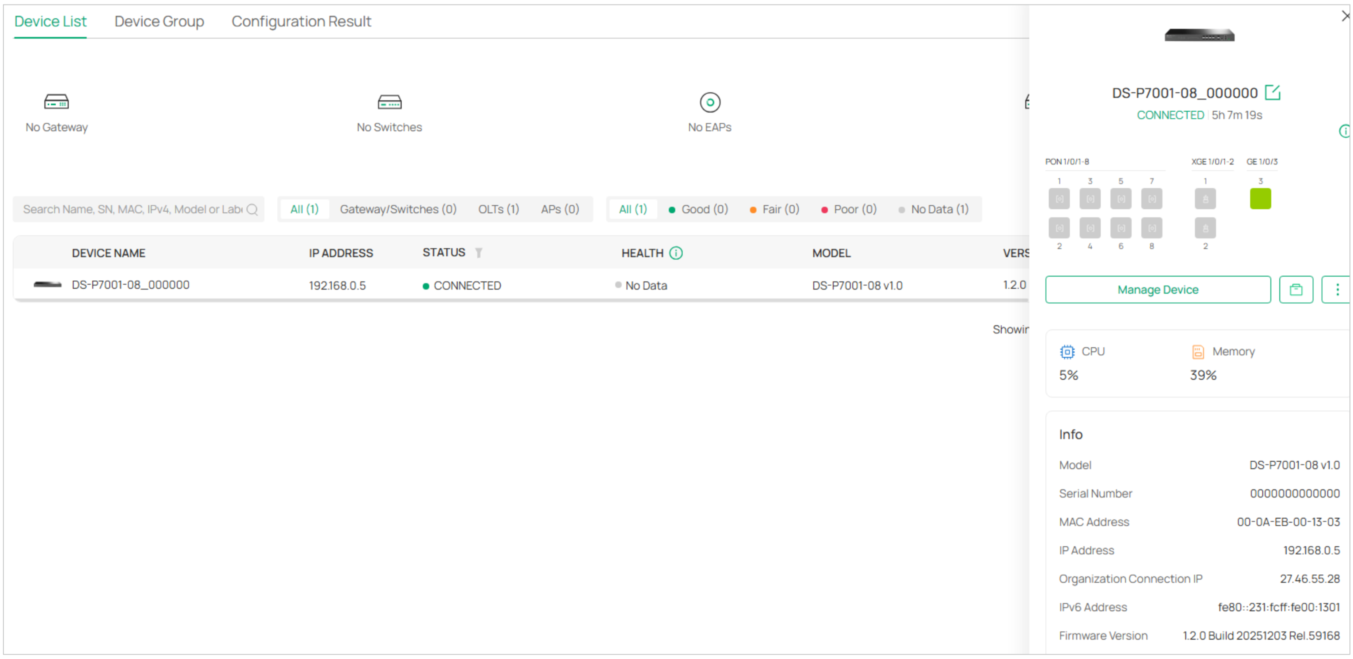
1.1 Properties Window

Launch the controller and access a site. Go to Devices > Device List. In the device list, click an OLT, then you can monitor and manage it in the Properties window and Device Management window.

1.1.1 Properties Window

The Properties window displays the device status, port status, and other device information.

Note: The available functions in the window may vary by device model and status.



Device List | Device Group | Configuration Result

No Gateway | No Switches | No EAPs

Search Name, SN, MAC, IPv4, Model or Labe

All (1) | Gateway/Switches (0) | OLTs (1) | APs (0)

All (1) | ● Good (0) | ● Fair (0) | ● Poor (0) | ● No Data (1)

DEVICE NAME	IP ADDRESS	STATUS	HEALTH	MODEL	VERS
DS-P7001-08_000000	192.168.0.5	● CONNECTED	● No Data	DS-P7001-08 v1.0	1.2.0

Showir

DS-P7001-08_000000

CONNECTED | 5h 7m 19s

Manage Device

CPU	Memory
5%	39%

Info

Model	DS-P7001-08 v1.0
Serial Number	0000000000000
MAC Address	00-0A-EB-00-13-03
IP Address	192.168.0.5
Organization Connection IP	27.46.55.28
IPv6 Address	fe80::231:fcff:fe00:1301
Firmware Version	1.2.0 Build 20251203 Rel.59168

1.1.2 Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

1.1.3 Network Tools

Click the 🧰 icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute.

1.2 Device Management Window

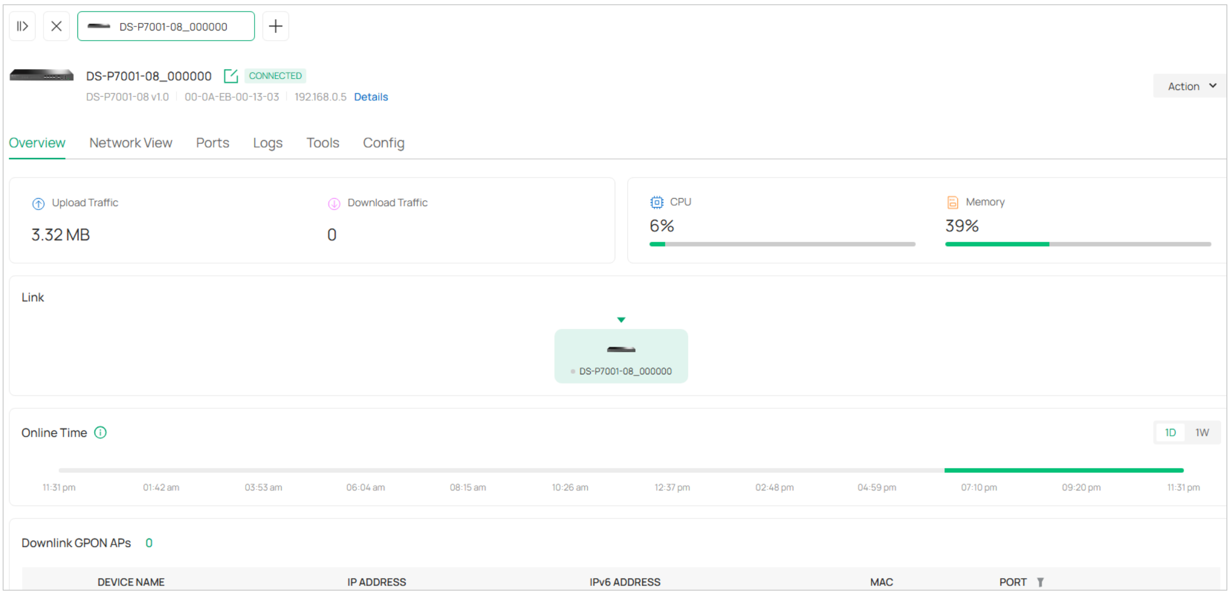
Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the II> icon in the top left to minimize the windows to the <II icon in the right side, and click the <II icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

1.2.1 Overview

In Overview, you can get an overview of the device, such as device status, link status, online time, downlink GPON APs, and more.



DS-P7001-08_000000 CONNECTED

DS-P7001-08 v1.0 | 00-0A-EB-00-13-03 | 192.168.0.5 Details

Upload Traffic: 3.32 MB

Download Traffic: 0

CPU: 6%

Memory: 39%

Link: DS-P7001-08_000000

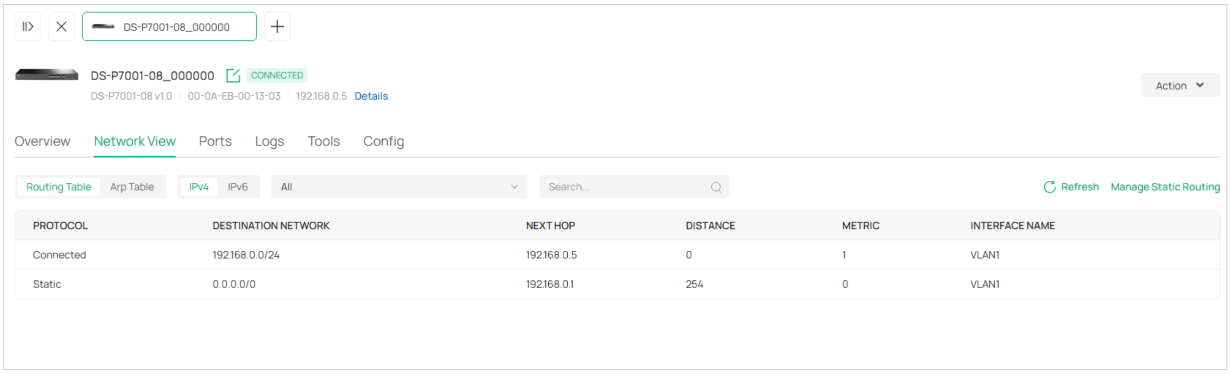
Online Time

Downlink GPON APs 0

DEVICE NAME	IP ADDRESS	IPv6 ADDRESS	MAC	PORT

1.2.2 Network View

In Network View, you can check the network information of the device, such as routing table and ARP table.



DS-P7001-08_000000 CONNECTED

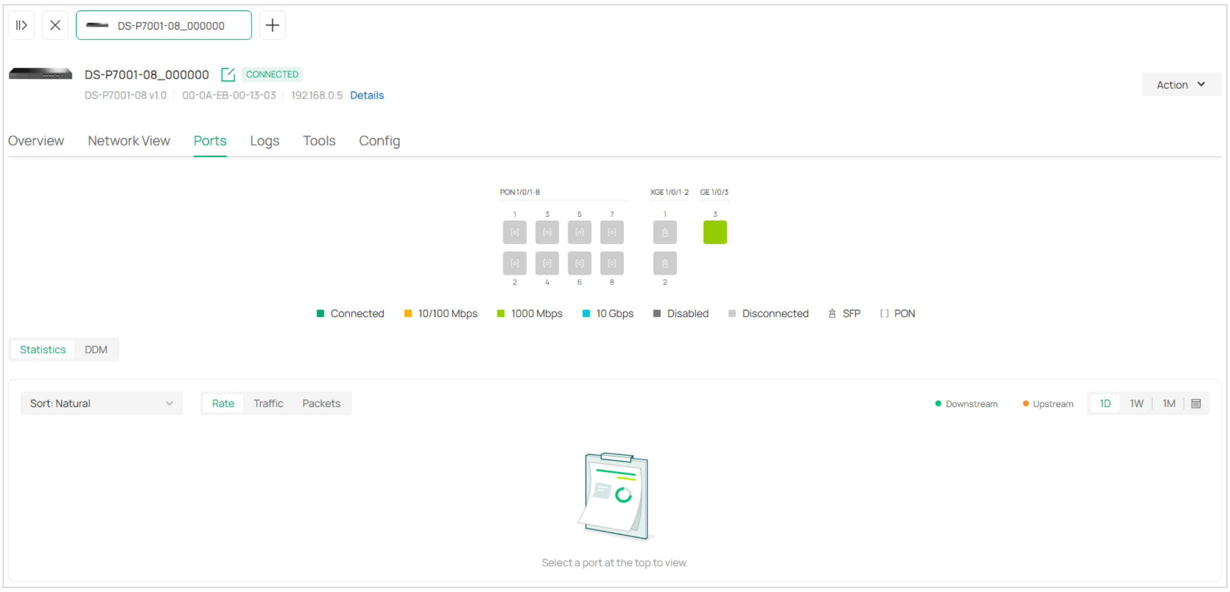
DS-P7001-08 v1.0 | 00-0A-EB-00-13-03 | 192.168.0.5 Details

PROTOCOL	DESTINATION NETWORK	NEXT HOP	DISTANCE	METRIC	INTERFACE NAME
Connected	192.168.0.0/24	192.168.0.5	0	1	VLAN1
Static	0.0.0.0/0	192.168.0.1	254	0	VLAN1

Note: The routing table is displayed in the IPv6 tab by default when there is no IPv4 data.

1.2.3 Ports

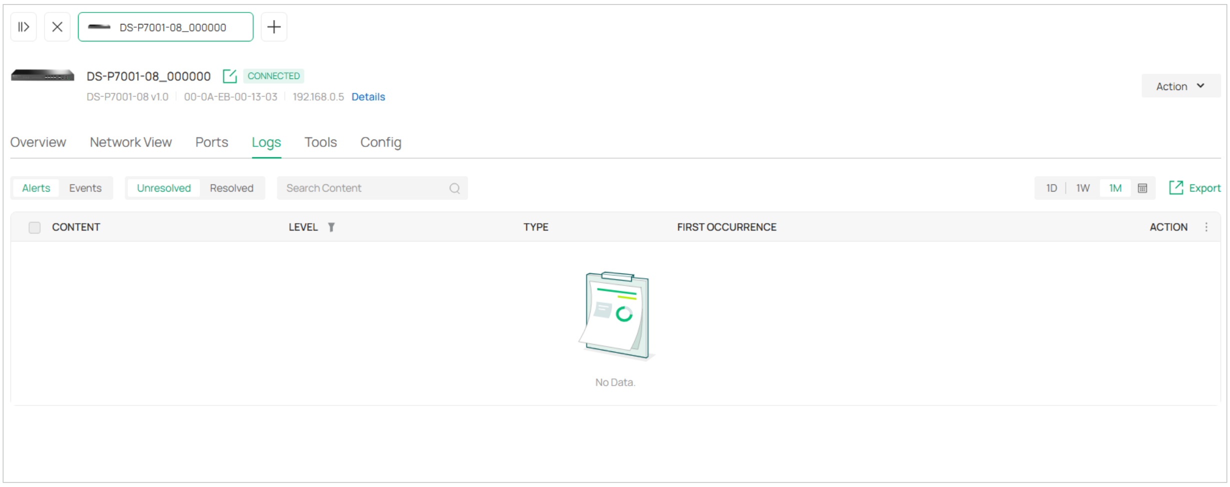
In Ports, you can view the port status and statistics.



Select a port at the top to view.

1.2.4 Logs

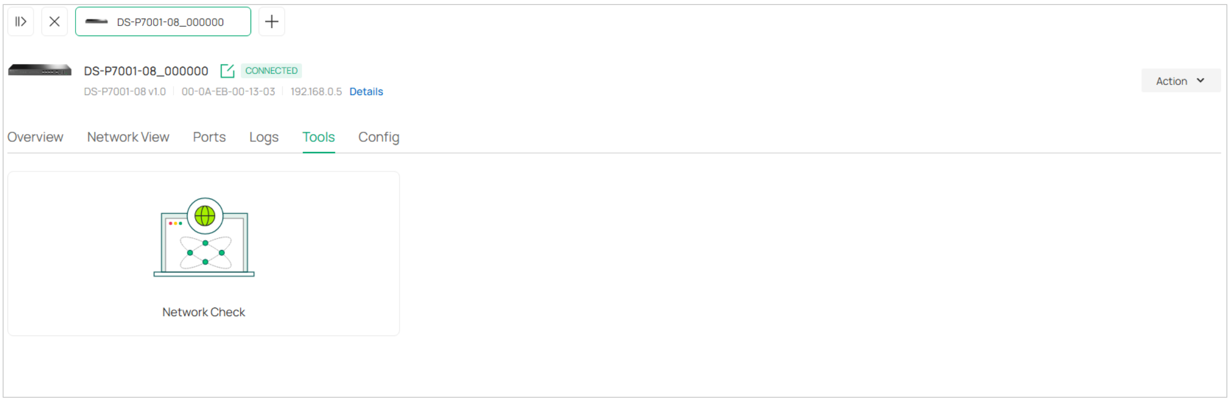
In Logs, you can check the logs of the device, such as alerts and events.



No Data.

1.2.5 Tools

In Tools, you can use the network tool to test the device connectivity.



Chapter 2

Configure General Info and Interface

This chapter guides you on how to configure the general information and interface of the OLT devices. The chapter includes the following sections:

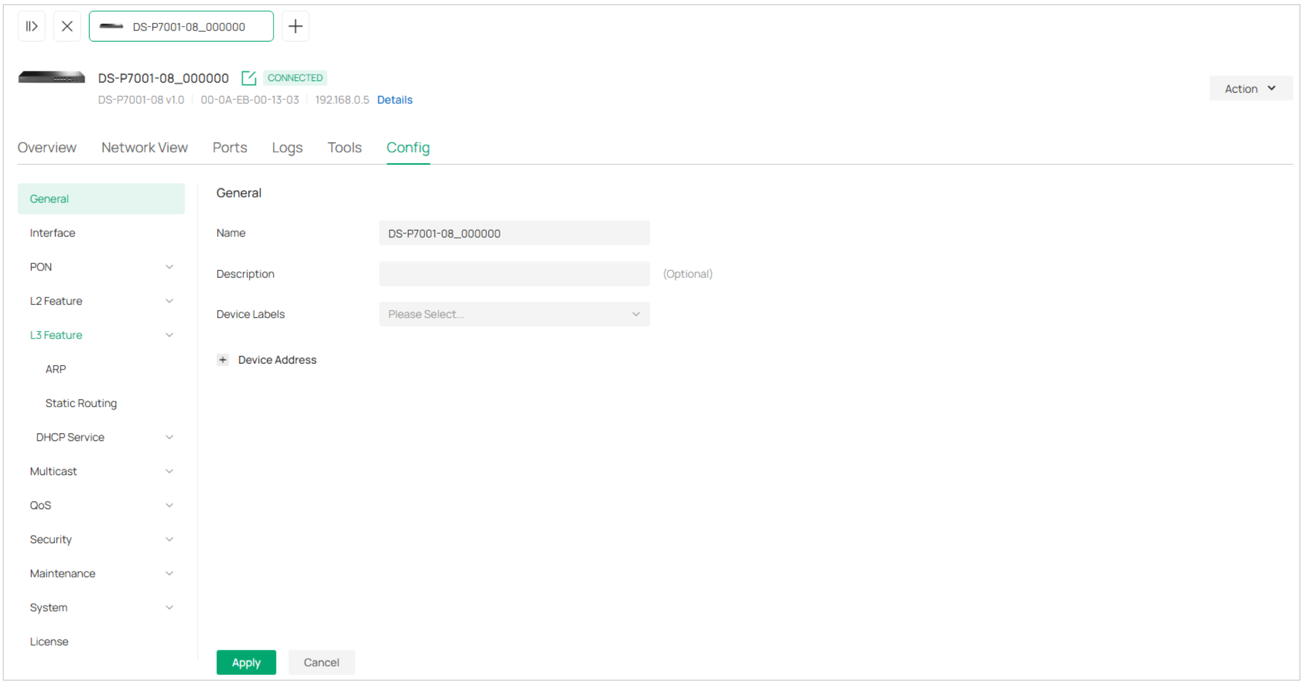
- 2.1 Configure General Info
- 2.2 Configure Interface

2.1 Configure General Info

Launch the controller and access a site. Go to Devices > Device List. In the device list, click an OLT, click Manage Device and go to the Config > General.

In General, you can configure the general information of the OLT, such as name, description, and device labels. Also, you can click + to add device address

Note: The available functions in the window may vary by device model and status.



General

Name: DS-P7001-08_000000

Description: (Optional)

Device Labels: Please Select...

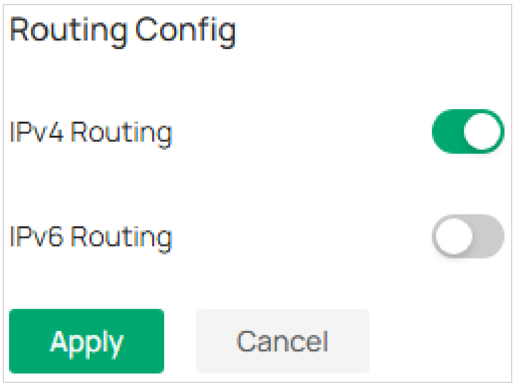
+ Device Address

2.2 Configure Interface

Interfaces are used to exchange data and interact with interfaces of other network devices. Interfaces are classified into Layer 2 interfaces and Layer 3 interfaces. Layer 2 interfaces are the physical ports on the OLT panel. They forward packets based on MAC address table. Layer 3 interfaces are used to forward IPv4 and IPv6 packets using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter-VLAN routing.

Launch the controller and access a site. Go to Devices > Device List. In the device list, click an OLT, click Manage Device and go to the Config > Interface.

1. In Routing Config, you can enable the desired routing.



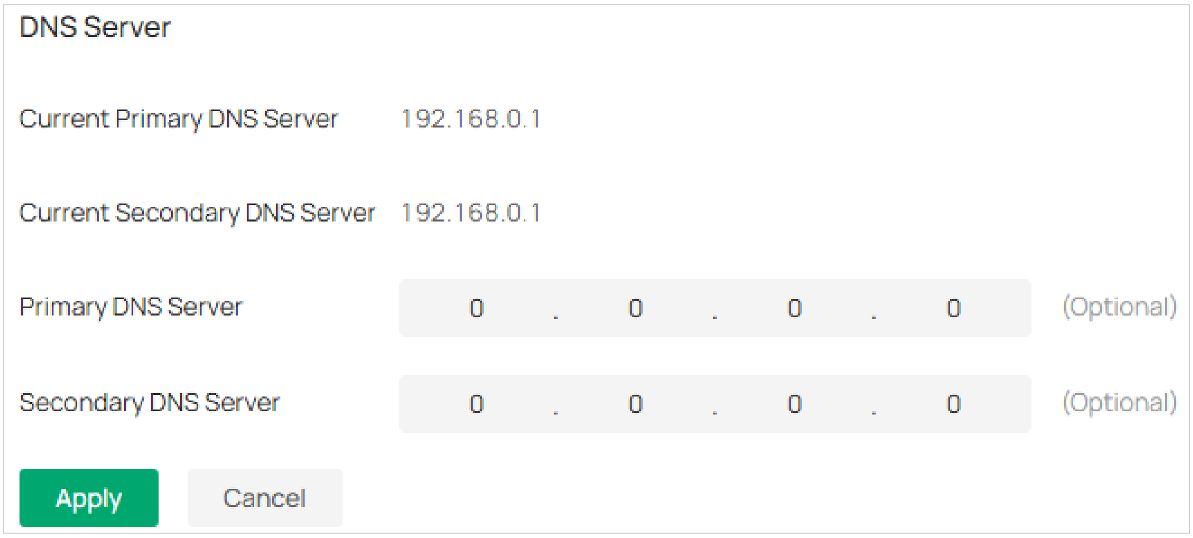
Routing Config

IPv4 Routing: ●

IPv6 Routing: ○

IPv4 Routing	Enable IPv4 routing function globally for all Layer 3 interfaces. It is enabled by default.
IPv6 Routing	Enable IPv6 routing function globally for all Layer 3 interfaces. It is disabled by default.

2. In DNS Server, you can configure the primary and secondary DNS server addresses.

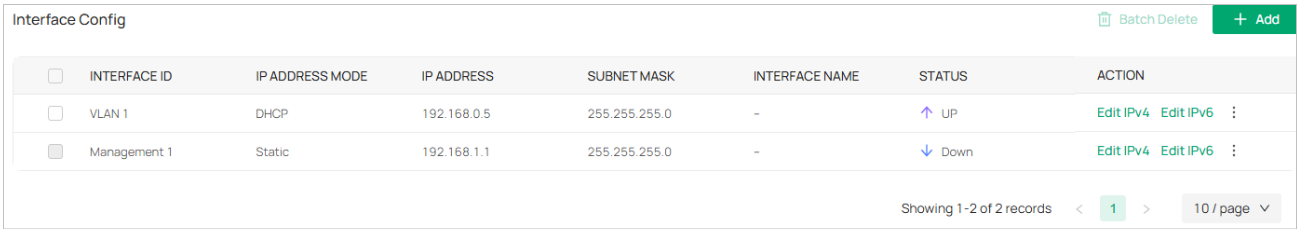


DNS Server

Current Primary DNS Server	192.168.0.1
Current Secondary DNS Server	192.168.0.1
Primary DNS Server	0 . 0 . 0 . 0 (Optional)
Secondary DNS Server	0 . 0 . 0 . 0 (Optional)

3. In Interface Config, you can configure the features of the interfaces. Click +Add on the upper right and configure the parameters. Click Create.

Note that the created interface is an IPv4 interface, if you want to configure the IPv6 features, please click Edit IPv6 after the interface is created.



Interface Config

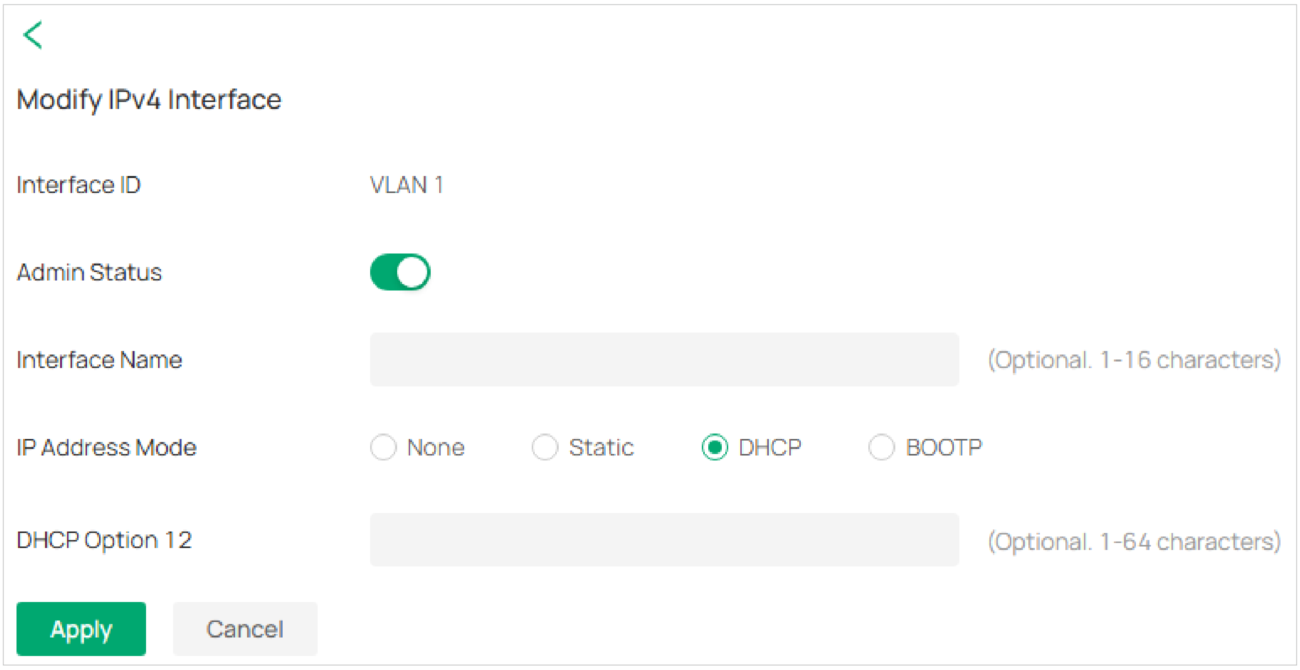
□	INTERFACE ID	IP ADDRESS MODE	IP ADDRESS	SUBNET MASK	INTERFACE NAME	STATUS	ACTION
□	VLAN 1	DHCP	192.168.0.5	255.255.255.0	-	↑ UP	Edit IPv4 Edit IPv6 ⋮
□	Management 1	Static	192.168.1.1	255.255.255.0	-	↓ Down	Edit IPv4 Edit IPv6 ⋮

Showing 1-2 of 2 records < 1 > 10 / page

Interface ID	Displays the ID of the interface.
IP Address Mode	Specify the IP address assignment mode of the interface. None: No IP address will be assigned to the interface. Static: Assign an IP address to the interface manually. DHCP: Assign an IP address to the interface through the DHCP server. BOOTP: Assign an IP address to the interface through the BOOTP server.
IP Address	If you select Static as the IP Address Mode, enter the IP address here.
Subnet Mask	If you select Static as the IP Address Mode, enter the subnet mask here.
DHCP Option 12	If you select DHCP as the IP Address Mode, configure the Option 12 here. DHCP Option 12 is used to specify the client's name.

Admin Status	Enable or disable the L3 capabilities of the interface.
Interface Name	(Optional) Enter a name for the interface.

After an interface is created, it will be displayed in the table of Interface Config. For interfaces whose IP Address Mode is set as Static, you can add a secondary IP, which allows you to have two logical subnets. Click Edit IPv4 or Edit IPv6 in the Action column of the interface to load the following page. In Secondary IP Config, click +Add on the upper right and configure the parameters. Click Create.



Modify IPv4 Interface

Interface ID: VLAN 1

Admin Status: On

Interface Name: (Optional. 1-16 characters)

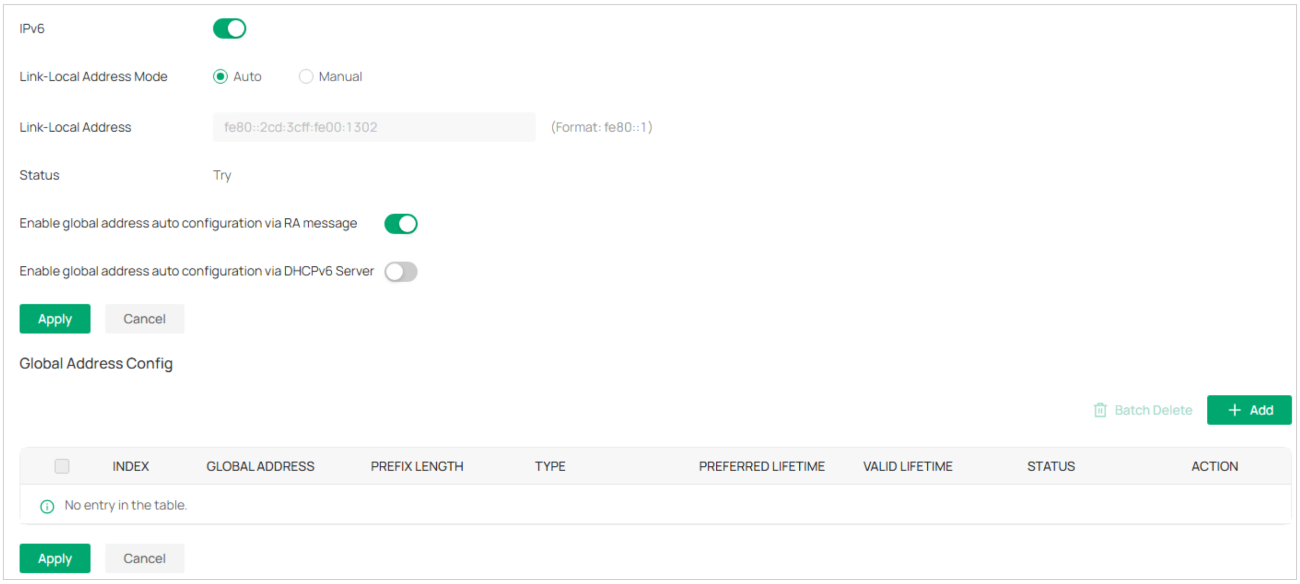
IP Address Mode: ○ None ○ Static ● DHCP ○ BOOTP

DHCP Option 12: (Optional. 1-64 characters)

IP Address	If you select Static as the IP Address Mode, enter the IP address here.
Interface Name	(Optional) Enter a name for the interface.
IP Address Mode	Specify the IP address assignment mode of the interface. None: No IP address will be assigned to the interface. Static: Assign an IP address to the interface manually. DHCP: Assign an IP address to the interface through the DHCP server. BOOTP: Assign an IP address to the interface through the BOOTP server.
DHCP Option 12	If you select DHCP as the IP Address Mode, configure the Option 12 here. DHCP Option 12 is used to specify the client's name.

(Optional) If you want to configure the IPv6 features of an interface, click Edit IPv6 in the Action column of the interface to load the following page. In Modify IPv6 Interface, configure the parameters. Click Apply.

If you want to manually assign an IPv6 global address to the interface, configure the parameters in Global Address Config. Click Apply.



IPv6: On

Link-Local Address Mode: ● Auto ○ Manual

Link-Local Address: fe80::2cd:3cff:fe00:1302 (Format: fe80::1)

Status: Try

Enable global address auto configuration via RA message: On

Enable global address auto configuration via DHCPv6 Server: Off

Global Address Config

□	INDEX	GLOBAL ADDRESS	PREFIX LENGTH	TYPE	PREFERRED LIFETIME	VALID LIFETIME	STATUS	ACTION

No entry in the table.

Interface ID	Displays the interface ID.
IPv6 Enable	Enable the IPv6 feature of the interface.
Link-local Address Mode	Select the link-local address configuration mode. Auto: With this option selected, the OLT generates a link-local address automatically. Manual: With this option selected, you can assign a link-local address manually.
Link-local Address	Enter a link-local address if you choose “Manual” as the Link-Local Address Mode.
Status	Displays the status of the link-local address. An IPv6 address cannot be used before pass the DAD (Duplicate Address Detection), which is used to detect the address conflicts. In the DAD process, the IPv6 address may in three different status: Normal: Indicates that the link-local address passes the DAD and can be used normally. Try: Indicates that the link-local address is in the progress of DAD and cannot be used right now. Repeat: Indicates that the link-local address is duplicated, this address is already used by another node and cannot be used by the interface.
Enable global address auto configuration via RA message	With this option enabled, the interface automatically generates a global address and other information according to the address prefix and other configuration parameters from the received RA (Router Advertisement) message.
Enable global address auto configuration via DHCPv6 Server	With this option enabled, the OLT will try to obtain the global address from the DHCPv6 Server.

Address Format	Select the global address format according to your needs. EUI-64: Indicates that you only need to specify an address prefix, then the system will create a global address automatically. Not EUI-64: Indicates that you have to specify an intact global address.
Global Address	When EUI-64 is selected, please input the address prefix here, otherwise, please input an intact IPv6 address here.
Prefix Length	Configure the prefix length of the global address.

Chapter 3

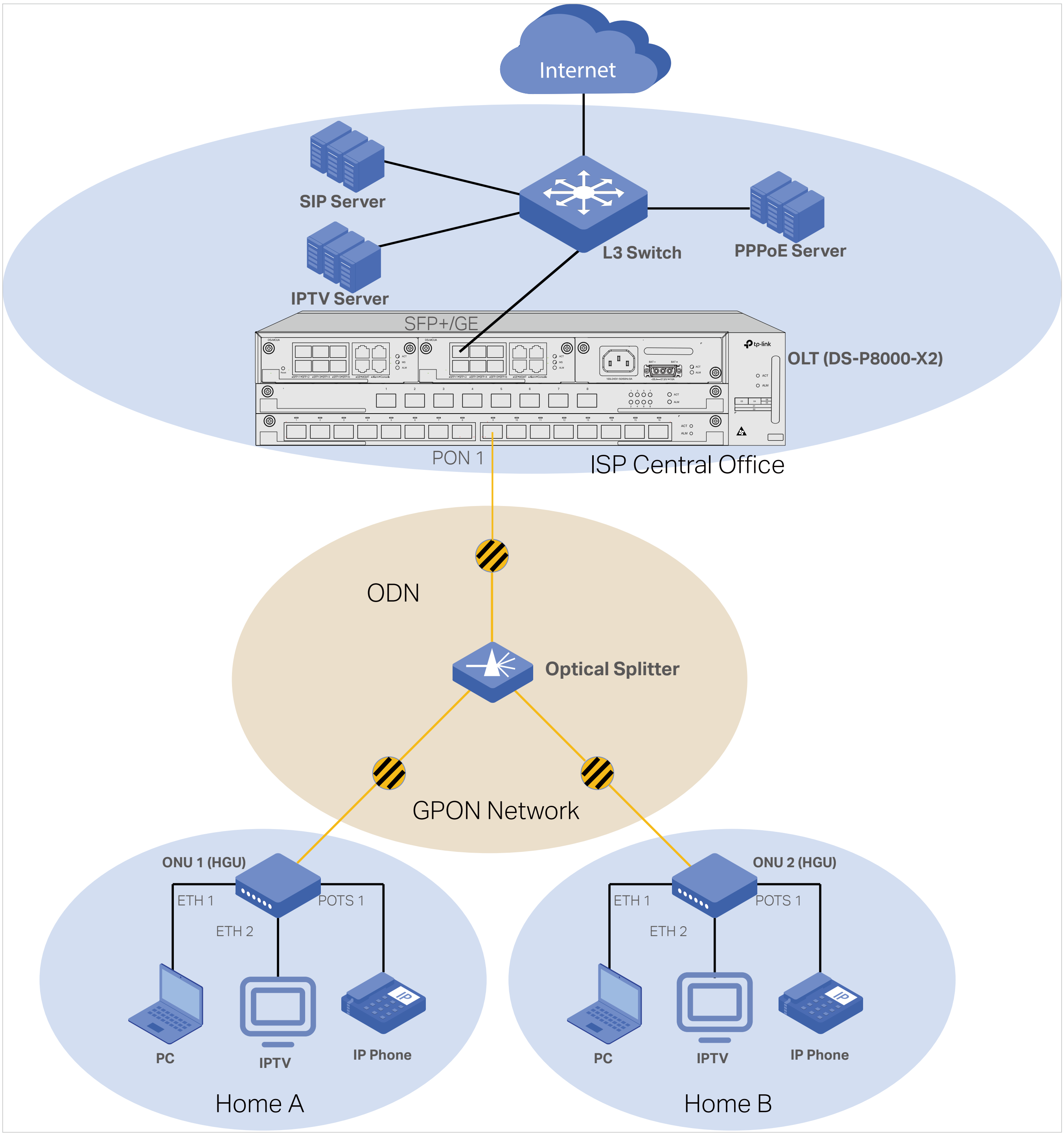
Configure PON

This chapter guides you on how to configure PON (Passive Optical Network) on OLT. The chapter includes the following sections:

3. 1 Overview

3. 1. 1 GPON Network Component

The following figure shows a typical network topology of FTTH (Fiber to the Home) service.



The GPON Network consists of the following components.

OLT	OLT (Optical Line Terminal), such as DS-P7001-08, is the core GPON network device, located at the ISP's central office. GPON networks are extended from the PON ports of OLT, and oriented to the locations of ISP's end users. OLT is uplinked, via the SFP+/SFP/GE ports, to the ISP's L3 Switch, connected to the ISP central network and internet.
ONU (ONT)	ONU (Optical Network Unit) is deployed at the end user's location, and used to access the GPON network of ISP. ONU is uplinked to the GPON network and have downlink ports connected to the user's local network. The user's devices, such as PC, IPTV, and IP Phone, enjoy multiple ISP's services via the connection between ONU and OLT. ONUs are managed and controlled by the OLT via OMCI (ONT Management and Control Interface). In this document, ONU and ONT (Optical Network Terminal) can be used interchangeably. There are different types of ONUs, such as HGU (Home Gateway Unit) and SFU (Single Family Unit).
ODN	ODN (Opitcal Distribution Network) is a network that consists of optical fibers and passive optical components, such as one or more optical splitters. The ODN network provides highly reliable optical paths to connect ONUs to an OLT.
L3 Switch of ISP	The L3 switch is the core component of the ISP's central network, which is used to distribute traffic of various services.
Servers of ISP	The servers of ISP provide multiple services for the users' client via the GPON network. The servers include the PPPoE server (for internet access service), the IPTV server, the SIP server (for VOIP service), and so on.
Clients of Users	Clients of users include PC, IPTV, IP Phone, and so on.

3. 1. 2 Configuration Scheme

We have the following demands when configuring GPON netowork.

1) The ONU is deployed in the user's home and connected to the GPON network. After registration, the ONU should be able to communicate with the OLT via GPON network.

2) ISP provides multiple services for the user, including internet service, IPTV service, and VoIP service. Different types of traffic should be managed seperately in different VLANs and with different QoS priorities.

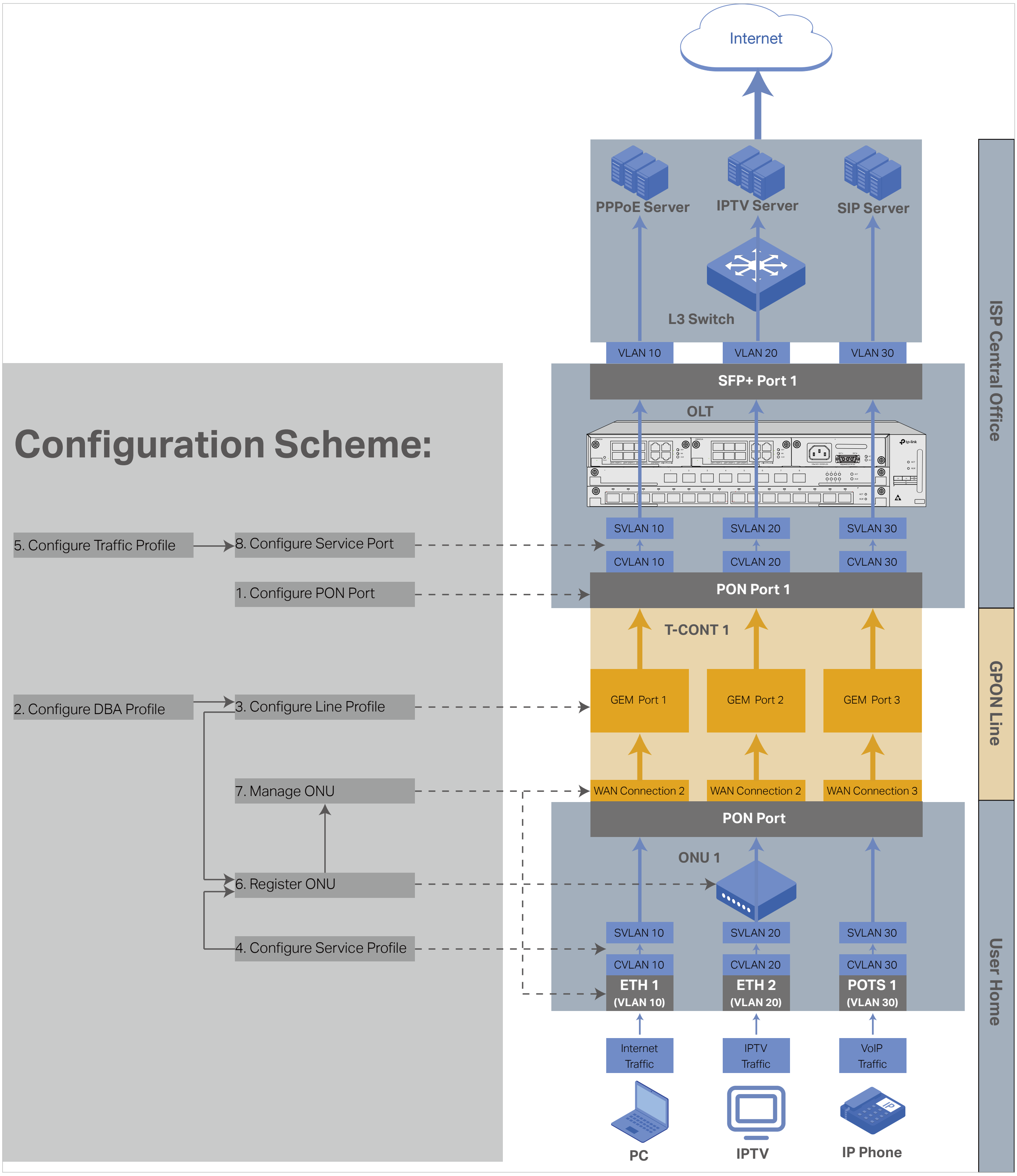
To meet the demands, take the following steps to configure the GPON network on OLT.

3. 2. 1 Configure PON Port	You can set parameters for each PON port and view the port information.
3. 2. 2 Configure DBA Profile	DBA (Dynamic Bandwidth Allocation) improves the efficiency of GPON upstream bandwidth by dynamically adjusting the bandwidth among the ONUs. DBA profile is used to set up the desired bandwidth allocation for any GPON line. When you create line profiles afterwards, you need to apply the DBA profile to the T-CONT in line profiles.

3. 2. 3 Configure Line Profile	A line profile includes T-CONTs, GEM ports and GEM mapping rules. GEM (GPON Encapsulation Mode) ports are the basic transmission units in the GPON network. The T-CONT (Transmission Container) functions as a tunnel which contains several GEM ports. Different types of traffic from the ONU are mapped to different GEM ports according to the GEM Mapping rules.
3. 2. 4 Configure Service Profile	Service Profiles are used by ONUs to transmit traffic of different services to different SVLANs based on ONU ports, VLAN and priority.
3. 2. 5 Configure Traffic Profile	Traffic profile is used to set up desired rate limit and VLAN priority for any traffic which uses this profile. Traffic profiles can be applied to service ports, and so on.
3. 2. 6 Configure Management Profile	Management profiles are used to uniformly configure ONU management settings, including ONU WAN connection configuration, ONU Wireless configuration, ONU VoIP configuration, ONU CWMP configuration, ONU CATV configuration, etc. If you want to configure the above settings uniformly, you can create management profiles according to your needs.
3. 2. 7 Register ONU	After connecting the ONU to the GPON network, the ONU is auto-found by the OLT. Then you need to authenticate and register the ONU. After that, the ONU goes online and is able to communicate with the OLT via the GPON network.
3. 2. 8 Manage ONU	In ONU management, you can view ONU status, configure ONU ports and WAN connections, and upgrade ONUs.
3. 2. 9 Service Ports	Service ports are used by OLT to map different types of traffic to different SVLANs according to PON ports, ONUs, GEM ports, User VLANs, and priorities, and then transmitted to the uplink network. The rate limit for inbound and outbound traffic of the uplink network is determined by traffic profiles which are applied to the service ports.

The configuration scheme is illustrated as the following figure.

Note: The VLAN ID, port number, T-CONT ID, GEM Port ID, WAN connection ID and other parameters used in this figure are only for demonstration. Please configure these parameters according to the requirements of your network.



3. 2 Configuration Steps

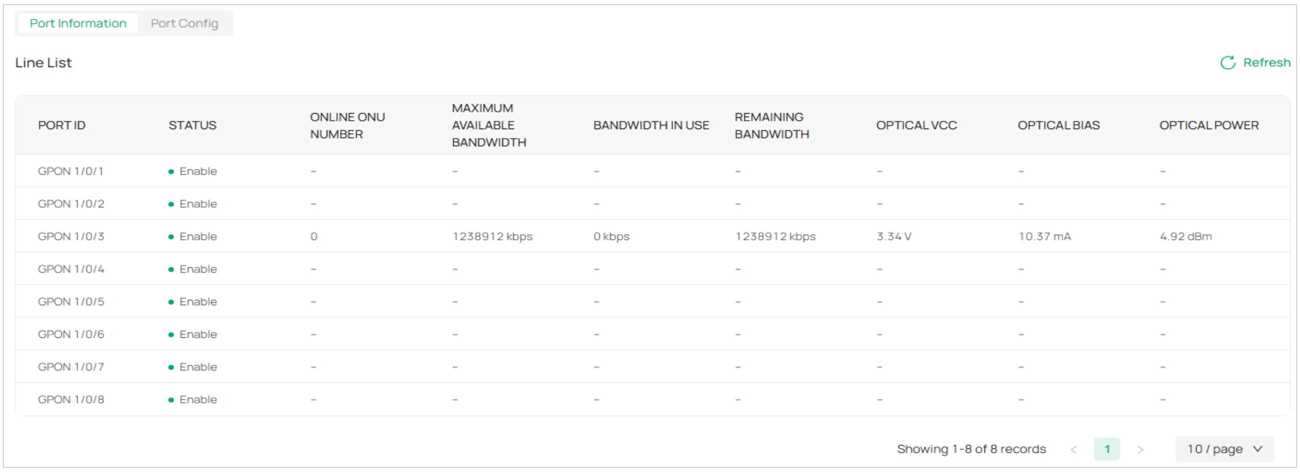
3. 2. 1 Configure PON Port

Overview

With PON Port, you can set parameters for each PON port and view the port information.

Configuration

1. Go to PON > PON Port > Port Information to load the following page. You can view the informaton of each PON port. You can click Refresh to refresh the information.

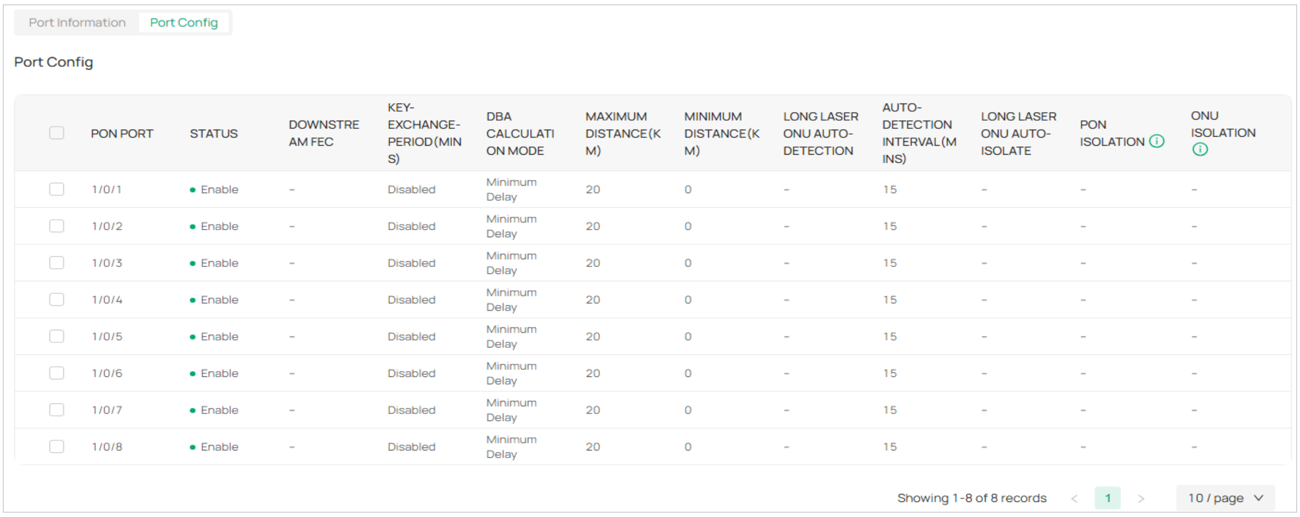


PORT ID	STATUS	ONLINE ONU NUMBER	MAXIMUM AVAILABLE BANDWIDTH	BANDWIDTH IN USE	REMAINING BANDWIDTH	OPTICAL VCC	OPTICAL BIAS	OPTICAL POWER
GPON 1/0/1	● Enable	-	-	-	-	-	-	-
GPON 1/0/2	● Enable	-	-	-	-	-	-	-
GPON 1/0/3	● Enable	0	1238912 kbps	0 kbps	1238912 kbps	3.34 V	10.37 mA	4.92 dBm
GPON 1/0/4	● Enable	-	-	-	-	-	-	-
GPON 1/0/5	● Enable	-	-	-	-	-	-	-
GPON 1/0/6	● Enable	-	-	-	-	-	-	-
GPON 1/0/7	● Enable	-	-	-	-	-	-	-
GPON 1/0/8	● Enable	-	-	-	-	-	-	-

Showing 1-8 of 8 records < 1 > 10 / page

Port ID	Displays the port ID of PON port.
Status	Displays the status of the PON port. If the PON port is disabled, the PON port does not work.
Online ONU Number	Displays the number of online ONUs which are connected to the PON port.
Maximum Available Bandwidth	Displays the maximum bandwidth available for the PON port.
Bandwidth In Use	Displays the bandwidth used by the PON port.
Remaining Bandwidth	Displays the remaining bandwidth that can be used by the PON port.
Optical VCC	Displays the optical supply voltage (V) of the PON port.
Optical Bias	Displays the optical bias current (mA) of the PON port.
Optical Power	Displays the optical power (dBm) of the PON port.

2. Go to PON > PON Port > Port Config to load the following page. Select the PON ports and configure the parameters of the PON ports.



Port Information | Port Config

Port Config

□	PON PORT	STATUS	DOWNSTREAM FEC	KEY-EXCHANGE-PERIOD(MINS)	DBA CALCULATION MODE	MAXIMUM DISTANCE(KM)	MINIMUM DISTANCE(KM)	LONG LASER ONU AUTO-DETECTION	AUTO-DETECTION INTERVAL(MINS)	LONG LASER ONU AUTO-ISOLATE	PON ISOLATION ⓘ	ONU ISOLATION ⓘ
□	1/0/1	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/2	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/3	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/4	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/5	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/6	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/7	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-
□	1/0/8	● Enable	-	Disabled	Minimum Delay	20	0	-	15	-	-	-

Showing 1-8 of 8 records < 1 > 10 / page

Port ID

Displays the port ID of PON port.

Status

Enable or disable the PON port. If the PON port is disabled, the PON port does not work.

Downstream FEC

Enable or disable the FEC (Forward Error Correction) function of the PON port. To enhance the data transmission reliability of the downstream link between an OLT and an ONT, enable Downstream FEC. After the FEC function is enabled, the system inserts the redundancy data into the normal packets. In this manner, the line is provided with error tolerance function, but certain bandwidth is wasted.

Key Exchange Period

Configure the intervals of updating the key used in line encryption of the PON port. Key Exchange Period should be between 0 and 60. If Key Exchange Period is set as 0, this means line encryption is disabled for the PON port.

In a GPON system, downstream data is broadcast to all ONUs. Then, unauthorized ONUs can receive the downstream data of authorized ONUs, causing system risks.

Line encryption is used to eliminate these security risks. The GPON system uses the Advanced Encryption Standard 128 (AES128) algorithm to encrypt the data packets transmitted in plaintext mode so that the packets are transmitted in ciphertext mode, improving system security.

DBA Calculation Mode

Set the DBA (dynamic bandwidth allocation) mode of a GPON port. Users can configure different DBA modes to meet different delay and bandwidth requirements.

Min-Delay: Indicates the minimum bandwidth delay. In this mode, the bandwidth is issued in DBA calculation period which increases with the number of the transmission container (T-CONT). Therefore, the delay is short. This mode must be used for TDM (Time Division Multiplexing) services.

Max-BW: Indicates the maximum bandwidth delay. In this mode, the bandwidth is issued in DBA calculation period which is fixed to eight frames. Each frame is 125 us. This mode is used for services that are not sensitive to delay.

Maximum Distance

Set the maximum distance of the ONUs which are connected to the PON port.

Minimum Distance

Set the minimum distance of the ONUs which are connected to the PON port.

Long Laser ONU Auto-Detection

Enable or disable the auto-detection of rogue ONUs which are connected to the PON port.

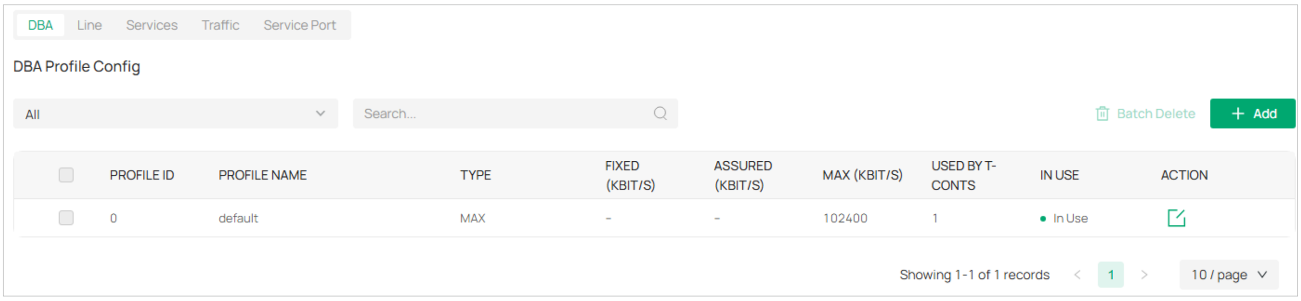
Auto-Detection Interval	Configure the intervals of detecting rougue ONUs which are connected to the PON port.
Long Laser ONU Auto-Isolation	Enable or disable the auto-isolation of rogue ONUs which are connected to the PON port.
Port Isolation	If the PORT ISOLATION is enabled on both PON ports, they will be isolated from each other; otherwise, they will be interconnected. **Note:** Enabling PON isolation may affect the 11r function of the downlink GPON AP.
ONU Isolation	If the ONU ISOLATION is enabled on the PON port, the ONUs under that port will be isolated from each other; otherwise, they will be interconnected. For Pizzabox OLT, these isolation functions are supported and enabled by default. For chassis OLT, these isolation functions are not supported. When either Port/ONU Isolation function in Configure PON Port or ONU VLAN Isolation function in View ONU Information is enabled, the isolation takes effect. **Note:** Enabling ONU isolation may affect the 11r function of the downlink GPON AP.

3. 2. 2 Configure DBA Profile

DBA (Dynamic Bandwidth Allocation) improves the efficiency of GPON upstream bandwidth by dynamically adjusting the bandwidth among the ONUs. DBA profiles are applied to T-CONTs, which are created in a line profile, to determine the desired bandwidth allocation for certain GPON lines.

When the default DBA profile cannot meet the service requirements, you can add DBA profiles according to the service requirements.

Go to PON > Profile > DBA, and click + Add. Configure the parameters and click Create.



DBA Profile Config

	PROFILE ID	PROFILE NAME	TYPE	FIXED (KBIT/S)	ASSURED (KBIT/S)	MAX (KBIT/S)	USED BY T-CONTS	IN USE	ACTION
□	0	default	MAX	-	-	102400	1	● In Use	

Profile ID	(Optional) Set the profile ID of the DBA profile. The profile ID is the unique identifier for the DBA profile. If you leave the profile ID as blank, the system automatically assigns the profile ID.
Profile Name	(Optional) Specify the profile name of the DBA profile.

Type	Select the type of bandwidth allocation of the DBA profile. Fix: Indicates a DBA profile of the fixed bandwidth type. The fixed bandwidth is reserved for a specified ONU or certain services of the ONU. It cannot be used for other ONUs even when the upstream service stream is not transmitted on the ONU. This type of bandwidth is mainly used for services, such as TDM and VoIP, that have a high QoS requirement. Assure: Indicates a DBA profile of the assured bandwidth type. The assured bandwidth is the available bandwidth of an ONU when the ONU requires the bandwidth. When the actual service stream does not reach the assured bandwidth, the DBA mechanism of the device is used to allocate the remaining bandwidth to services of other ONUs. Because of the DBA mechanism that allocates the remaining bandwidth to services of other ONUs, the assured bandwidth has a poorer real-time performance than fixed bandwidth does. Assure+Max: Indicates a DBA profile of the assured bandwidth + maximum bandwidth type. This type of bandwidth is the bandwidth of the combined type. When it is used, the user is allocated with a certain bandwidth and at the same time occupies certain bandwidths. The total bandwidth, however, cannot exceed the maximum bandwidth configured for the user. This type of bandwidth is mainly used for VoIP and IPTV service. Max: Indicates a DBA profile of the maximum bandwidth type. This type of bandwidth is the maximum bandwidth that can be used by an ONU to meet the ONU bandwidth requirement to the greatest extent. It is used for services such as Internet access service. Fix+Assure+Max: Indicates a DBA profile of the fixed bandwidth + assured bandwidth + maximum bandwidth type. This type of bandwidth is the bandwidth of the combined type. When it is used, the user is allocated with the fixed bandwidth that cannot be used by other users. In addition, the user can use the assured bandwidth when necessary and can occupy certain bandwidths. The total bandwidth, however, cannot exceed the maximum bandwidth configured for the user.
Fix Bandwidth	Indicates the fixed bandwidth. After the fixed bandwidth is allocated to a user, even the user does not use the bandwidth, others cannot use the bandwidth. Fix Bandwidth is only available for the type of Fix or Fix+Assure+Max.
Assure Bandwidth	Indicates the assured bandwidth. After the assured bandwidth is allocated to a user, if the user does not use the bandwidth, others can use the bandwidth. Assure Bandwidth is only available for the type of Assure, Assure+Max, or Fix+Assure+Max.
Max Bandwidth	Indicates the maximum bandwidth. Maximum bandwidth is the bandwidth that a user can use at most. Max Bandwidth is only available for the type of Assure+Max, Max, or Fix+Assure+Max.

3. 2. 3 Configure Line Profile

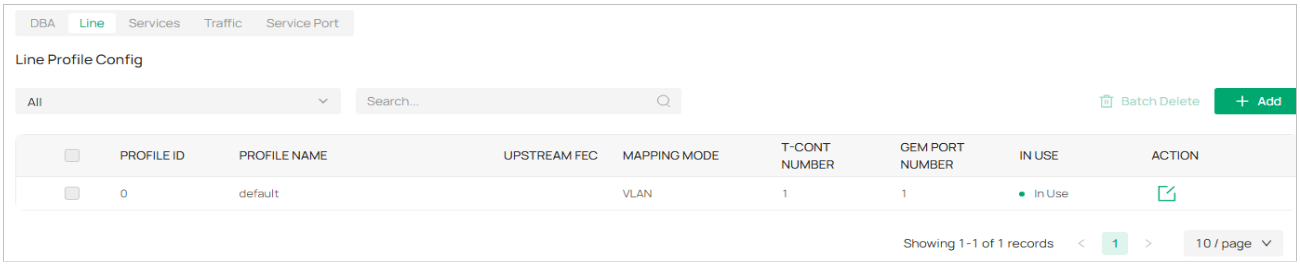
A line profile is used to configure the DBA (Dynamic Bandwidth Allocation), T-CONT (Transmission Container), GEM (GPON Encapsulation Mode) ports, and GEM mapping rules about a GPON ONU line.

GEM ports are the basic transmission units in the GPON network. Different types of traffic from the ONU are mapped to different GEM ports according to the GEM Mapping rules. The T-CONT functions as a tunnel which contains several GEM ports. A DBA profile is applied to the T-CONT to control the bandwidth allocation among different T-CONTs.

When the ONU is registered, a line profile is applied to the ONU to control the GPON ONU line.

When the default line profile cannot meet the service requirements, you can add line profiles according to the service requirements.

1. Go to PON > Profile > Line, and click + Add. In General Config, configure the parameters and click Apply.



Line Profile Config

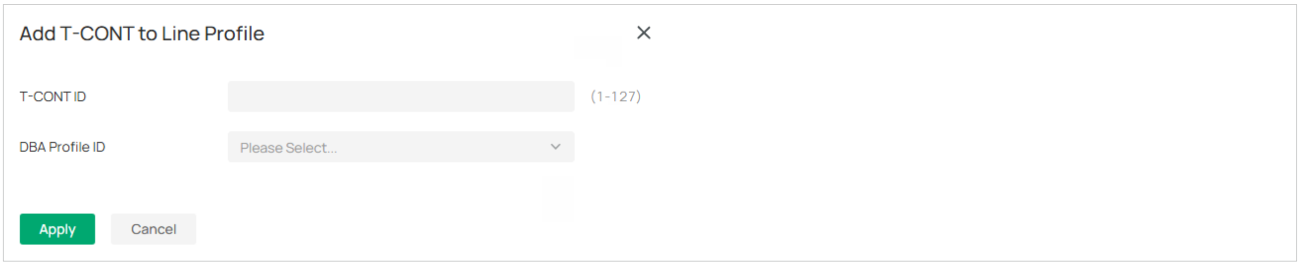
□	PROFILE ID	PROFILE NAME	UPSTREAM FEC	MAPPING MODE	T-CONT NUMBER	GEM PORT NUMBER	IN USE	ACTION
□	0	default		VLAN	1	1	● In Use	

Showing 1-1 of 1 records < 1 > 10 / page

Profile ID	(Optional) Set the profile ID of the Line profile. The profile ID is the unique identifier for the DBA profile. If you leave the profile ID as blank, the system automatically assigns the profile ID.
Profile Name	(Optional) Specify the profile name of the Line profile.
Upstream FEC	Enable or disable the Upstream FEC (Forward Error Correction) function of a GPON ONU line to enhance the data transmission reliability of the upstream link between an OLT and an ONT. After the Upstream FEC function is enabled, the system inserts the redundancy data into the normal packets. In this manner, the line is provided with error tolerance function, but certain bandwidth is wasted. Therefore, enable Upstream FEC when the bandwidth resources are sufficient.
OMCC Encrypt	Enable or disable the encryption function of the ONT management and control channel (OMCC). When the encryption function of the OMCC is enabled, the GEM port of the OMCC is encrypted. When the encryption function of the OMCC is disabled, the GEM port of the OMCC is not encrypted.
Mapping Mode	Select GEM mapping mode of the line profile. The GEM mapping mode determines how to create the mapping between user services and the GEM ports when you configure GEM mapping rules. VLAN: Indicates that user services are mapped to GEM ports based on VLANs. Priority: Indicates that user services are mapped to GEM ports based on priorities. VLAN-Priority: Indicates that user services are mapped to GEM ports based on VLANs and priorities. Port: Indicates that user services are mapped to GEM ports based on ONU ports. Port-VLAN: Indicates that user services are mapped to GEM ports based on ONU ports and VLANs. Port-Priority: Indicates that user services are mapped to GEM ports based on ONU ports and priorities. Port-VLAN-Prioriity: Indicates that user services are mapped to GEM ports based on ONU ports, VLANs, and priorities.

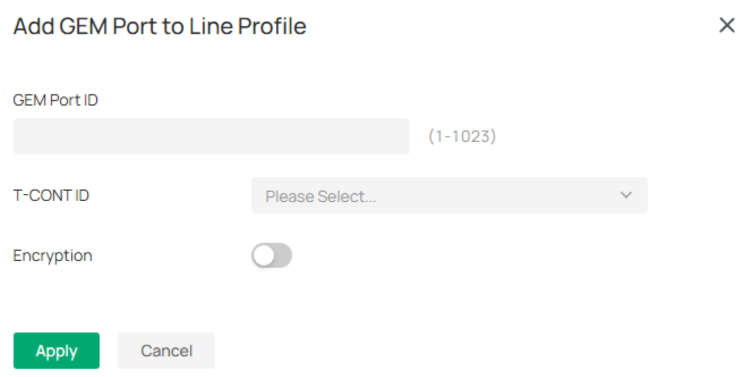
2. Add T-CONTs to the line profile. Go to the T-Conts tab, and click + Add. Configure the parameters

and click Create.



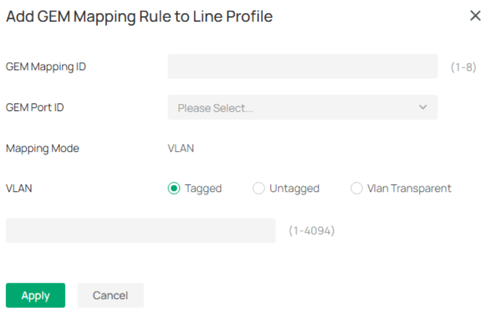
T-CONT ID	Set the T-CONT ID, which is the unique identifier for the T-CONT in this line profile.
DBA Profile ID	Select the DBA profile which is applied to the T-CONT. To create DBA profiles, go to **PON** > **Profile** > **DBA**.

3. Add GEM ports to the line profile. Go to the GEM Ports tab, and click + Add. Configure the parameters and click Create.



GEM Port ID	Set the GEM Port ID, which is the unique identifier for the GEM port in this line profile.
T-CONT ID	Select the T-CONT which the GEM port belongs to. To create T-CONTS, go to the **T-CONT** tab.
Encryption	Enable or disable the encryption function for the GEM port. When the encryption function is enabled, the device encrypts the services on the GEM port to enhance the data security. The encryption does not increase extra overhead nor have impact on the bandwidth usages.

4. Add GEM mapping rules to the line profile. Go to the GEM Mapping Rules tab, and click + Add. Configure the parameters and click Create.



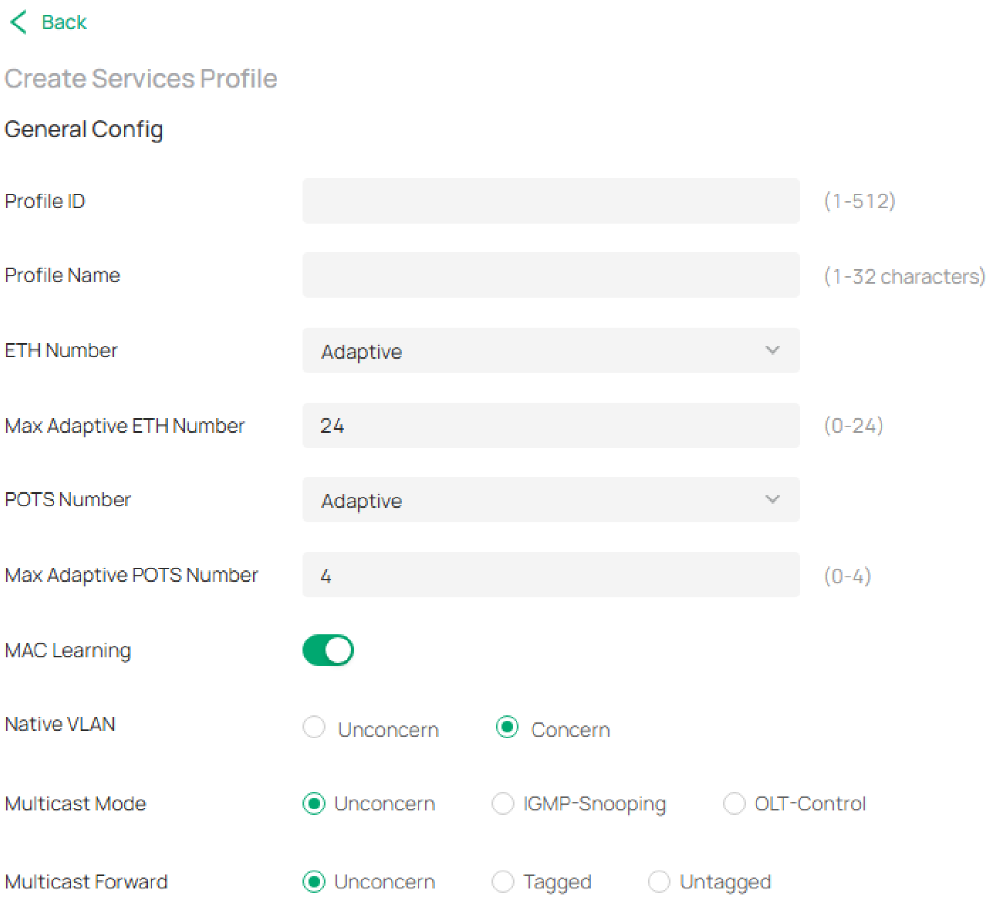
GEM Mapping ID	Set the ID for the GEM mapping rule, which is the unique identifier for the GEM mapping rule in this line profile.
GEM Port ID	Select the GEM port which the specified user service is mapped to according to this GEM mapping rule. To create GEM ports, go to the **GEM Ports** tab.
Mapping Mode	Displays the GEM mapping mode of the line profile. To configure the GEM mapping mode of the line profile, go to the **General Config** section.
VLAN	Specify the VLAN type and ID, ranging from 1-4094.

3. 2. 4 Configure Service Profile

Service profiles determines parameter settings for services on an ONU managed by an OLT via OMCI (ONU Management and Control Interface), including ONU port numbers of different types, multicast settings, port settings for transmitting user services, and so on.

When the default service profile cannot meet the service requirements, you can add service profiles according to the service requirements.

1. Go to PON > Profile > Services, and click + Add. In General Config, configure the parameters and click Apply.



< Back

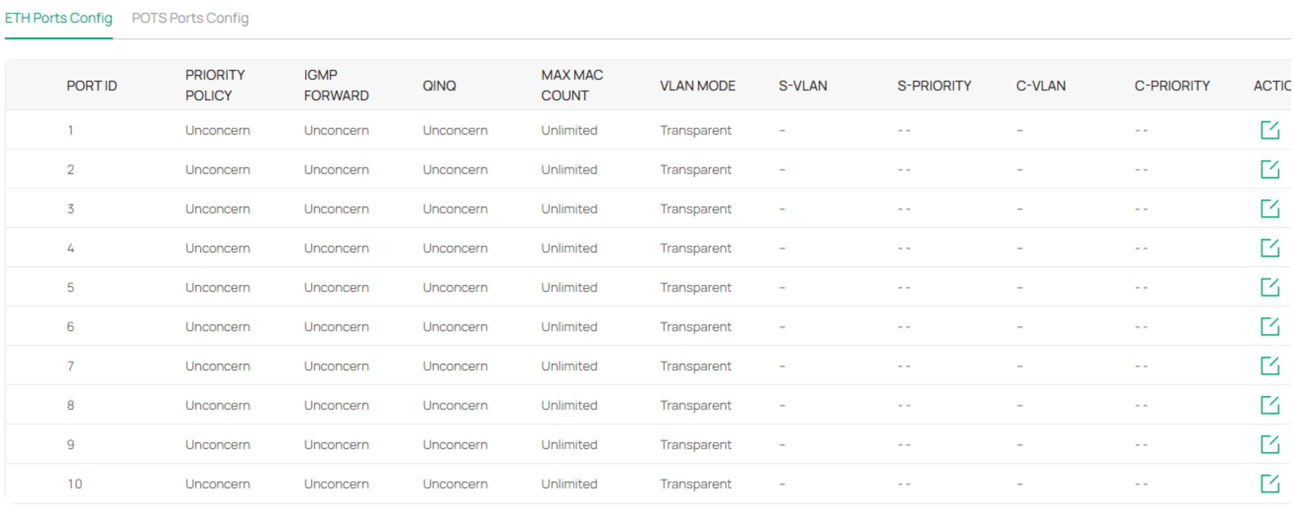
Create Services Profile

General Config

Profile ID		(1-512)
Profile Name		(1-32 characters)
ETH Number	Adaptive	
Max Adaptive ETH Number	24	(0-24)
POTS Number	Adaptive	
Max Adaptive POTS Number	4	(0-4)
MAC Learning	On	
Native VLAN	○ Unconcern ● Concern	
Multicast Mode	● Unconcern ○ IGMP-Snooping ○ OLT-Control	
Multicast Forward	● Unconcern ○ Tagged ○ Untagged	

Profile ID	(Optional) Set the profile ID of the Service profile. The profile ID is the unique identifier for the service profile. If you leave the profile ID as blank, the system automatically assigns the profile ID.
Profile Name	(Optional) Specify the profile name of the service profile.
ETH Number	Select the number of ONU ETH ports. If you select **Adaptive**, the OLT automatically detects the number of available ONU ETH ports
Max Adaptive ETH Number	Specify the maximum number of ONU ETH ports which can be detected by the OLT.
POTS Number	Select the number of ONU POTS ports. If you select **Adaptive**, the OLT automatically detects the number of available ONU POTS ports
MAX Adaptive POTS Number	Specify the maximum number of ONU POTS ports which can be detected by the OLT.
MAC Learning	Enable or disable the ONU MAC learning function.
Native VLAN	Select whether the ONU concerns the native VLAN when the ONU receives untagged traffic from the user.
Multicast Mode	Set the multicast mode of the ONU in the GPON service profile. In different multicast modes, the multicast program streams are processed in different ways and the multicast users are authenticated in different ways. Unconcern: The ONU does not support the multicast mode or the OLT does not specify the ONU multicast mode. IGMP Snooping Mode: The ONU is required to maintain multicast forwarding tables. OLT-Control Mode: The OLT is required to maintain ONT multicast forwarding tables.
Multicast Forward	Configure the multicast forwarding mode of the ONU in a GPON service profile. In different multicast forwarding modes, the downstream multicast packets from the ONU to the Ethernet port are different. Unconcern: The ONU does not support setting the multicast forwarding mode or the OLT does not specify the ONU multicast forwarding mode. Untagged: Select the Untagged mode if the ONU is directly connected to the STB (set-top box) or PC. Tagged: Select the Tagged mode If the ONU is directly connected to the home gateway.

2. In the ETH Ports Config tab, select the desired ETH ports of the ONU and click ✎ to configure the parameters of the ports. Then click Save.



PORT ID	PRIORITY POLICY	IGMP FORWARD	QINQ	MAX MAC COUNT	VLAN MODE	S-VLAN	S-PRIORITY	C-VLAN	C-PRIORITY	ACTIC
1	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
2	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
3	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
4	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
5	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
6	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
7	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
8	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
9	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎
10	Unconcern	Unconcern	Unconcern	Unlimited	Transparent	-	- -	-	- -	✎

QinQ

Set the QinQ attribute of an ONU port in the GPON service profile.

Unconcern: The OLT does not specify the QinQ attribute of an ONU port, and the QinQ attribute of the ONU port is determined based on the ONU condition.

Enable: When the packet needs to be identified on the OLT side, enable the QinQ attribute of the port.

Disable: When the packet does not need to be identified on the OLT side, disable the QinQ attribute of the port.

TLS VLAN

Set the TLS (Transparent LAN Service) VLAN. Untagged traffic and non TLS VLAN traffic are tagged with the native VLAN ID of the ONU port and then forwarded, while the TLS VLAN traffic is forwarded directly.

TLS VLAN is only available when the QinQ attribute of the ONU port is enabled.

Priority Policy

Set the upstream priority source on the ONU port in the GPON service profile.

Unconcern: The OLT does not specify the upstream priority source on the ONU port, and the upstream priority source on the ONU port is determined based on the ONU condition.

Assigned: The OLT Assigns the priority of traffic. The outer layer priority of the non TLS VLAN traffic is the same as native VLAN priority.

Copy-CoS: The priority of traffic is copied from C-TAG in the user packet. You do not need to set the packet priority through the OLT.

Priority Policy is only available when the QinQ attribute of the ONU port is enabled.

VLAN Config

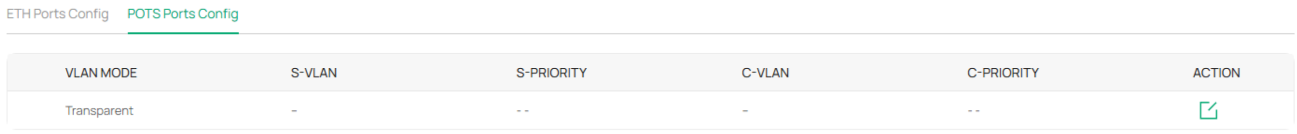
Configure the VLAN settings for the ONU port.

Transparent: The ONU port keeps the VLAN tag of the traffic unchanged.

Non-Transparent: The ONU port deals with the VLAN tag of the traffic in the specified mode, including Translation, QinQ, and Trunk. Click +Add to add VLAN entries of the port and specify the VLAN Mode, S-VLAN, S-Priority, C-VLAN, C-Priority of each entry.

VLAN Mode	Translation: The VLAN tag of the packet is switched based on the settings of this entry. The upstream and downstream packets are not differentiated. When a packet is sent upstream, the C-VLAN (User-Side VLAN) and C-Priority (User-Side Priority) is switched to the S-VLAN (Service VLAN) and S-Priority (Service Priority). QinQ: A VLAN packet with the QinQ attribute contains an inner VLAN tag from the private network of the user and an outer VLAN tag allocated by the device. The two layers of VLAN tags form an L2 VPN channel between private networks for transparently transmitting services between the private networks. When a packet is sent upstream, the packet with C-VLAN and C-Priority is added an outer VLAN tag with the S-VLAN and S-Priority. Trunk: The ONU port only transfers packets with the specified S-VLAN and S-Priority and drop other packets. In the Trunk mode, the S-VLAN is required and S-Priority is optional.
IGMP Forward	Configure the IGMP Forward mode for the ONU port. Unconcern: The OLT does not specify the IGMP Foward mode on the ONU port, and the IGMP Foward mode on the ONU port is determined based on the ONU condition. Translation: In network application, the VLAN tags carried by user-side packets are different and the VLANs need to be planned on the optical line terminal (OLT). In translation mode, the ONU switches the VLAN tags of user-side packets to new VLAN tags and then forwards the packets to the OLT. If the VLAN tags carried by user-side packets have been planned, the ONU does not need to translate the VLAN tags of IGMP packets by translation parameter again. In the Translation mode, the VLAN is required and the priority is optional. Default: The ONU adds a new VLAN tag to the user-side packets and then forwards the packets upstream to the OLT. In the Default mode, the VLAN is required and the priority is optional. Transparent: The ONU does not process VLAN tags of all user-side packets including broadcast packets and multicast packets but only forwards these packets upstream to the other side.
Max MAC Count	Set the maximum number of MAC addresses that can be learned by the ONU port in the GPON service profile. By default, the maximum number of MAC addresses that can be learned by the ONU is not limited.

3. In the POTS Ports Config tab, select the desired POTS ports of the ONU and click ✎ to configure the parameters of the ports. Then click Save.



VLAN MODE	S-VLAN	S-PRIORITY	C-VLAN	C-PRIORITY	ACTION
Transparent	-	--	-	--	✎

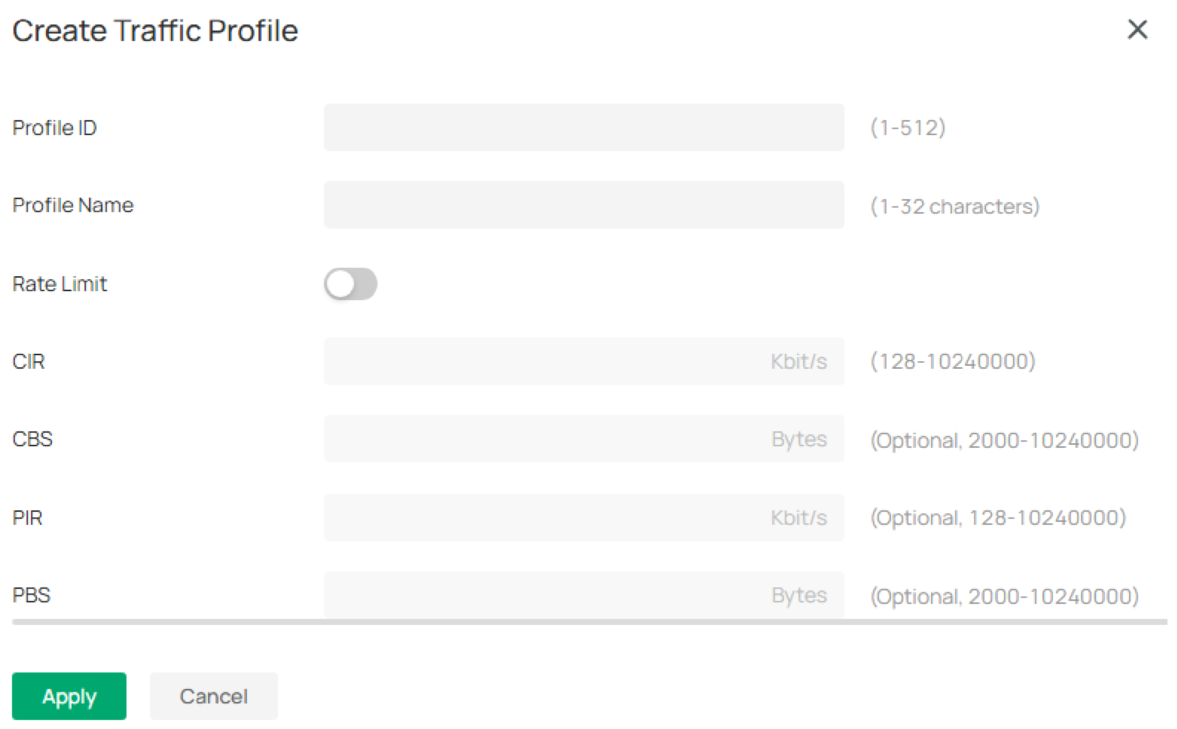
VLAN Config	Configure the VLAN settings for the ONU port. Transparent: The ONU port keeps the VLAN tag of the traffic unchanged. Non-Transparent: The ONU port deals with the VLAN tag of the traffic in the specified mode, including Translation, QinQ, and Trunk. Click +Add to add VLAN entries of the port and specify the VLAN Mode, S-VLAN, S-Priority, C-VLAN, C-Priority of each entry.

VLAN Mode	Translation: The VLAN tag of the packet is switched based on the settings of this entry. The upstream and downstream packets are not differentiated. When a packet is sent upstream, the C-VLAN (User-Side VLAN) and C-Priority (User-Side Priority) is switched to the S-VLAN (Service VLAN) and S-Priority (Service Priority). QinQ: A VLAN packet with the QinQ attribute contains an inner VLAN tag from the private network of the user and an outer VLAN tag allocated by the device. The two layers of VLAN tags form an L2 VPN channel between private networks for transparently transmitting services between the private networks. When a packet is sent upstream, the packet with C-VLAN and C-Priority is added an outer VLAN tag with the S-VLAN and S-Priority. Trunk: The ONU port only transfers packets with the specified S-VLAN and S-Priority and drop other packets. In the Trunk mode, the S-VLAN is required and S-Priority is optional.

3. 2. 5 Configure Traffic Profile

In Traffic profile, you can set up desired rate limit and VLAN priority for any traffic which uses this profile, such as the inbound and outbound traffic of service ports.

Go to PON > Profile > Traffic, and click + Add. Configure the parameters and click Create.



Create Traffic Profile

Profile ID		(1-512)
Profile Name		(1-32 characters)
Rate Limit	○	
CIR	Kbit/s	(128-10240000)
CBS	Bytes	(Optional, 2000-10240000)
PIR	Kbit/s	(Optional, 128-10240000)
PBS	Bytes	(Optional, 2000-10240000)

Profile ID	Set the profile ID of the traffic profile. The profile ID is the unique identifier for the traffic profile. If you leave the profile ID as blank, the system automatically assigns the profile ID.
Profile Name	Specify the profile name of the traffic profile.
Rate Limit	Enable or disable the rate limit function. If the rate limit function is enabled, you can set the parameters of CIR, CBS, PIR, and PBS.

CIR	Set the CIR (Committed Information Rate). In general, the CIR is greater than the actual traffic rate. The CIR must be a multiple of 64. If the entered value is not a multiple of 64, round it down to a nearest integer.
CBS	(Optional) Set the CBS (Committed Burst Size). It is the traffic allowed for service flows or ports when a traffic burst occurs. If this parameter is not specified, the CBS is determined by min(2000+CIR*32, 1024000000).
PIR	(Optional) Set the PIR (Peak Information Rate). If the parameter is not specified, it can be obtained by the formula max (min(CIR*2, 10240000) ,64). The PIR cannot be smaller than CIR.
PBS	(Optional) Set the PBS (Peak Burst Size), which specifies the maximum burst traffic allowed to pass. If you leave this parameter not specified, the system calculates the burst size using the formula of min (2000+32*PIR, 1024000000).
Priority	Set the priority mode for the traffic. Assigned: Assign the 802.1p priority to the S-VLAN packets. The larger value indicates higher priority. You need to set the priority value. user-cos: Copy the 802.1p priority value of the outer layer of the packets. You need to set the priority value. If the traffic is untagged, the priority value is used.
Inner-Priority	Set the inner priority mode for the traffic. None: Do not assign the 802.1p priority. Assigned: Assign the 802.1p priority to the inner layer of the packets. The larger value indicates higher priority. You need to set the priority value. user-cos: Copy the 802.1p priority value of the outer layer of the packets. You need to set the priority value. If the traffic is untagged, the priority value is used.
Priority-Policy	Set the priority scheduling policy of the packet queue. Local-Setting: When congestion occurs, packets are scheduled by the 802.1p priority specified in the traffic profile. If the priority tag policy is to specify the priority, that is, when prival is set, you are recommended to use this scheduling policy. Tag-In-Package: When congestion occurs, the system schedules packets based on the priority in outbound packets. This policy applies to both upstream and downstream packets. If the priority tag policy is user-cos, use the Tag-In-Package scheduling policy. Tag-In-Ingress-Package: When congestion occurs, the system schedules downstream packets by the priority contained in ingress packets.

3. 2. 6 Register ONU

Overview

After connecting the ONU to the GPON network, the ONU is auto-found by the OLT. Then you need to authenticate and register the ONU. You can also set auto authentication for ONUs. After the ONU is registered, the ONU goes online and is able to communicate with the OLT via the GPON network.

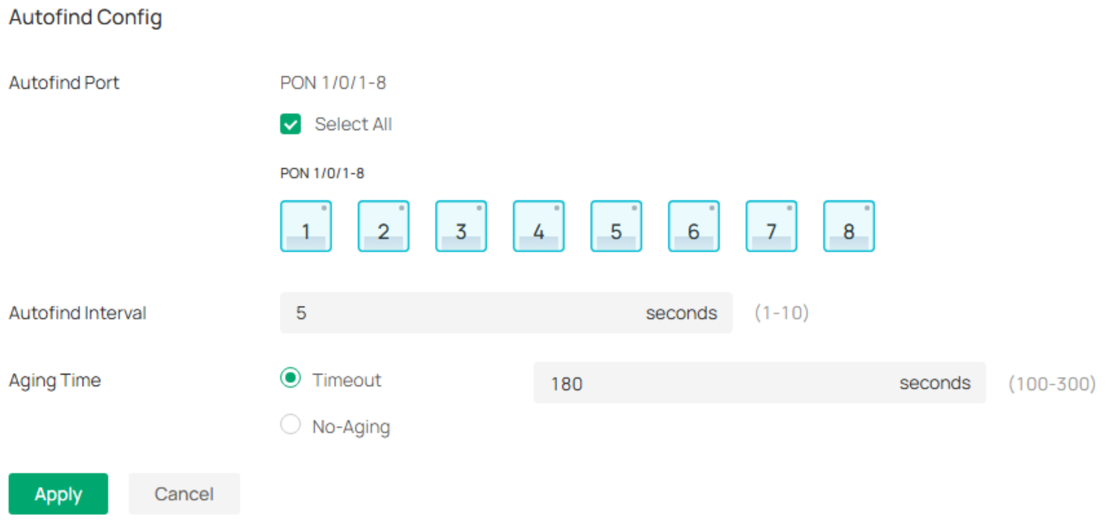
You have the following three methods to authenticate and register ONUs:

- Authenticate and register the ONU manaully after the ONU is found by the OLT
- Authenticate and register the ONU beforehand
- Auto-Authenticate and register the ONUs in batches beforehand

Configuration

Authenticate and register the ONU manaully after the ONU is found by the OLT

1. Go to PON > ONU Register > Autofind. In the Autofind Config section, configure the parameters, and click Apply.



Autofind Config

Autofind Port: PON 1/0/1-8

☑ Select All

PON 1/0/1-8

1 2 3 4 5 6 7 8

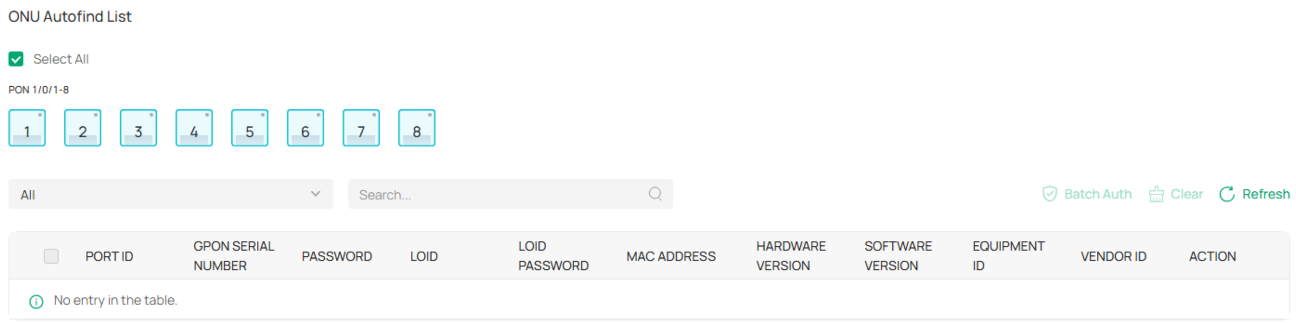
Autofind Interval: 5 seconds (1-10)

Aging Time: ● Timeout 180 seconds (100-300)

○ No-Aging

Autofind Port	Select the desired ports to enable the Autofind feature.
Autofind Interval	Set the interval between each time the OLT automatically finds the ONU.
Aging Time	Set the aging time of the ONU which is automatically found by the OLT. If the ONU is not registered within the aging time, the ONU is removed from the memory of the OLT. If you select No-Aging, aging time is not specified.

2. In the ONU Autofind List section, select the ports to display the ONUs which are connected to the specified ports and automatically found by the OLT. You can click ✓ to authenticate and register the ONU. The ONU can work normally only after you register the ONU. You can click 🧹 to remove the ONU from the list.



ONU Autofind List

☑ Select All

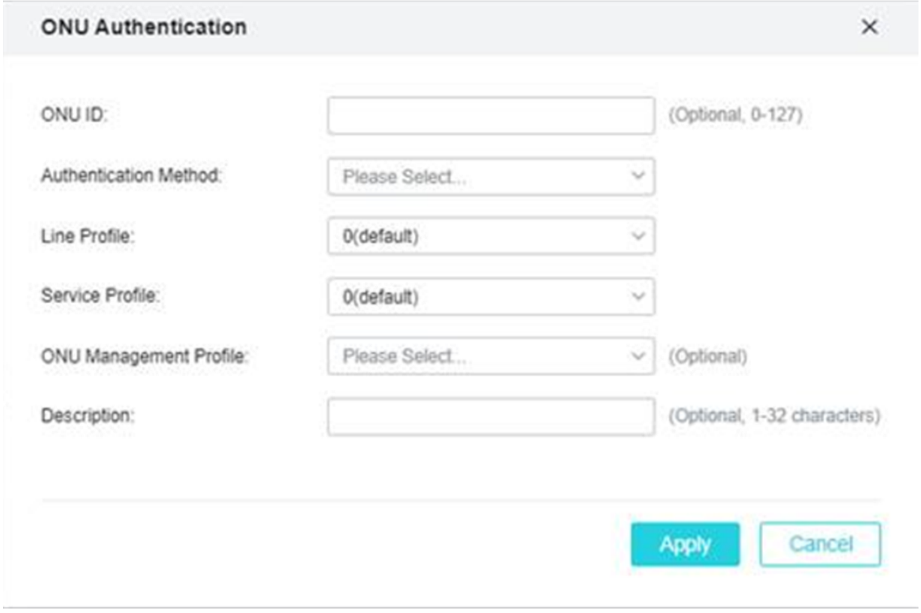
PON 1/0/1-8

1 2 3 4 5 6 7 8

□	PORT ID	GPON SERIAL NUMBER	PASSWORD	LOID	LOID PASSWORD	MAC ADDRESS	HARDWARE VERSION	SOFTWARE VERSION	EQUIPMENT ID	VENDOR ID	ACTION

No entry in the table.

3. Select the desired ONU on the list and click ✓ to authenticate and register the ONU.



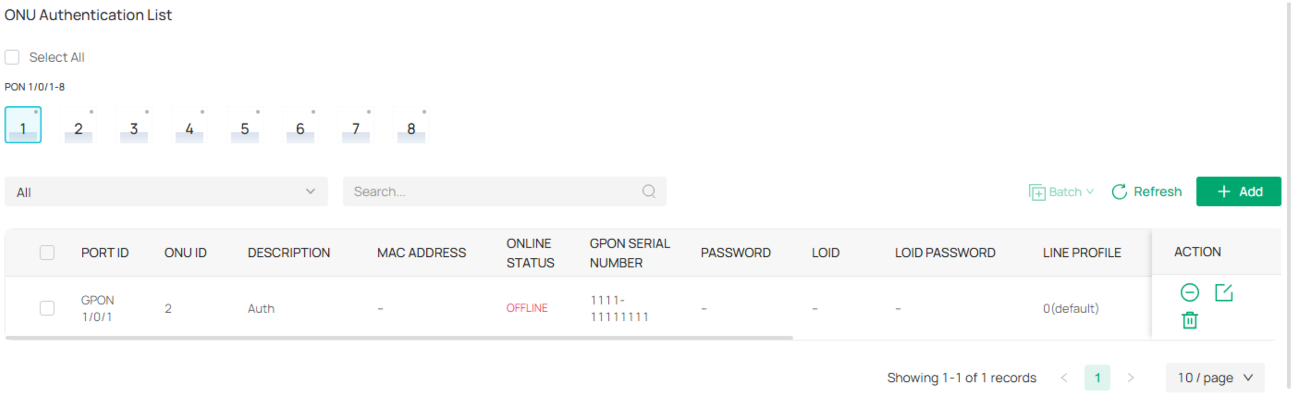
ONU Authentication ×

ONU ID:		(Optional, 0-127)
Authentication Method:	Please Select...	
Line Profile:	0(default)	
Service Profile:	0(default)	
ONU Management Profile:	Please Select...	(Optional)
Description:		(Optional, 1-32 characters)

ONU ID	(Optional) Set the ONU ID. The ONU ID is the unique identifier for the ONU. If you leave the ONU ID as blank, the system automatically assigns the ONU ID.
Authentication Method	Select the method to authenticate the ONU. Password-Auth: The ONU is authenticated using the password. When the ONU goes online again, the ONU can be re-authenticated using the password. The authentication passwords of the ONUs connected to the same port must be unique. SN-Auth: The ONU is authenticated using the SN (Serial Number). When the ONU goes online again, the ONU can be re-authenticated using the SN. LOID-Auth: The ONU is authenticated using the LOID (Logical ONU ID). When the ONU goes online again, the ONU can be re-authenticated using the LOID. SN-and-Password-Auth: The ONU is authenticated using the SN and password. When the ONU goes online again, the ONU can be re-authenticated using the SN and password. LOID-and-Password-Auth: The ONU is authenticated using the LOID and password. When the ONU goes online again, the ONU can be re-authenticated using the LOID and password.
Discovery Mode	Select the mode to discover the ONU when the ONU goes online again. Always-On: When the ONU goes online again, the OLT does not check the SN of the ONU. The ONU can still go online even though the ONU SN is changed. Once-On: The ONU is required to start authentication within the specified time, and cannot go online if the specified time period expires. The SN of the ONU cannot be modified once the ONU passes the authentication. Discovery Mode is only available for the Authentication Method of Password-Auth, LOID-Auth, and LOID-and-Password-Auth.

Re-Register-Auth-Mode	Select the mode to re-authenticate the ONU when the ONU goes online again. SN: The ONU is re-authenticated using the SN. SN-Password: The ONU is re-authenticated using the SN and password. Re-Register-Auth-Mode is only available when the Authentication Method is Password-Auth and Discovery Mode is Once-On.
Line Profile	Select the line profile used by the ONU. To create line profiles, go to **PON** > **Profile** > **Line**.
Service Profile	Select the service profile used by the ONU. To create service profiles, go to **PON** > **Profile** > **Services**.
ONU Management Profile	Select the management profile used by the ONU. To create management profiles, go to **PON** > **Profile** > **ONU Management**.
Description	(Optional) Enter the description of the ONU.

4. Go to PON > ONU Register > Authentication Config. Select the PON ports which the ONUs are connected. The ONUs which are authenticated and registered appears in the ONU Authentication List. You can click ⊖ to deactivate the ONU. You can click ⚡ to activate the ONU. You can click ✎ to edit the settings of ONU Authentication. You can click 🗑 to delete the ONU.



ONU Authentication List

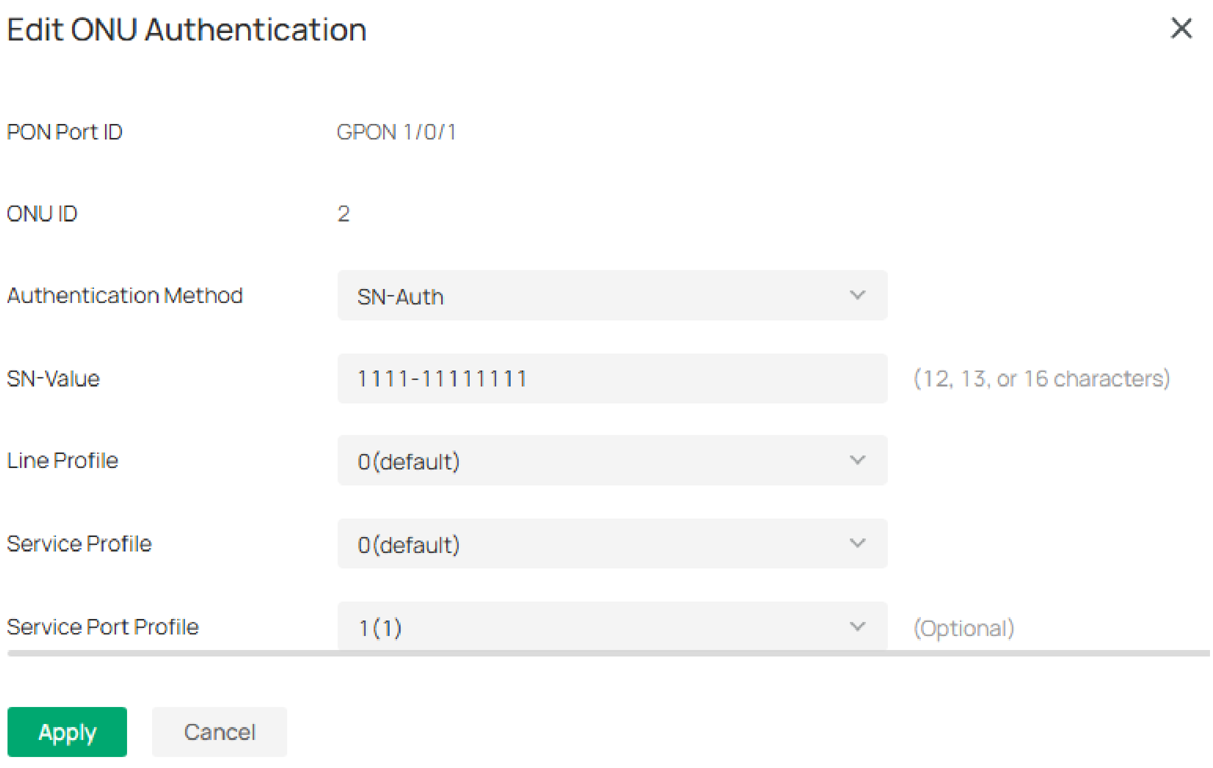
□ Select All

PON 1/0/1-8

□	PORT ID	ONU ID	DESCRIPTION	MAC ADDRESS	ONLINE STATUS	GPON SERIAL NUMBER	PASSWORD	LOID	LOID PASSWORD	LINE PROFILE	ACTION
□	GPON 1/0/1	2	Auth	-	OFFLINE	1111-11111111	-	-	-	0(default)	⊖ ✎ 🗑

Showing 1-1 of 1 records < 1 > 10 / page

5. In the ONU Authentication List, select the ONU and click ✎ to edit the settings of ONU Authentication.


Edit ONU Authentication

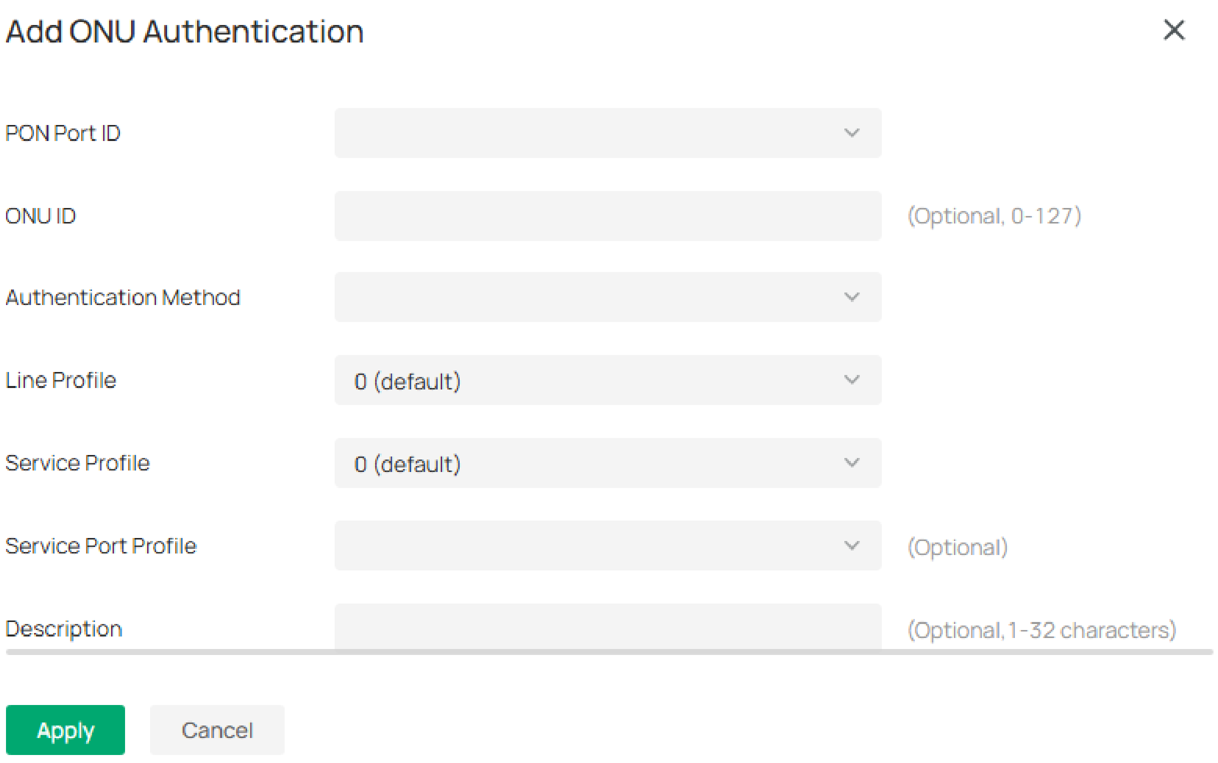
PON Port ID	GPON 1/0/1
ONU ID	2
Authentication Method	SN-Auth
SN-Value	1111-11111111 (12, 13, or 16 characters)
Line Profile	0(default)
Service Profile	0(default)
Service Port Profile	1(1) (Optional)

PON Port ID	Displays the PON port which the ONU is connected to.
ONU ID	Displays the ONU ID. The ONU ID is the unique identifier for the ONU.
Authentication Method	Select the method to authenticate the ONU. Password-Auth: The ONU is authenticated using the password. When the ONU goes online again, the ONU can be re-authenticated using the password. The authentication passwords of the ONUs connected to the same port must be unique. SN-Auth: The ONU is authenticated using the SN (Serial Number). When the ONU goes online again, the ONU can be re-authenticated using the SN. LOID-Auth: The ONU is authenticated using the LOID (Logical ONU ID). When the ONU goes online again, the ONU can be re-authenticated using the LOID. SN-and-Password-Auth: The ONU is authenticated using the SN and password. When the ONU goes online again, the ONU can be re-authenticated using the SN and password. LOID-and-Password-Auth: The ONU is authenticated using the LOID and password. When the ONU goes online again, the ONU can be re-authenticated using the LOID and password.
Password	Set the password of the ONU. You can set the format of the password as ASCII or HEX. Password is only available for the Authentication Method of Password Auth and SN-and-Password-Auth.
SN-Value	Set the SN of the ONU which is used for authentication. SN value is only available for the Authentication Method of SN-Auth and SN-and-Password-Auth.

LOID	Set the LOID of the ONU which is used for authentication. LOID is only available for the Authentication Method of LOID-Auth and LOID-and-Password-Auth.
LOID Password	Set the LOID password of the ONU which is used for authentication. LOID Password is only available for the Authentication Method of LOID-and-Password-Auth.
Discovery Mode	Select the mode to discover the ONU when the ONU goes online again. Always-On: When the ONU goes online again, the OLT does not check the SN of the ONU. The ONU can still go online even though the ONU SN is changed. Once-On: The ONU is required to start authentication within the specified time, and cannot go online if the specified time period expires. The SN of the ONU cannot be modified once the ONU passes the authentication. Discovery Mode is only available for the Authentication Method of Password-Auth, LOID-Auth, and LOID-and-Password-Auth.
Re-Register-Auth-Mode	Select the mode to re-authenticate the ONU when the ONU goes online again. SN: The ONU is re-authenticated using the SN. SN-Password: The ONU is re-authenticated using the SN and password. Re-Register-Auth-Mode is only available when the Authentication Method is Password-Auth and Discovery Mode is Once-On.
Line Profile	Select the line profile used by the ONU. To create line profiles, go to **PON** > **Profile** > **Line**.
Service Profile	Select the service profile used by the ONU. To create service profiles, go to **PON** > **Profile** > **Services**.
ONU Management Profile	Select the management profile used by the ONU. To create management profiles, go to **PON** > **Profile** > **ONU Management**.
Description	(Optional) Enter the description of the ONU.

- **Authenticate and register the ONU beforehand**

Go to PON > ONU Register > Authentication Config. Select the PON ports which the ONUs are connected. Click + Add Auth to add an authentication entry to authenticate and register the ONU beforehand. Configure the parameters and click Create. After the ONU is found by the OLT, the ONU is automatically authenticated and registered according to the settings of the authentication entry.



Add ONU Authentication

PON Port ID

ONU ID (Optional, 0-127)

Authentication Method

Line Profile 0 (default)

Service Profile 0 (default)

Service Port Profile (Optional)

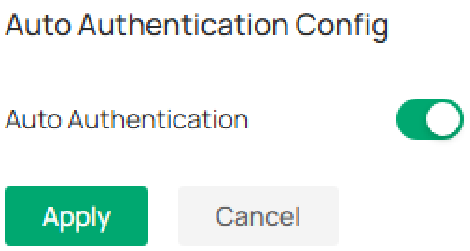
Description (Optional, 1-32 characters)

PON Port ID	Select the PON port which the ONU is connected to.
ONU ID	(Optional) Set the ONU ID. The ONU ID is the unique identifier for the ONU. If you leave the ONU ID as blank, the system automatically assigns the ONU ID.
Authentication Method	Select the method to authenticate the ONU. Password-Auth: The ONU is authenticated using the password. When the ONU goes online again, the ONU can be re-authenticated using the password. The authentication passwords of the ONUs connected to the same port must be unique. SN-Auth: The ONU is authenticated using the SN (Serial Number). When the ONU goes online again, the ONU can be re-authenticated using the SN. LOID-Auth: The ONU is authenticated using the LOID (Logical ONU ID). When the ONU goes online again, the ONU can be re-authenticated using the LOID. SN-and-Password-Auth: The ONU is authenticated using the SN and password. When the ONU goes online again, the ONU can be re-authenticated using the SN and password. LOID-and-Password-Auth: The ONU is authenticated using the LOID and password. When the ONU goes online again, the ONU can be re-authenticated using the LOID and password.
Line Profile	Select the line profile used by the ONU. To create line profiles, go to **PON** > **Profile** > **Line**.
Service Profile	Select the service profile used by the ONU. To create service profiles, go to **PON** > **Profile** > **Services**.

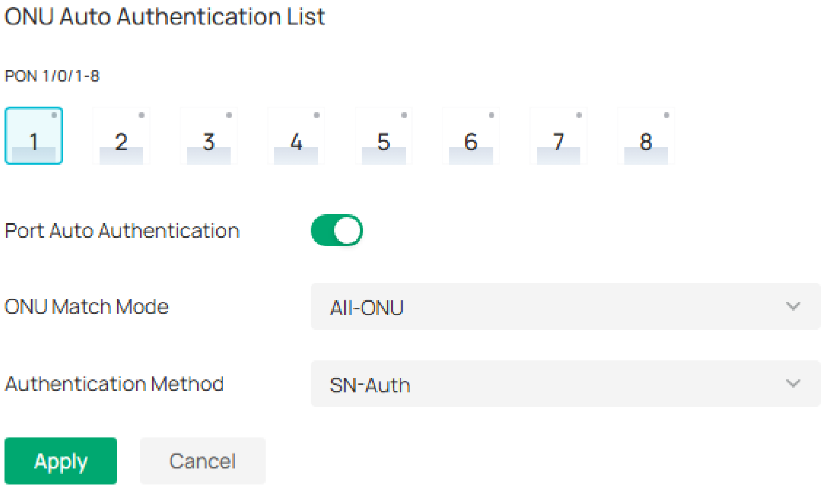
Service Port Profile	Select the service port profile used by the ONU. To create service port profiles, go to **PON** > **Profile** > **Service Port**.
Description	(Optional) Enter the description of the ONU.

- **Auto-Authenticate and register the ONUs in batches beforehand**

1. Go to PON > ONU Register > Auto Authentication. In the Auto Authentication Config section, enable Auto Authentication globally and click Apply.



2. In the ONU Auto Authentication List, Select the port which the ONUs are connected to, enable Port Auto Authentication and configure the parameters. Click Apply.



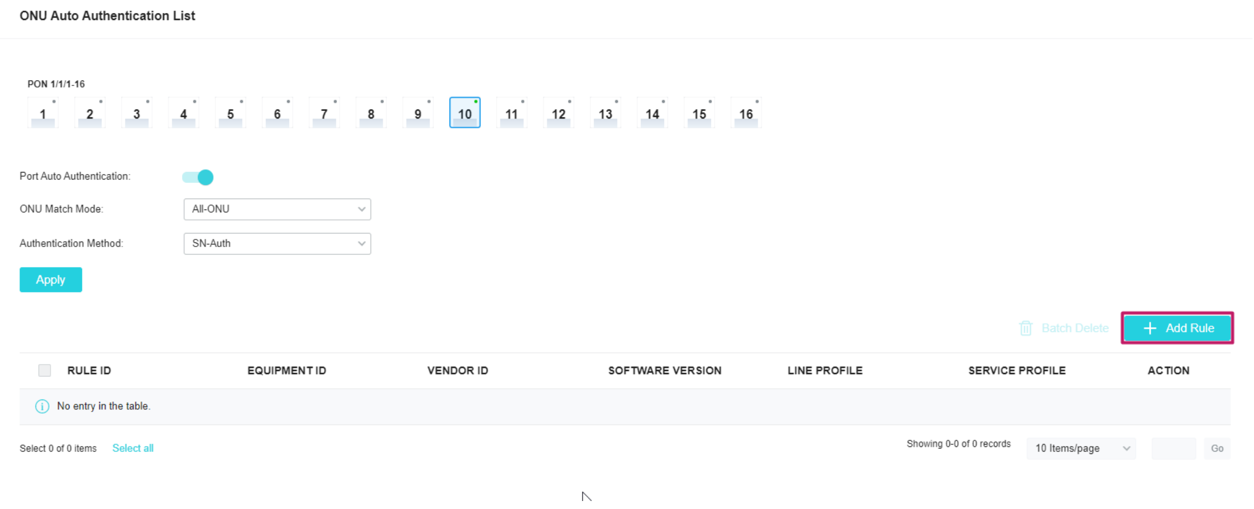
ONU Match Mode: All-ONU

Authentication Method: SN-Auth

Port Auto Authentication	Enable or disable Auto Authentication on the port.
ONU Match Mode	Select the mode to match the ONUs in auto authentication. Equid-Auth: The ONUs with the specified equipment ID are matched in auto authentication. Equid-Swver-Auth: The ONUs with the specified equipment ID and software version are matched in auto authentication. Vendor-Auth: The ONUs with the specified vendor ID are matched in auto authentication. All-ONU: All the ONUs are matched in auto authentication.

Authentication Method	Select the method to authenticate the ONU. Password-Auth: The ONU is authenticated using the password. When the ONU goes online again, the ONU can be re-authenticated using the password. The authentication passwords of the ONUs connected to the same port must be unique. SN-Auth: The ONU is authenticated using the SN (Serial Number). When the ONU goes online again, the ONU can be re-authenticated using the SN. LOID-Auth: The ONU is authenticated using the LOID (Logical ONU ID). When the ONU goes online again, the ONU can be re-authenticated using the LOID. SN-and-Password-Auth: The ONU is authenticated using the SN and password. When the ONU goes online again, the ONU can be re-authenticated using the SN and password. LOID-and-Password-Auth: The ONU is authenticated using the LOID and password. When the ONU goes online again, the ONU can be re-authenticated using the LOID and password.

3. Select the port which the ONUs are connected to, click +Add to add ONU Auto Authentication rules according to the ONU match mode you selected. Configure the parameters and click Create.



ONU Auto Authentication List

PON 1/1/1-16

Port Auto Authentication: on

ONU Match Mode: All-ONU

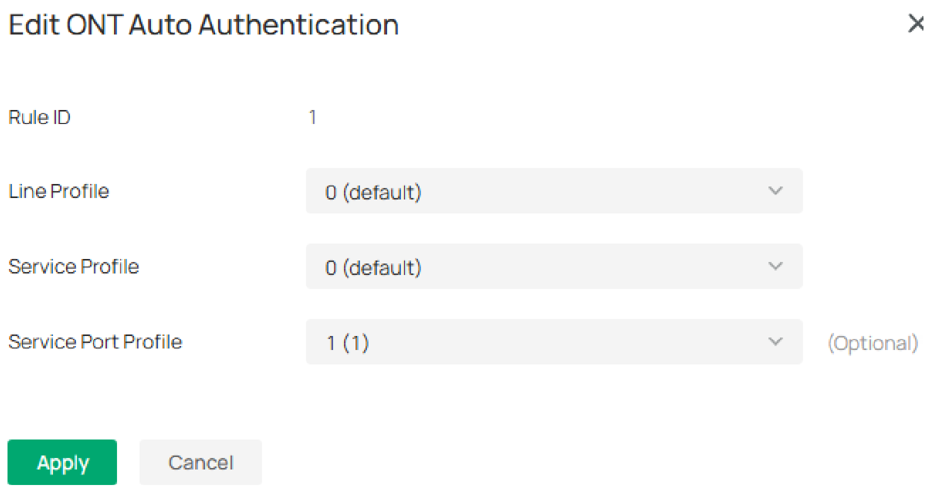
Authentication Method: SN-Auth

□ RULE ID	EQUIPMENT ID	VENDOR ID	SOFTWARE VERSION	LINE PROFILE	SERVICE PROFILE	ACTION
No entry in the table.						

Select 0 of 0 items Select all

Showing 0-0 of 0 records 10 Items/page

4. In the ONU Auto Authentication List, select the ONU and click ☑ to edit the settings of ONU Auto Authentication.



Edit ONT Auto Authentication

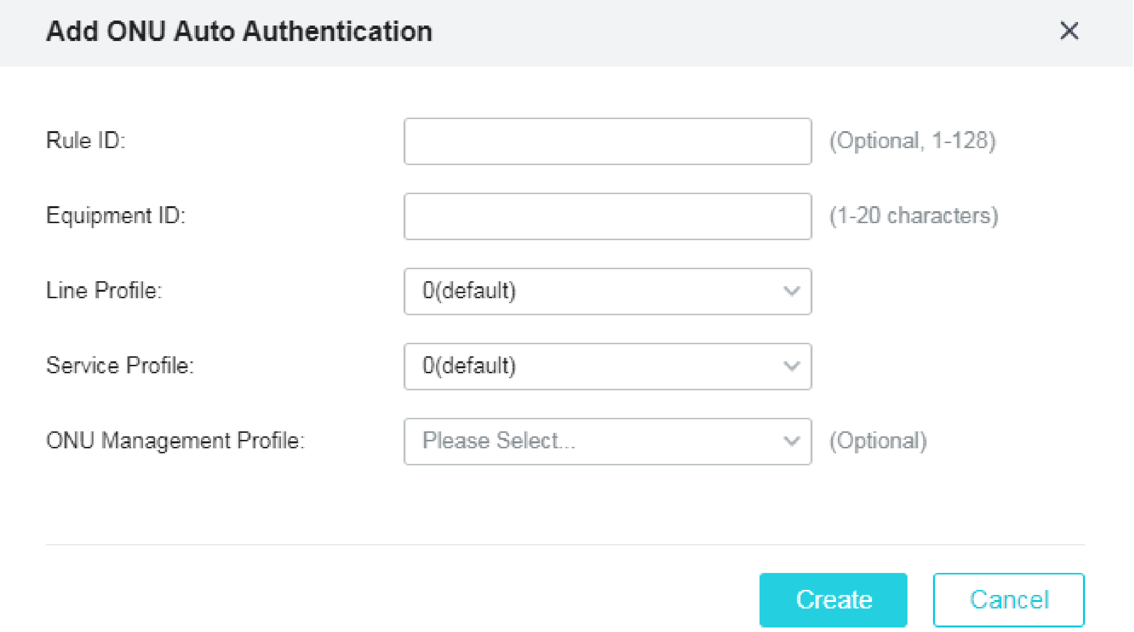
Rule ID 1

Line Profile 0 (default)

Service Profile 0 (default)

Service Port Profile 1 (1) (Optional)

- **For Equid-Auth**

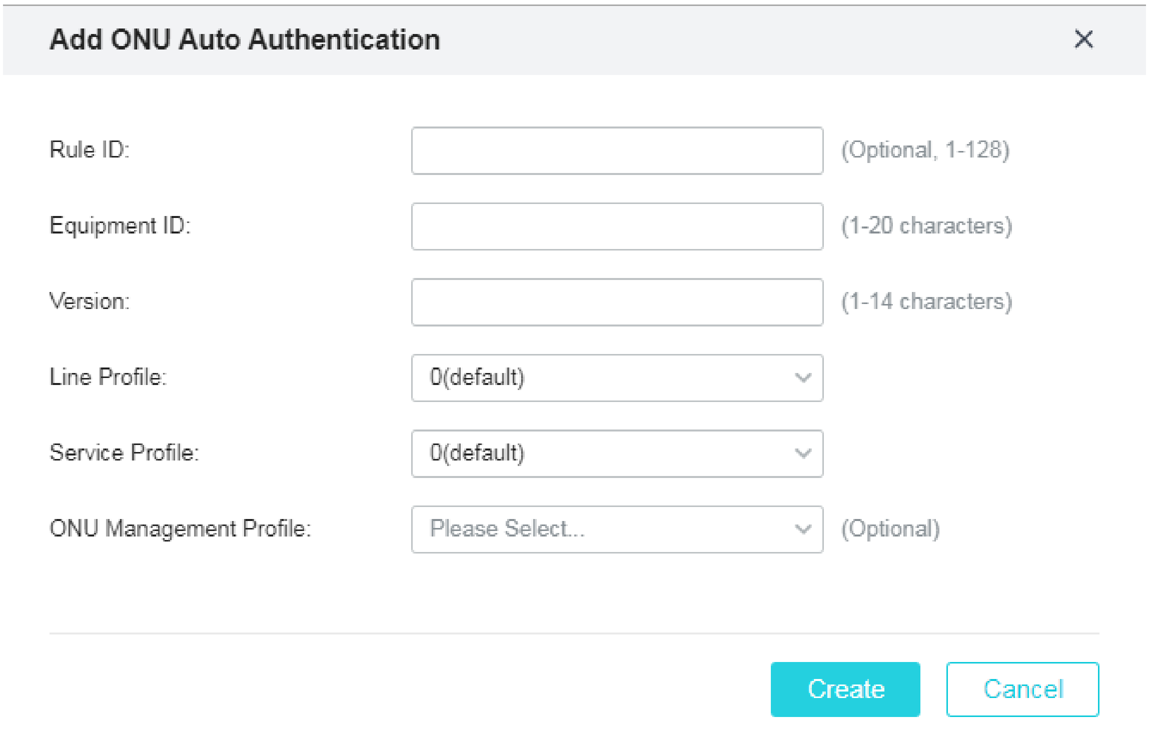


Add ONU Auto Authentication

Rule ID:		(Optional, 1-128)
Equipment ID:		(1-20 characters)
Line Profile:	0(default)	
Service Profile:	0(default)	
ONU Management Profile:	Please Select...	(Optional)

Rule ID	(Optional) Set the Rule ID. The Rule ID is the unique identifier for the ONU Auto authentication rule. If you leave the Rule ID as blank, the system automatically assigns the Rule ID.
Equiment ID	Specify the Equiment ID. The ONUs with the equipment ID are auto-authenticated.
Line Profile	Select the line profile used by the ONUs. To create line profiles, go to **PON** > **Profile** > **Line**.
Service Profile	Select the service profile used by the ONUs. To create service profiles, go to **PON** > **Profile** > **Services**.
ONU Management Profile	Select the management profile used by the ONU. To create management profiles, go to **PON** > **Profile** > **ONU Management**.

- **For Equid-Swver-Auth**



Add ONU Auto Authentication

Rule ID: (Optional, 1-128)

Equipment ID: (1-20 characters)

Version: (1-14 characters)

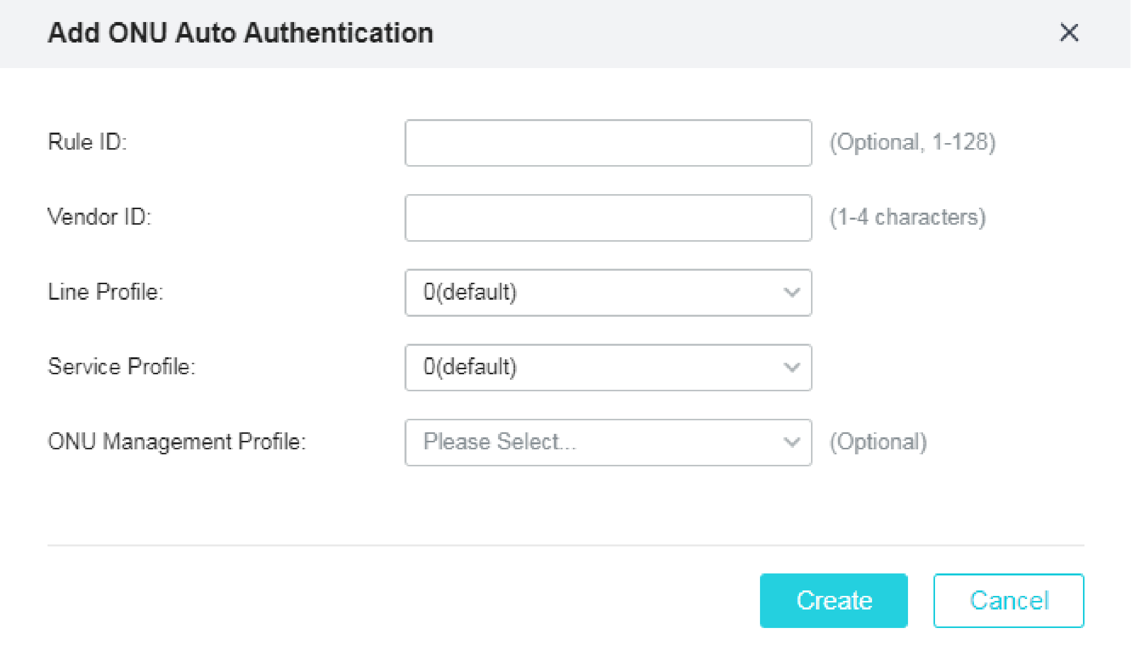
Line Profile: 0(default)

Service Profile: 0(default)

ONU Management Profile: Please Select... (Optional)

Rule ID	(Optional) Set the Rule ID. The Rule ID is the unique identifier for the ONU Auto authentication rule. If you leave the Rule ID as blank, the system automatically assigns the Rule ID.
Equiment ID / Version	Specify the Equiment ID and Software Version. The ONUs with the equipment ID and the software version are auto-authenticated.
Line Profile	Select the line profile used by the ONUs. To create line profiles, go to **PON** > **Profile** > **Line**.
Service Profile	Select the service profile used by the ONUs. To create service profiles, go to **PON** > **Profile** > **Services**.
ONU Management Profile	Select the management profile used by the ONU. To create management profiles, go to **PON** > **Profile** > **ONU Management**.

- **For Vendor-Auth**



Add ONU Auto Authentication

Rule ID:		(Optional, 1-128)
Vendor ID:		(1-4 characters)
Line Profile:	0(default)	
Service Profile:	0(default)	
ONU Management Profile:	Please Select...	(Optional)

Rule ID	(Optional) Set the Rule ID. The Rule ID is the unique identifier for the ONU Auto authentication rule. If you leave the Rule ID as blank, the system automatically assigns the Rule ID.
Vendor ID	Specify the Vendor ID. The ONUs with the Vendor ID are auto-authenticated.
Line Profile	Select the line profile used by the ONUs. To create line profiles, go to **PON** > **Profile** > **Line**.
Service Profile	Select the service profile used by the ONUs. To create service profiles, go to **PON** > **Profile** > **Services**.
ONU Management Profile	Select the management profile used by the ONU. To create management profiles, go to **PON** > **Profile** > **ONU Management**.

- **For All-ONU**

For the ONU Match Mode of All-ONU, you do not need to add any ONU Auto Authentication rules, and all the ONUs are matched in auto authentication.

3. 2. 7 Manage ONU

Overview

After the ONU is authenticated and registered, you can manage the ONUs. ONU management includes the following functions:

- View ONU Information

Configuration

■ View ONU Information

Go to PON > ONU Management. In the ONU VLAN Isolation section, enable the ONU VLAN Isolation. Click Apply.

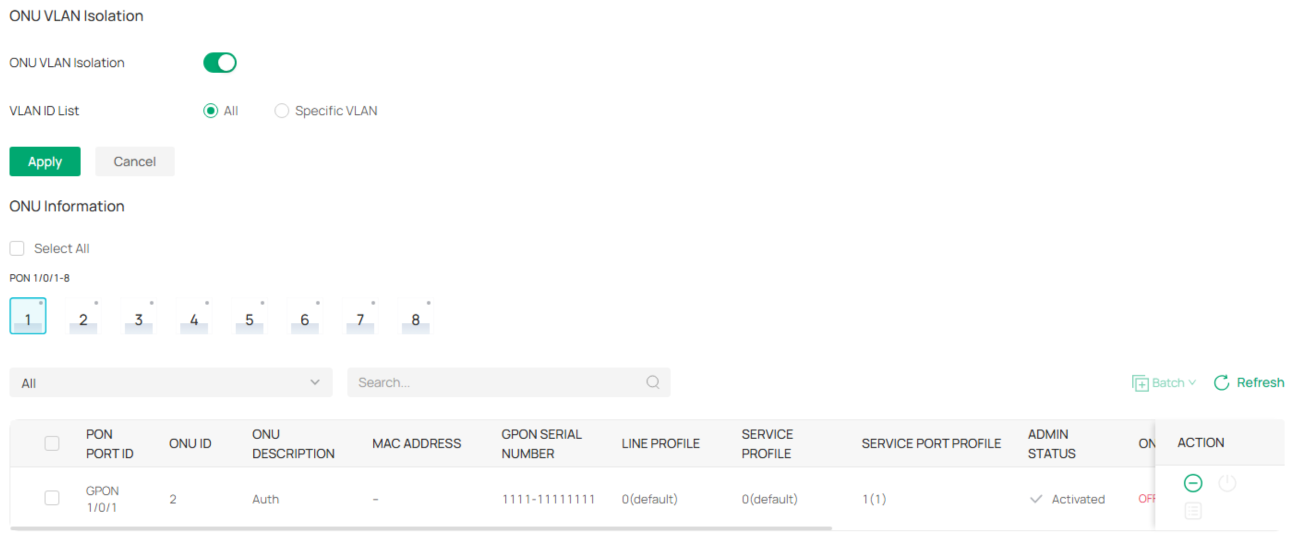
The ONU VLAN Isolation feature is used to configure whether ONUs within the same VLAN can have mutual access.

For Pizzabox OLT, the ONU VLAN isolation feature is disabled by default. When you click to enable it, the VLAN ID List configuration option will be expanded. You can choose between “All” or “Specific VLAN.” If you choose “Specific VLAN,” you are allowed to input the VLAN that will enable ONU isolation.

On the other hand, for Chassis OLT, the ONU VLAN isolation feature is enabled by default. The VLAN ID List is set to “All” by default, meaning that all VLANs are included in the ONU isolation.

When either Port/ONU Isolation function in 3. 2. 1 Configure PON Port or ONU VLAN Isolation function in View ONU Information is enabled, the isolation takes effect.

Select the PON ports which the ONUs are connected. The ONUs which are authenticated and registered appears in the List. You can click ⊖ to deactivate the ONU. You can click ⚡ to activate the ONU. You can click ⏻ to reboot the ONU.



ONU VLAN Isolation

ONU VLAN Isolation: on

VLAN ID List: ● All ○ Specific VLAN

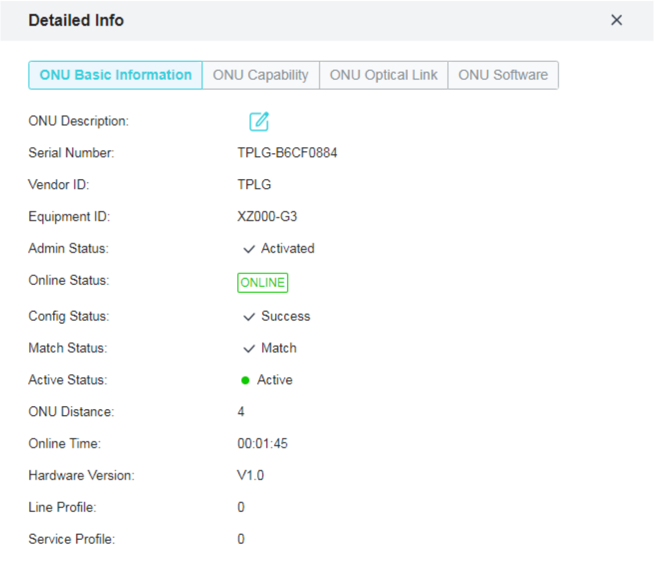
ONU Information

□ Select All

PON 1/0/1-8

□	PON PORT ID	ONU ID	ONU DESCRIPTION	MAC ADDRESS	GPON SERIAL NUMBER	LINE PROFILE	SERVICE PROFILE	SERVICE PORT PROFILE	ADMIN STATUS	ON	ACTION
□	GPON 1/0/1	2	Auth	-	1111-11111111	0(default)	0(default)	1(1)	✓ Activated	OFF	⊖ ⏻ ☰

You can click ☰ to view the detailed info of the ONU.



Detailed Info

ONU Description:
Serial Number: TPLG-B6CF0884
Vendor ID: TPLG
Equipment ID: XZ000-G3
Admin Status: ✓ Activated
Online Status: ONLINE
Config Status: ✓ Success
Match Status: ✓ Match
Active Status: ● Active
ONU Distance: 4
Online Time: 00:01:45
Hardware Version: V1.0
Line Profile: 0
Service Profile: 0

3. 2. 8 Service Port

Overview

Service ports are used by OLT to map different types of traffic to different SVLANs according to PON ports, ONUs, GEM ports, User VLANs, and priorities, and then transmitted to the uplink network. The rate limit for inbound and outbound traffic of the uplink network is determined by traffic profiles which are applied to the service ports.

Service Ports include the following functions:

- Configure Service Port

You can configure Service Port for an ONU before or after the ONU goes online.

- Configure Auto Service Ports

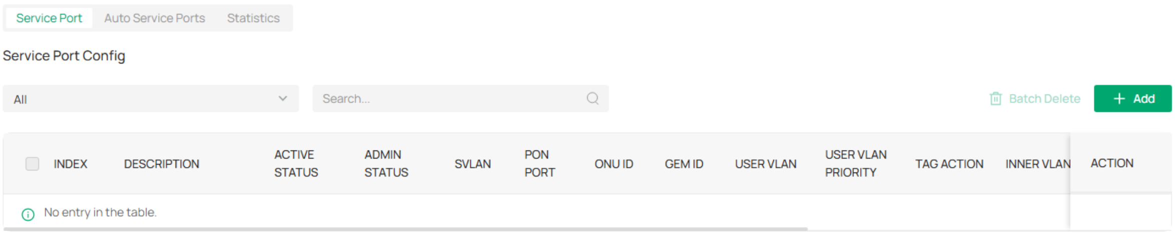
You can configure Auto Service Ports for the ONUs which are connected to a PON port in batches.

- View the statistics of Service Ports

Configuration

■ **Configure Service Port**

Go to PON > Service Port > Service Port. Click + Add to add a service port entry. Configure the parameters and click Apply.

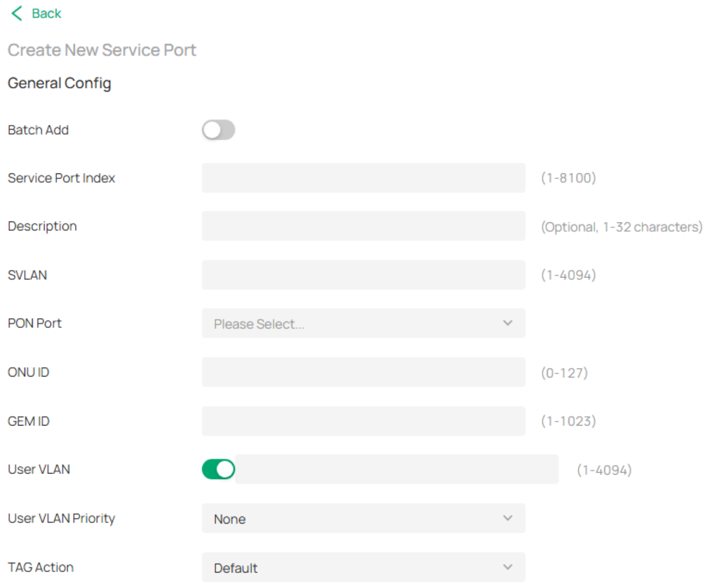


Service Port Config

All

Search...

☐	INDEX	DESCRIPTION	ACTIVE STATUS	ADMIN STATUS	SVLAN	PON PORT	ONU ID	GEM ID	USER VLAN	USER VLAN PRIORITY	TAG ACTION	INNER VLAN	ACTION
No entry in the table.													



Create New Service Port

General Config

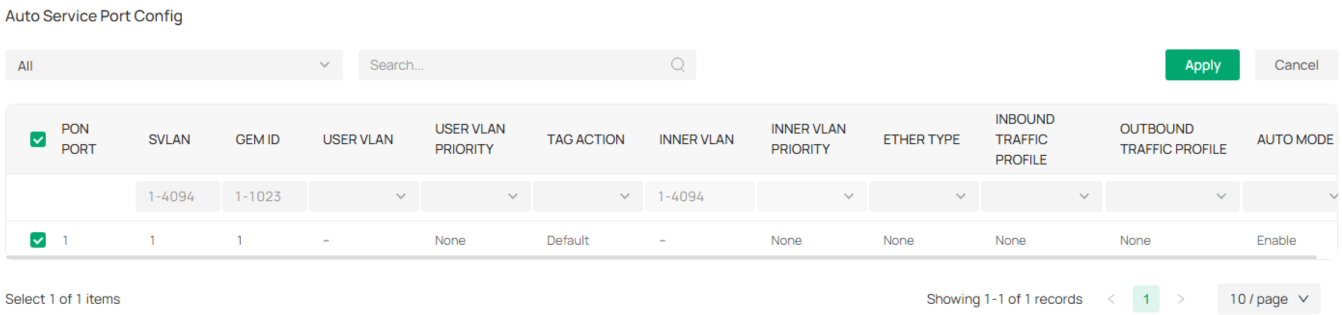
Batch Add	○	
Service Port Index		(1-8100)
Description		(Optional, 1-32 characters)
SVLAN		(1-4094)
PON Port	Please Select...	
ONU ID		(0-127)
GEM ID		(1-1023)
User VLAN	●	(1-4094)
User VLAN Priority	None	
TAG Action	Default	

Batch Config	Enable Batch Config if you want to add several service ports in batches. During batch configuration, the system will automatically assign the smallest available Index.
Service Port Index	Set the Service Port Index, which is the unique identifier for the Service Port.
Description	(Optional) Enter the description of the Service Port.
SVLAN	The traffic which is matched by the Service Port entry is mapped to the SVLAN in the side of ISP network.
PON Port / ONU ID / GEM ID / User VLAN / User VLAN Priority	The Service Port entry only matches the traffic of the specified PON port, ONU ID, GEM ID, User VLAN, and User VLAN Priority. If the User VLAN is disabled, the Service Port entry matches all User VLANs. If the User VLAN Priority is set as None, the Service Port entry matches all User VLAN Priorities.
TAG Action	Select the method to deal with the tagged traffic. Default: The Serivice Port adds the specified SVLAN and keeps the User VLAN unchanged. Transparent: The Serivice Port uses the User VLAN as the SVLAN. Translate: The Serivice Port translates the User VLAN to the specified SVLAN. Translate-And-Add: The Serivice Port translates the User VLAN to the specified inner VLAN and then add an outer layer of SLAN. Add-Double: The Service Port adds the inner VLAN and an outer layer of SVLAN.

EtherType	The Service Port entry only matches the specified type of traffic. If the EtherType is set as None, The Service Port matches all the types.
Inbound Traffic Profile / Outbound Traffic Profile	Select the Traffic Profile used by the Service Port for the inbound / outbound traffic. To create traffic profiles, go to **PON** > **Profile** > **Traffic**.
Admin Status	Enable or disable the Service Port entry.
Performance Statistics	Enable or disable the performance statistics function of the Service Port entry.

■ Configure Auto Service Ports

Go to PON > Service Port > Auto Service Ports. Select the PON ports which the ONUs are connected. Configure the parameters of Auto Service Ports and click Apply.



Auto Service Port Config

All | Search... | Apply | Cancel

☑	PON PORT	SVLAN	GEM ID	USER VLAN	USER VLAN PRIORITY	TAG ACTION	INNER VLAN	INNER VLAN PRIORITY	ETHER TYPE	INBOUND TRAFFIC PROFILE	OUTBOUND TRAFFIC PROFILE	AUTO MODE
		1-4094	1-1023				1-4094					
☑	1	1	1	-	None	Default	-	None	None	None	None	Enable

Select 1 of 1 items

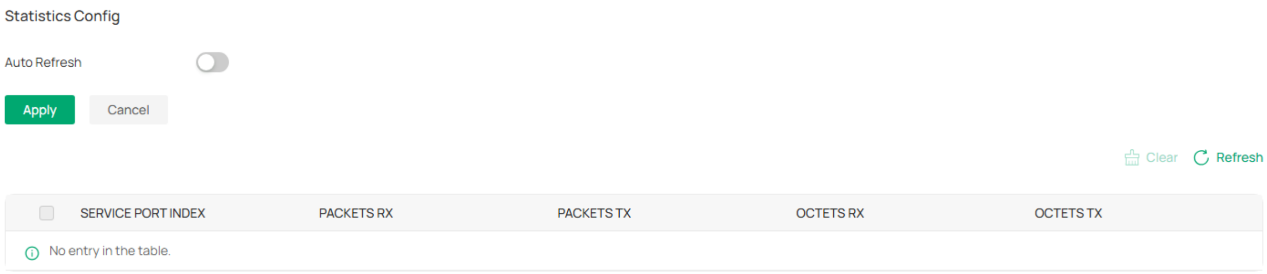
Showing 1-1 of 1 records < 1 > 10 / page

SVLAN	The traffic which is matched by the Service Port entry is mapped to the SVLAN in the side of ISP network.
PON Port / GEM ID / User VLAN / User VLAN Priority	The Service Port entry only matches the traffic of the specified PON port, GEM ID, User VLAN, and User VLAN Priority. If the User VLAN is disabled, the Service Port entry matches all User VLANs. If the User VLAN Priority is set as None, the Service Port entry matches all User VLAN Priorities.
TAG Action	Select the method to deal with the tagged traffic. Default: The Serivice Port adds the specified SVLAN and keeps the User VLAN unchanged. Transparent: The Serivice Port uses the User VLAN as the SVLAN. Translate: The Serivice Port translates the User VLAN to the specified SVLAN. Translate-And-Add: The Serivice Port translates the User VLAN to the specified inner VLAN and then add an outer layer of SLAN. Add-Double: The Serivice Port adds the inner VLAN and an outer layer of SVLAN.
Inner VLAN / Inner VLAN Priority	If the Tag Action is Translate-And-Add or Add-Double, you can specify the Inner VLAN and Inner VLAN Priority.
EtherType	The Service Port entry only matches the specified type of traffic. If the EtherType is set as None, The Service Port matches all the types.

Inbound Traffic Profile / Outbound Traffic Profile	Select the Traffic Profile used by the Service Port for the inbound / outbound traffic. To create traffic profiles, go to **PON** > **Profile** > **Traffic**.
Auto Mode	Enable or disable the Auto Service Port entry.

- **View the statistics of Service Ports**

1. Go to PON > Service Port > Statistics. In the Statistcs Config section, configure the parameters and click Apply. you can view the statistics of Service Ports in the table.



Statistics Config

Auto Refresh ○

☐	SERVICE PORT INDEX	PACKETS RX	PACKETS TX	OCTETS RX	OCTETS TX

No entry in the table.

Auto Refresh	Enable or disable the Auto Refresh function of the Service Port Statistics.
Refresh Interval	If you enable Auto Refresh, set the refresh interval.
Service Port Index	Displays the Service Port Index, which is the unique identifier of the Service Port.
Packets Rx	Displays the number of packets which the Service Port receives.
Packets Tx	Displays the number of packets which the Service Port transmits.
Octets Rx	Displays the number of bytes which the Service Port receives.
Octets Tx	Displays the number of bytes which the Service Port transmits.

Chapter 4

Configure L2 Features

This chapter guides you on how to configure L2 features. The chapter includes the following sections:

4. 1 Configure ETH Port

Overview

ETH Port is used to configure the physical interfaces, which the OLT uses to exchange data and interact with interfaces of other network devices including ONU and ONT. With ETH Port, you can configure the following features: Port Config, Port Isolation, and Loopback Detection.

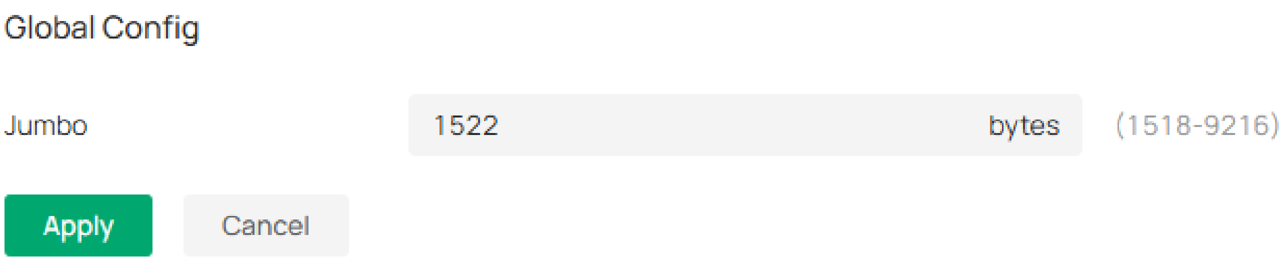
4. 1. 1 Port Config

Overview

With Port Config, you can configure the basic parameters of the OLT interfaces, including speed mode, duplex mode, status, and description.

Configuration

1. Go to L2 Features > ETH Port > Port Config to load the following page. In Global Config, configure the MTU size of jumbo frames for all ports. Click Apply.

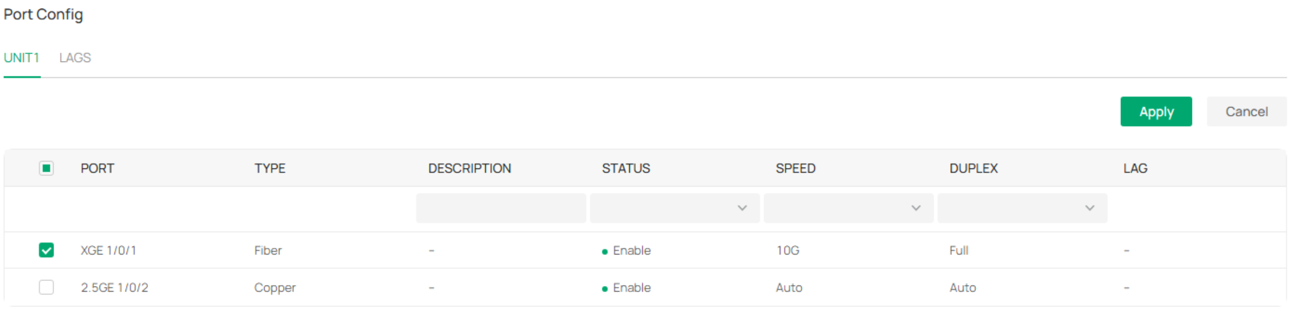


Global Config

Jumbo: 1522 bytes (1518-9216)

Jumbo	Configure the size of jumbo frames. By default, it is 1522 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1522 bytes. If you want the OLT to transmit frames whose MTU size is larger than 1522 bytes, you can set the desired size here for all the interfaces.

2. In Port Config, select one or multiple ports to configure their basic parameters. Click Apply.



Port Config

■	PORT	TYPE	DESCRIPTION	STATUS	SPEED	DUPLEX	LAG
☑	XGE 1/0/1	Fiber	-	● Enable	10G	Full	-
□	2.5GE 1/0/2	Copper	-	● Enable	Auto	Auto	-

Unit/LAGS	Click the Unit number to configure the physical ports. Click LAGS to configure LAG (Link Aggregation Group) ports.
Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the ID of the LAG.
Type (Only for Unit)	Displays the port type. Copper: The port is an Ethernet port. Fiber: The port is an SFP port.
Description	(Optional) Enter a description for easy identification of the port.
Status	Select the working status of the port. Enable: The port can transmit and receive packets. Disable: The port cannot transmit and receive packets.
Speed	Select the appropriate speed mode for the port. Auto: The port automatically negotiates speed mode with connected devices. 10M/100M/1000M/10G: The port can only uses the chosen speed.
Duplex	Select the appropriate duplex mode for the port. Auto: The port automatically negotiates duplex mode with the connected devices. Full: The port can transmit and receive packets simultaneously.
LAG (Only for Unit)	Displays which LAG the port belongs to.

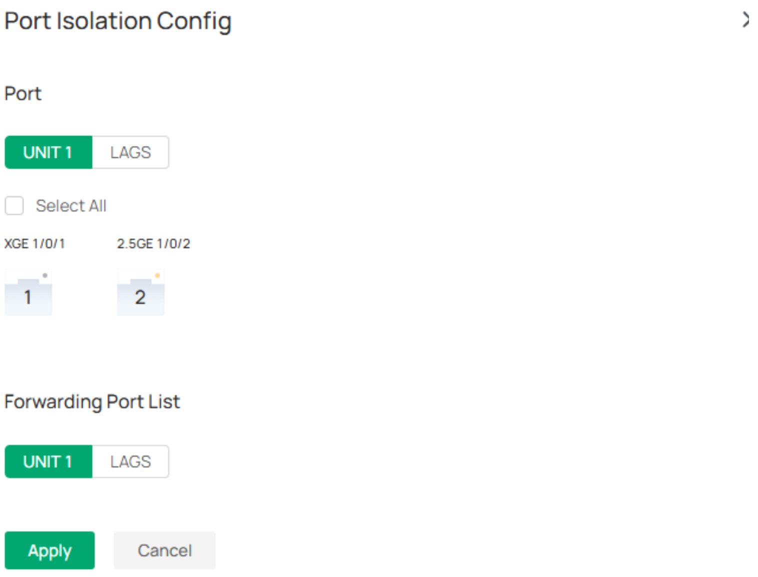
4. 1. 2 Port Isolation

Overview

Port Isolation is used to limit the data transmitted by a port, and the isolated port can only transmit packets to the ports you chosen in its Forwarding Port List.

Configuration

1. Go to L2 Features > ETH Port > Port Isolation, click Edit to load the following page.



2. In Port, select one or multiple ports / LAGs to be isolated.
3. In Forwarding Port List, select one or multiple ports / LAGs as the forwarding ports, and the isolated ports / LAGs can only communicated with the chosen ones. Click Apply.

4. 1. 3 Loopback Detection

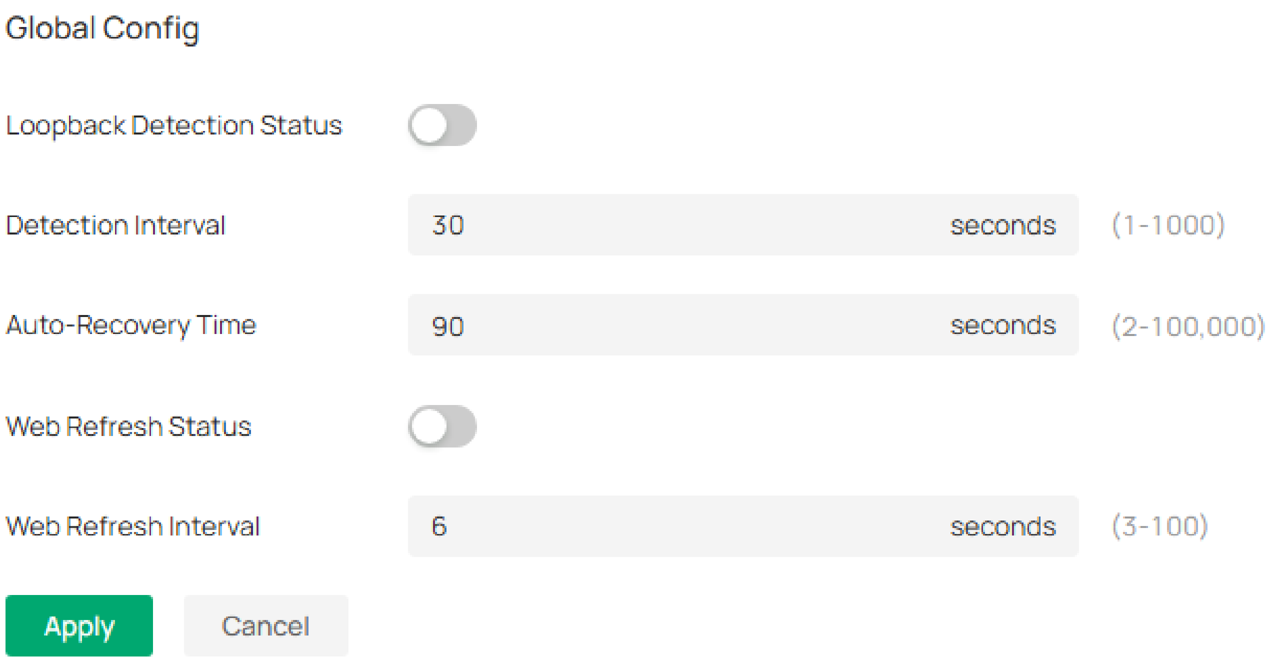
Overview

This function allows the OLT to detect loops in the network. When a loop is detected on a port or VLAN, an alert will be displayed and the OLT will block the corresponding port or VLAN according to your configurations.

Configuration

1. Go to L2 Features > ETH Port > Loopback Detection to load the following page. In Global Config,

enable Loopback Detection Status and configure the global parameters. Click Apply.

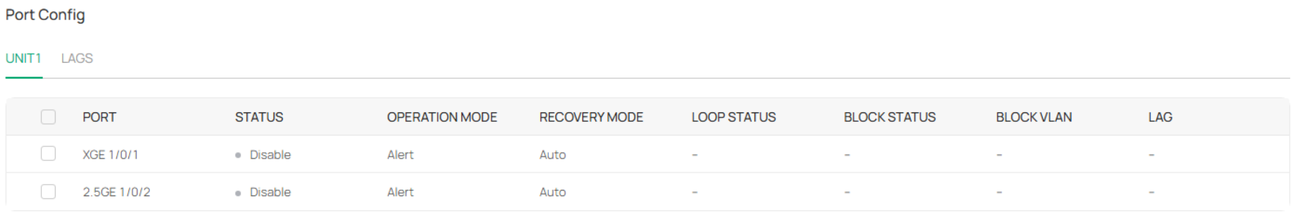


Global Config

Loopback Detection Status	○		
Detection Interval	30	seconds	(1-1000)
Auto-Recovery Time	90	seconds	(2-100,000)
Web Refresh Status	○		
Web Refresh Interval	6	seconds	(3-100)

Loopback Detection Status	Enable Loopback Detection globally.
Detection Interval	Set the interval of sending loopback detection packets in seconds. The valid value ranges from 1 to 1000 and the default value is 30.
Auto-recovery Time	Set the recovery time globally. The blocked port whose Recovery Mode is set as Auto will automatically recover to its normal status after the Auto-recovery Time. The value ranges from 2 to 100,000 in seconds, and the default value is 90.
Web Refresh Status	With this option enabled, the OLT will refresh the configuration page timely to show the detection results. By default, it is disabled.
Web Refresh Interval	If you enabled web refresh status, set the refresh interval in seconds between 3 and 100. The default value is 6.

2. In Port Config, select one or multiple ports to configure the parameters for Loopback Detection. Click Apply.



Port Config

□	PORT	STATUS	OPERATION MODE	RECOVERY MODE	LOOP STATUS	BLOCK STATUS	BLOCK VLAN	LAG
□	XGE 1/0/1	● Disable	Alert	Auto	-	-	-	-
□	2.5GE 1/0/2	● Disable	Alert	Auto	-	-	-	-

Unit/LAGS	Click the Unit number to configure the physical ports. Click LAGS to configure LAG (Link Aggregation) ports.

Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the ID of the LAG.
Status	Select the Loopback Detection status of the port. Enable: Loopback Detection is enabled for the port. Disable: Loopback Detection is disabled for the port.
Operation Mode	Select the operation mode when a loopback is detected on the port: Alert: The Loop Status will display whether there is a loop detected on the corresponding port. It is the default setting for Operation Mode. Port Based: In addition to displaying alerts, the OLT will block the port on which the loop is detected. VLAN Based: If a loop is detected in a VLAN on that port, in addition to displaying alerts, the OLT will block that VLAN. The traffic of the other VLANs can still be forwarded by the port.
Recovery Mode	If you select Port Based or VLAN Based as the operation mode, you also need to configure the recovery mode for the blocked port: Auto: The blocked port will automatically recover to its normal status after the automatic recovery time. It is the default setting. Manual: You need to manually release the blocked port. by clicking **Recover** on the upper right to release the selected port.
Loop Status	Displays whether a loop is detected on the port.
Block Status	Displays whether the port is blocked.
Block VLAN	Displays the blocked VLANs.
LAG (Only for Unit)	Displays which LAG the port belongs to.

Note: If the port is a member port of an LAG, it will follow the port configuration of the LAG and not its own.

4. 2 Configure LAG

Overview

With LAG (Link Aggregation Group) function, you can aggregate multiple physical ports into a logical interface, increasing link bandwidth and providing backup ports to enhance the connection reliability. OLT provides two types of LAG configuration: static LAG and LACP (Link Aggregation Control Protocol).

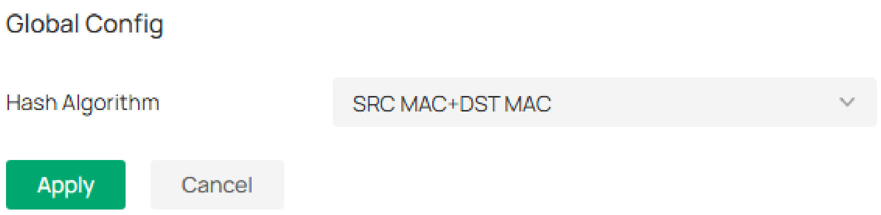
4. 2. 1 LAG Table

Overview

With LAG Table, you can set the load-balancing algorithm (Hash Algorithm) globally, and view the information of the static LAG and LACP you have configured.

Configuration

1. Go to L2 Features > LAG> LAG Table to load the following page. In Global Config, configure the Hash Algorithm for all LAG ports. Click Apply.



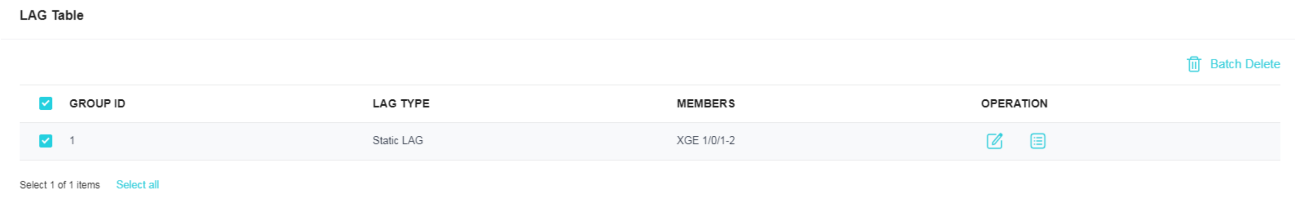
Global Config

Hash Algorithm: SRC MAC+DST MAC

Hash Algorithm	Select the Hash Algorithm, and the OLT will choose the port to forward the received packets based on your chosen Hash Algorithm . In this way, different data flows are forwarded on different physical links to implement load balancing. SRC MAC: The computation is based on the source MAC addresses of the packets. DST MAC: The computation is based on the destination MAC addresses of the packets. SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets. SRC IP: The computation is based on the source IP addresses of the packets. DST IP: The computation is based on the destination IP addresses of the packets. SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets. Note: Please properly choose the load-balancing algorithm to avoid data stream transferring only on one physical link.

2. View the configured static LAG and LACP in the LAG Table. Click ✎ to edit the entry, and click ☰

to view its details.



LAG Table

Batch Delete

☑	GROUP ID	LAG TYPE	MEMBERS	OPERATION
☑	1	Static LAG	XGE 1/0/1-2	

Select 1 of 1 items Select all

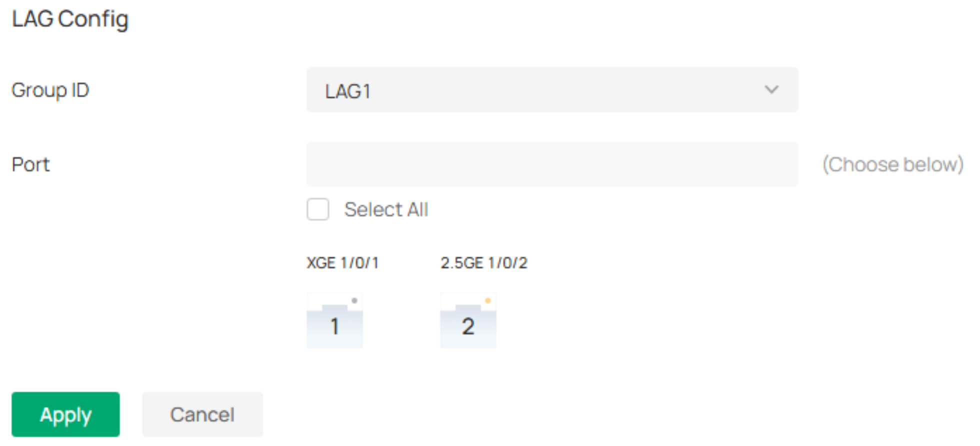
4. 2. 2 Static LAG

Overview

For Static LAG, the member ports are manually added.

Configuration

Go to L2 Features > LAG > Static LAG to load the following page and select member ports for the configured LAG. Click Apply.



LAG Config

Group ID: LAG1

Port: (Choose below)

□ Select All

Group ID	Select an LAG ID for the static LAG entry.
Description	Displays the LAG mode.
Port	Select the member ports of the LAG by clicking the port icons below.

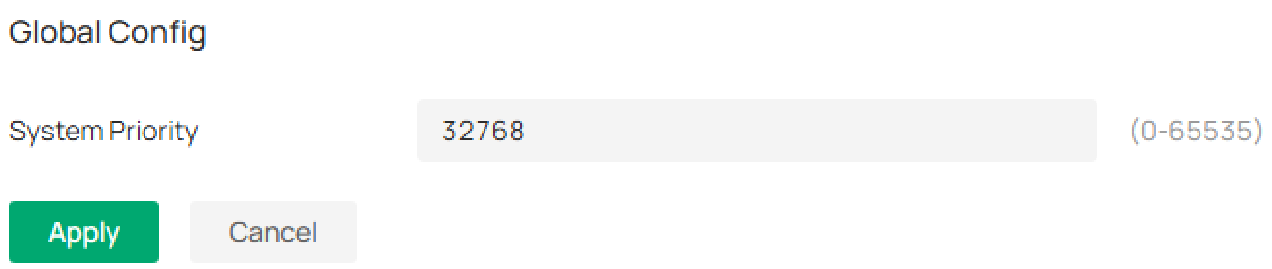
4. 2. 3 LACP

Overview

With LACP feature, the OLT uses LACP to implement dynamic link aggregation and disaggregation by exchanging LACP packets with its peer device. LACP extends the flexibility of the LAG configuration.

Configuration

1. Go to L2 Features > LAG > LACP Config to load the following page and specify the System Priority for the OLT. Click Apply.

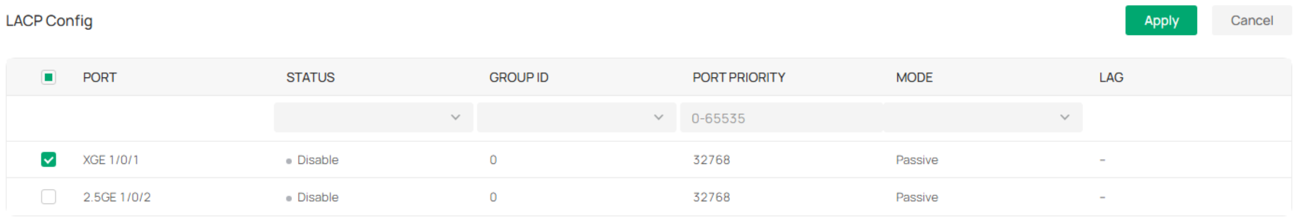


Global Config

System Priority: 32768 (0-65535)

System Priority	Specify the system priority for the OLT. A smaller value means a higher priority. To keep active ports consistent at both ends, you can set the system priority of one device to be higher than that of the other device. The device with higher priority will determine its active ports, and the other device can select its active ports according to the selection result of the device with higher priority. If the two ends have the same system priority value, the device with a smaller MAC address has the higher priority.

2. In LACP Config, select member ports and configure the parameters. Click Apply.



LACP Config

■	PORT	STATUS	GROUP ID	PORT PRIORITY	MODE	LAG
				0-65535		
☑	XGE 1/0/1	● Disable	0	32768	Passive	-
☐	2.5GE 1/0/2	● Disable	0	32768	Passive	-

Port	Displays the port number.
Status	Whether to enable the LACP feature for the LAG. By default, it is disabled. Enable: LACP feature is enabled for the LAG. Disable: LACP feature is disabled for the LAG.
Group ID	Specify the group ID of the LAG. Note that the group ID of other static LAGs cannot be the same as the value you set. The valid value of the Group ID is determined by the maximum number of LAGs supported by your OLT. For example, if your OLT supports up to 4 LAGs, the valid value ranges from 1 to 4.

Port Priority	Specify the Port Priority, ranging from 0 to 65535. A smaller value means a higher port priority. The port with higher priority in an LAG will be selected as the working port to forward data, and eight ports can work simultaneously at most. If two ports have the same priority value, the port with a smaller port number has the higher priority.
Mode	Select the LACP mode for the port. In LACP, the OLT uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. The LACP mode determines whether the port will take the initiative to send the LACPDU. Passive: The port will not send LACPDU before receiving the LACPDU from the peer end. Active: The port will take the initiative to send LACPDU.
LAG	Displays which LAG the port belongs to.

4. 3 Configure MAC Address

Overview

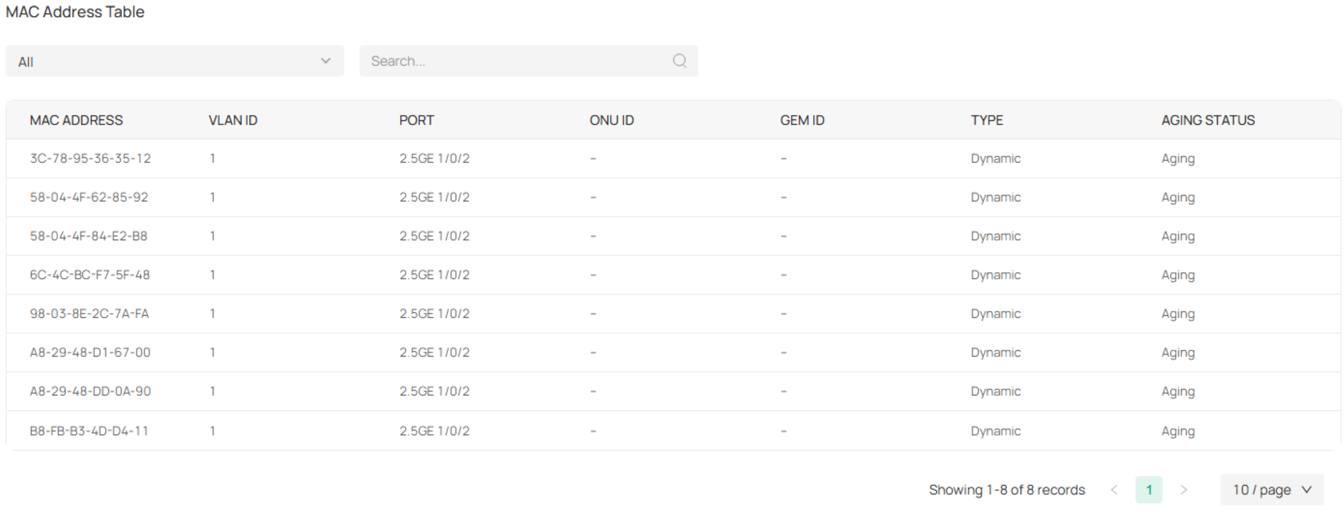
In MAC Address, you can view the address information that the OLT uses to forward packets. Also, you can configure and manage static MAC addresses and filtering rules.

4. 3. 1 MAC Address Table

Overview

The MAC address table contains address information that the OLT uses to forward packets. As shown below, the table lists map entries of MAC addresses, VLAN IDs, ports, type and its aging status. These entries can be manually added or automatically learned by the OLT. Based on the MAC-address-to-port mapping in the table, the OLT can forward packets only to the associated port.

To search for a specific MAC address entry, you can select the parameter and type in the key words in the search bar.



MAC Address Table

MAC ADDRESS	VLAN ID	PORT	ONU ID	GEM ID	TYPE	AGING STATUS
3C-78-95-36-35-12	1	2.5GE 1/0/2	-	-	Dynamic	Aging
58-04-4F-62-85-92	1	2.5GE 1/0/2	-	-	Dynamic	Aging
58-04-4F-84-E2-B8	1	2.5GE 1/0/2	-	-	Dynamic	Aging
6C-4C-BC-F7-5F-48	1	2.5GE 1/0/2	-	-	Dynamic	Aging
98-03-8E-2C-7A-FA	1	2.5GE 1/0/2	-	-	Dynamic	Aging
A8-29-48-D1-67-00	1	2.5GE 1/0/2	-	-	Dynamic	Aging
A8-29-48-DD-0A-90	1	2.5GE 1/0/2	-	-	Dynamic	Aging
B8-FB-B3-4D-D4-11	1	2.5GE 1/0/2	-	-	Dynamic	Aging

Showing 1-8 of 8 records

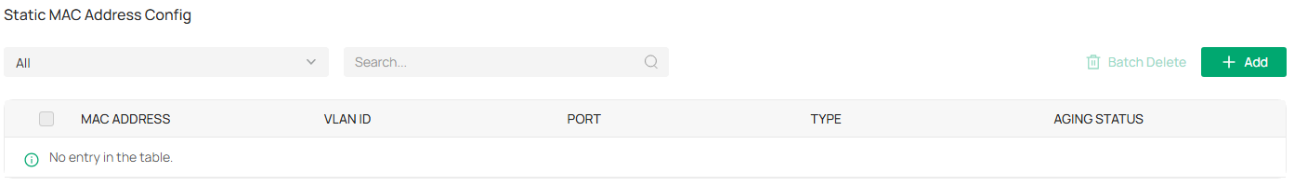
4. 3. 2 Static MAC Address

Overview

Static MAC addresses are manually added to the address table and they do not age. For some relatively fixed connection, you can manually set the MAC address of the device as a static entry to enhance the forwarding efficiency of the OLT.

Configuration

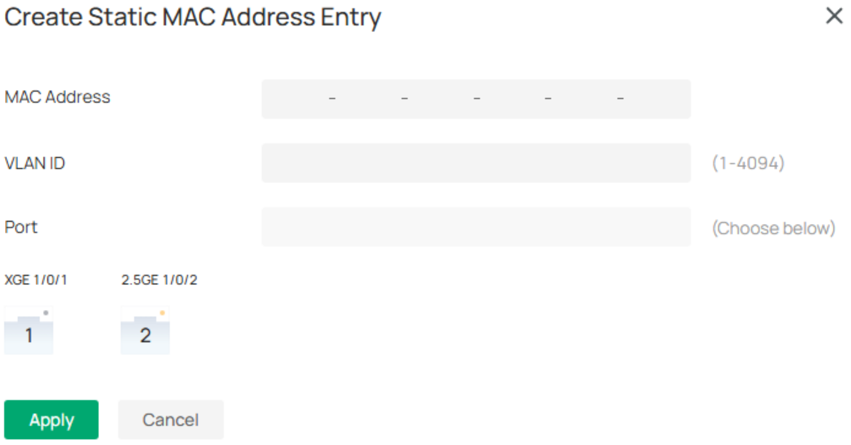
1. Go to L2 Features > MAC Address > Static MAC Address to load the following page.



Static MAC Address Config

MAC ADDRESS	VLAN ID	PORT	TYPE	AGING STATUS
No entry in the table.				

2. Click +Add on the upper right and configure the parameters to add a new static MAC address entry. Click Create.



Create Static MAC Address Entry

MAC Address: - - - - -

VLAN ID: (1-4094)

Port: (Choose below)

MAC Address	Enter the static MAC address of the static MAC address entry.
VLAN ID	Enter the VLAN ID of an existing VLAN, and the packets with the specific MAC address are received in the specified VLAN.
Port	Select a port by clicking the port icon below, and the packets with the specific MAC address are forwarded to the port. The port must belong to the specified VLAN above. After you have added the static MAC address, if the corresponding port number of the MAC address is not correct, or the connected port (or the device) has been changed, the OLT cannot forward the packets correctly. Please add a new static address entry accordingly.

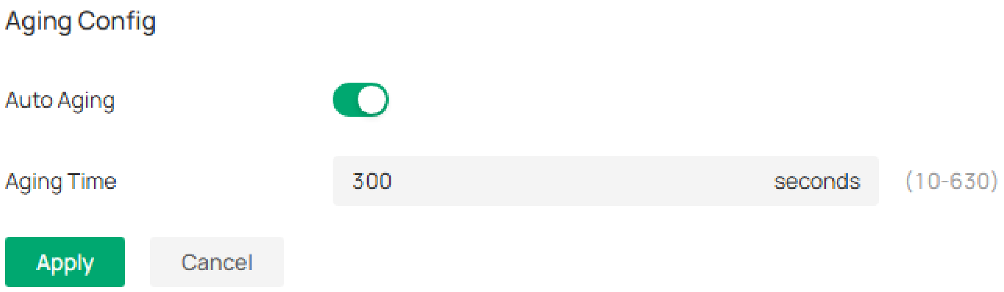
4. 3. 3 Dynamic MAC Address

Overview

Dynamic addresses are addresses learned by the OLT automatically, and the OLT regularly ages out those entries that are not in use. That is, the OLT removes the MAC address entries related to a network device if no packet is received from the device after the aging time.

Configuration

1. Go to L2 Features > MAC Address > Dynamic MAC Address to load the following page. Configure the automatic aging parameters. Click Apply.



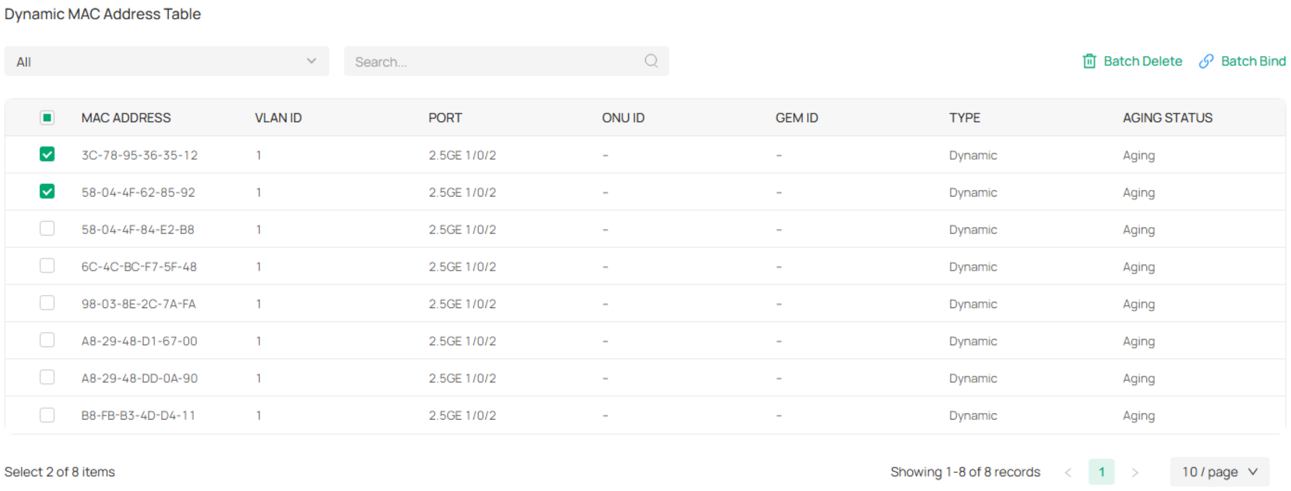
Aging Config

Auto Aging ●

Aging Time 300 seconds (10-630)

Auto Aging	Enable auto aging of the dynamic MAC addresses. By default, it is enabled.
Aging Time	Specify the auto aging time for the dynamic MAC addresses in seconds. By default, it is 300 seconds.

2. In Dynamic MAC Address Table, the automatically learned MAC addresses are displayed. You can click Batch Delete on the upper right to manually delete entries. Also, if you want to bind certain MAC address with ports and VLAN ID, you can click Batch Bind, and then the dynamic MAC address entries will become static MAC address entries and they will not age.



Dynamic MAC Address Table

■	MAC ADDRESS	VLAN ID	PORT	ONU ID	GEM ID	TYPE	AGING STATUS
☑	3C-78-95-36-35-12	1	2.5GE 1/0/2	-	-	Dynamic	Aging
☑	58-04-4F-62-85-92	1	2.5GE 1/0/2	-	-	Dynamic	Aging
□	58-04-4F-84-E2-B8	1	2.5GE 1/0/2	-	-	Dynamic	Aging
□	6C-4C-BC-F7-5F-48	1	2.5GE 1/0/2	-	-	Dynamic	Aging
□	98-03-8E-2C-7A-FA	1	2.5GE 1/0/2	-	-	Dynamic	Aging
□	A8-29-48-D1-67-00	1	2.5GE 1/0/2	-	-	Dynamic	Aging
□	A8-29-48-DD-0A-90	1	2.5GE 1/0/2	-	-	Dynamic	Aging
□	B8-FB-B3-4D-D4-11	1	2.5GE 1/0/2	-	-	Dynamic	Aging

Select 2 of 8 items

Showing 1-8 of 8 records

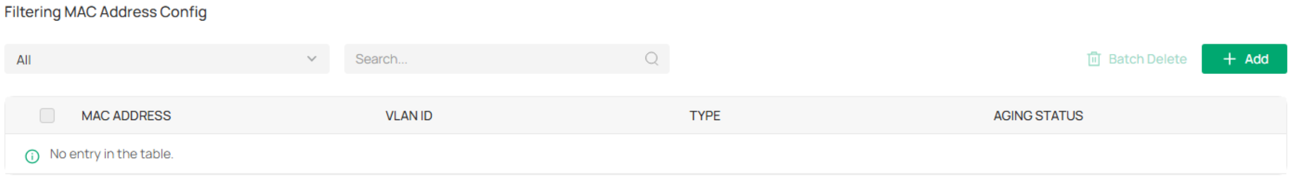
4. 3. 4 Filtering MAC Address

Overview

Filtering MAC Address allows you to manually added filtering entries, and determine that the OLT drops the packets received from the devices of specific MAC addresses.

Configuration

1. Go to L2 Features > MAC Address > Filtering MAC Address to load the following page. To search for a specific entry, you can select the parameter and type in the key words in the search bar.

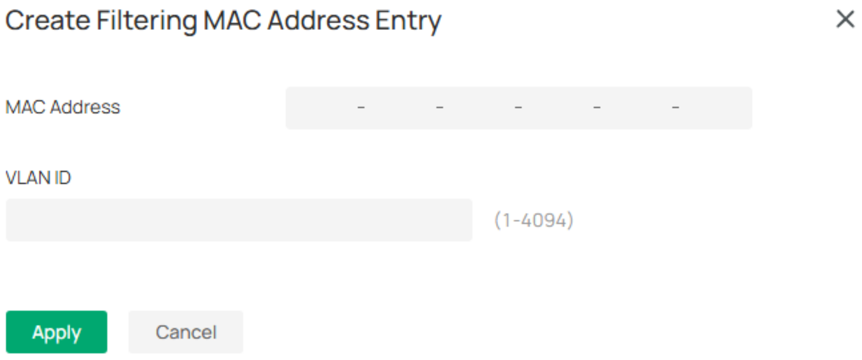


Filtering MAC Address Config

□	MAC ADDRESS	VLAN ID	TYPE	AGING STATUS

No entry in the table.

2. Click +Add on the upper right and configure the parameters to add a new MAC address filtering entry. Click Create.



Create Filtering MAC Address Entry

MAC Address: - - - - -

VLAN ID: (1-4094)

MAC Address	Enter the MAC address for the OLT to filter the received packets.
VLAN ID	Specify an existing VLAN in which packets with the specific MAC address are dropped.

4. 4 Configure VLAN

Overview

VLAN (Virtual Local Area Network) is a network technique that solves broadcasting issues in local area networks, and OLT provides four types of VLAN: 802.1Q VLAN, MAC VLAN, Protocol VLAN, and GVRP. VLAN is usually applied to achieve the following purposes:

1) To restrict broadcast domain: VLAN technique divides a big local area network into several VLANs, and all VLAN traffic remains within its VLAN. It reduces the influence of broadcast traffic in Layer 2 network to the whole network.

2) To enhance network security: Devices from different VLANs cannot achieve Layer 2 communication, and thus users can group and isolate devices to enhance network security.

3) For easier management: VLANs group devices logically instead of physically, so devices in the same VLAN need not be located in the same place. It eases the management of devices in the same work group but located in different places.

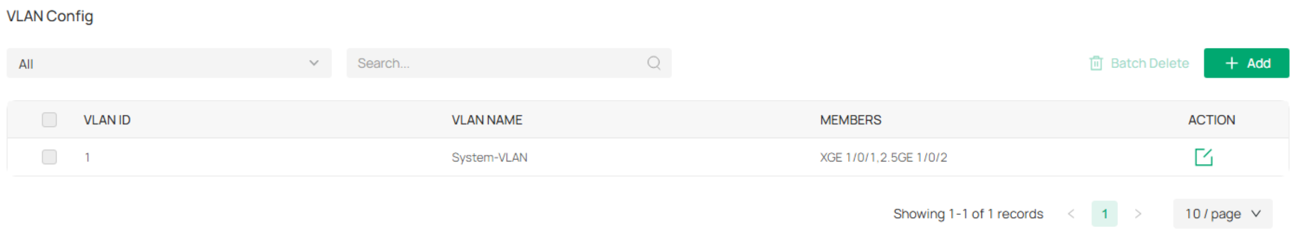
4. 4. 1 802.1Q VLAN

Overview

IEEE 802.1Q is the networking standard that supports VLANs on an IEEE 802.3 Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures used in handling such frames.

Configuration

1. Go to L2 Features > VLAN > 802.1Q VLAN to load the following page. VLAN 1 is the default system VLAN. To search for a specific entry, you can select the parameter and type in the key words in the search bar.

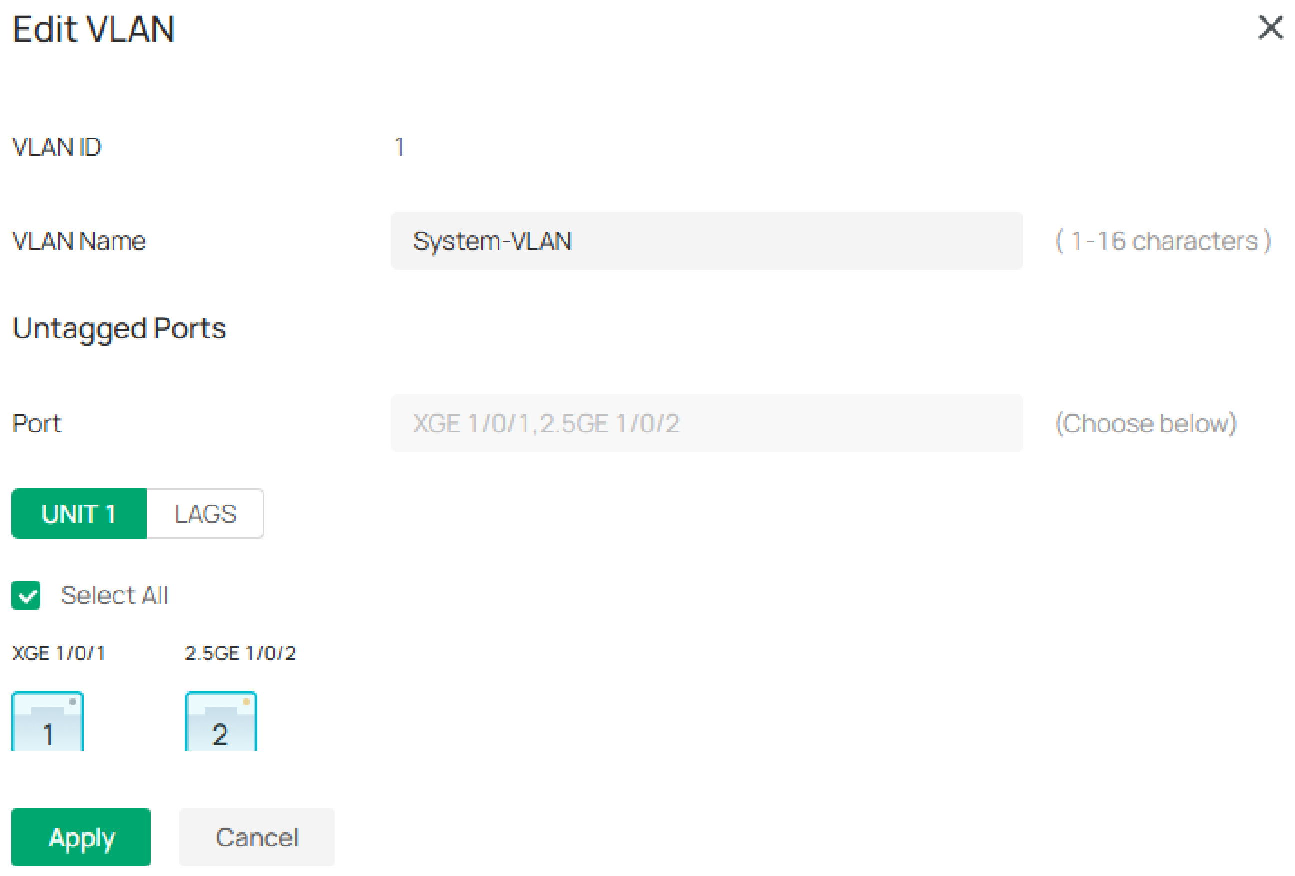


VLAN Config

□	VLAN ID	VLAN NAME	MEMBERS	ACTION
□	1	System-VLAN	XGE 1/0/1,2.5GE 1/0/2	✎

2. Click +Add on the upper right to load the following page. Configure the parameters and click

Create.



Edit VLAN

VLAN ID 1

VLAN Name System-VLAN (1-16 characters)

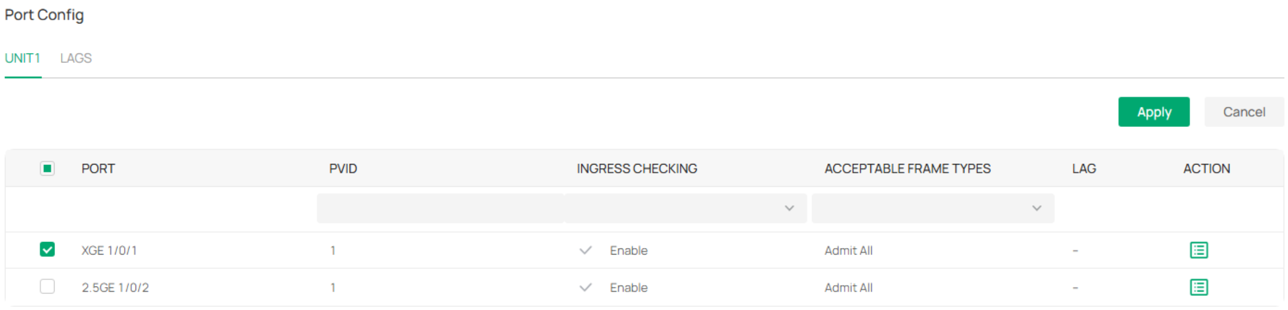
Untagged Ports

Port XGE 1/0/1,2.5GE 1/0/2 (Choose below)

VLAN ID	Enter a VLAN ID for identification with the values between 2 and 4094. VLAN 1 is the default system VLAN.
VLAN Name	Enter a description for easy identification.
Untagged Ports	Select the ports by clicking the port icons below, and the ports will forward untagged packets in the target VLAN.
Tagged Ports	Select the ports by clicking the port icons below, and the ports will forward tagged packets in the target VLAN.

3. Select a port and configure the parameters. Click Apply. You can also view details of a port by

clicking ☰.



Port Config

UNIT1 LAGS

Apply Cancel

☑	PORT	PVID	INGRESS CHECKING	ACCEPTABLE FRAME TYPES	LAG	ACTION
☑	XGE 1/0/1	1	✓ Enable	Admit All	-	☰
□	2.5GE 1/0/2	1	✓ Enable	Admit All	-	☰

Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the LAG ID.
PVID	Set the default VLAN ID of the port. Valid values are from 1 to 4094. When the port receives an untagged packet, the OLT inserts a VLAN tag to the packet based on the PVID.
Ingress Checking	Enable or disable Ingress Checking. With this function enabled, the port will check the packets and only accept the packet whose VLAN ID is in the VLAN list of the port and discard others. With this function disabled, the port will forward the packet directly without checking.
Acceptable Frame Types	Select the acceptable frame type for the port and the port will perform the operation before Ingress Checking. Admit All: The port will accept both the tagged packets and the untagged packets. Tagged Only: The port will accept the tagged packets only.
LAG (Only for Unit)	Displays the LAG which the port belongs to.

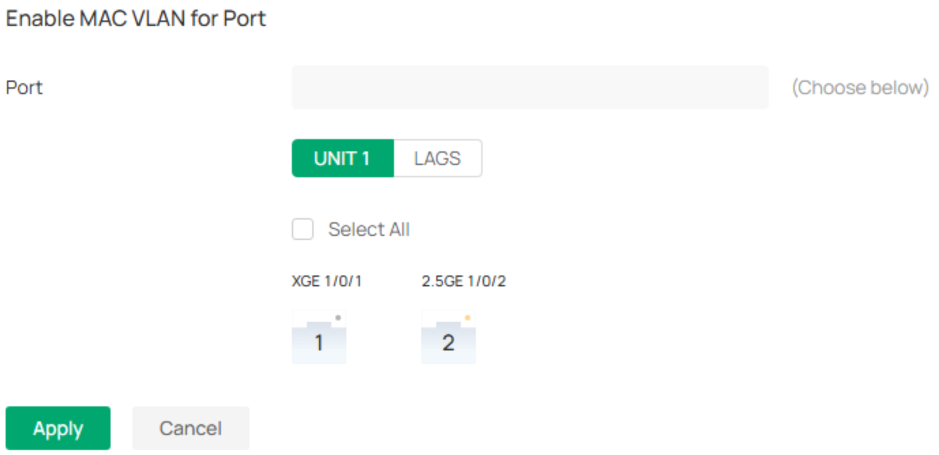
4. 4. 2 MAC VLAN

Overview

VLAN is generally divided by ports. It is a common way of division but isn’t suitable for the networks that require frequent topology changes. For example, a terminal device that accessed the OLT via port XGE 1/0/1 last time may change to port XGE 1/0/2 this time. If the two ports belong to different VLANs, re-configuration is required in order to to access the original VLAN. Using MAC VLAN can free the user from such a problem. It divides VLANs based on the MAC addresses of devices. In this way, devices always belong to their MAC VLANs even when their access ports change.

Configuration

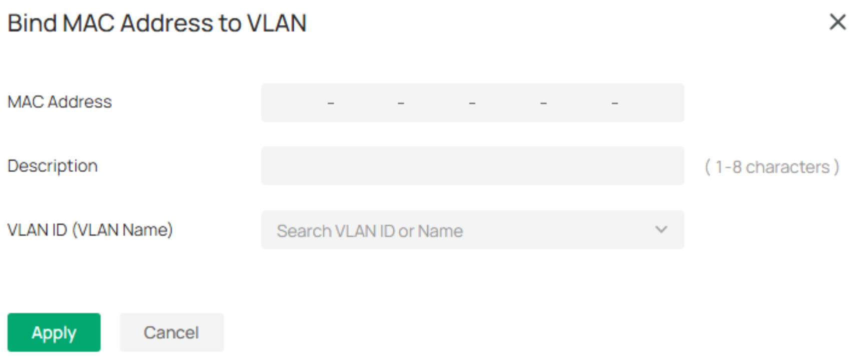
1. Go to L2 Features > VLAN >802.1Q VLAN to create a 802.1Q VLAN, which will be bound to the MAC VLAN later. For details, refer to 4. 4. 1 802.1Q VLAN.
2. Go to L2 Features > VLAN > MAC VLAN to load the following page. Select the ports/LAGs you want to enable MAC VLAN by clicking the port icons.



Enable MAC VLAN for Port

Port (Choose below)

3. Click +Add on the upper right of MAC VLAN Config to load the following page. Configure the parameters and click Create.



Bind MAC Address to VLAN

MAC Address - - - - -

Description (1-8 characters)

VLAN ID (VLAN Name) Search VLAN ID or Name

MAC Address	Enter the MAC address of the device you want to bind to the VLAN.
Description	Enter a description for easy identification.
VLAN ID/Name	Enter the ID number or name of the 802.1Q VLAN that will be bound to the MAC VLAN. For details of configuring 802.1Q VLAN, refer to 4. 4. 1 802.1Q VLAN.

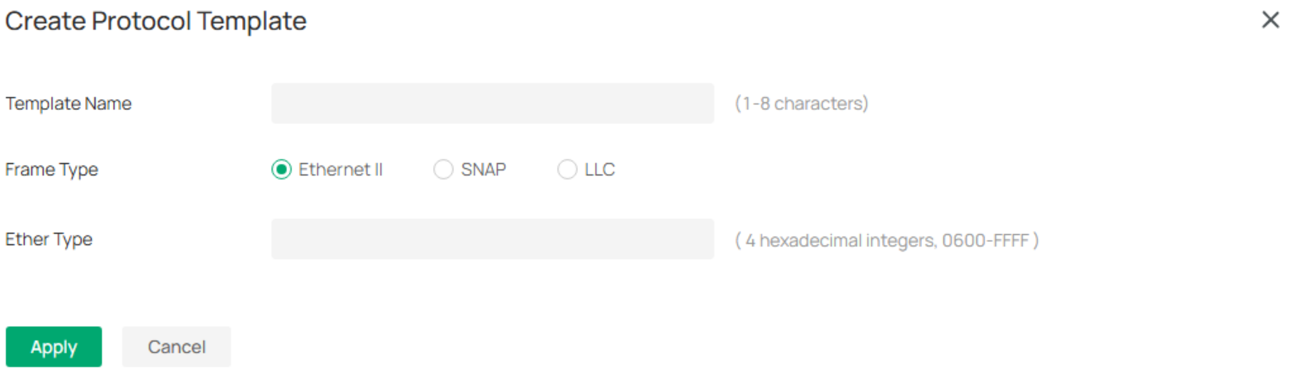
4. 4. 3 Protocol VLAN

Overview

Protocol VLAN is a technology that divides VLANs based on the network layer protocol. With the protocol VLAN rule configured on the basis of the existing 802.1Q VLAN, the OLT can analyze specific fields of received packets, encapsulate the packets in specific formats, and forward the packets with different protocols to the corresponding VLANs. Since different applications and services use different protocols, network administrators can use protocol VLAN to manage the network based on specific applications and services.

Configuration

1. Go to L2 Features > VLAN >802.1Q VLAN to create a 802.1Q VLAN first. For details, refer to 4. 4. 1 802.1Q VLAN.
2. Go to L2 Features > VLAN > Protocol VLAN. In Protocol Template Config, check if your desired template exists. If not, click +Add on the upper right to create a new template. Click Create.



Create Protocol Template

Template Name (1-8 characters)

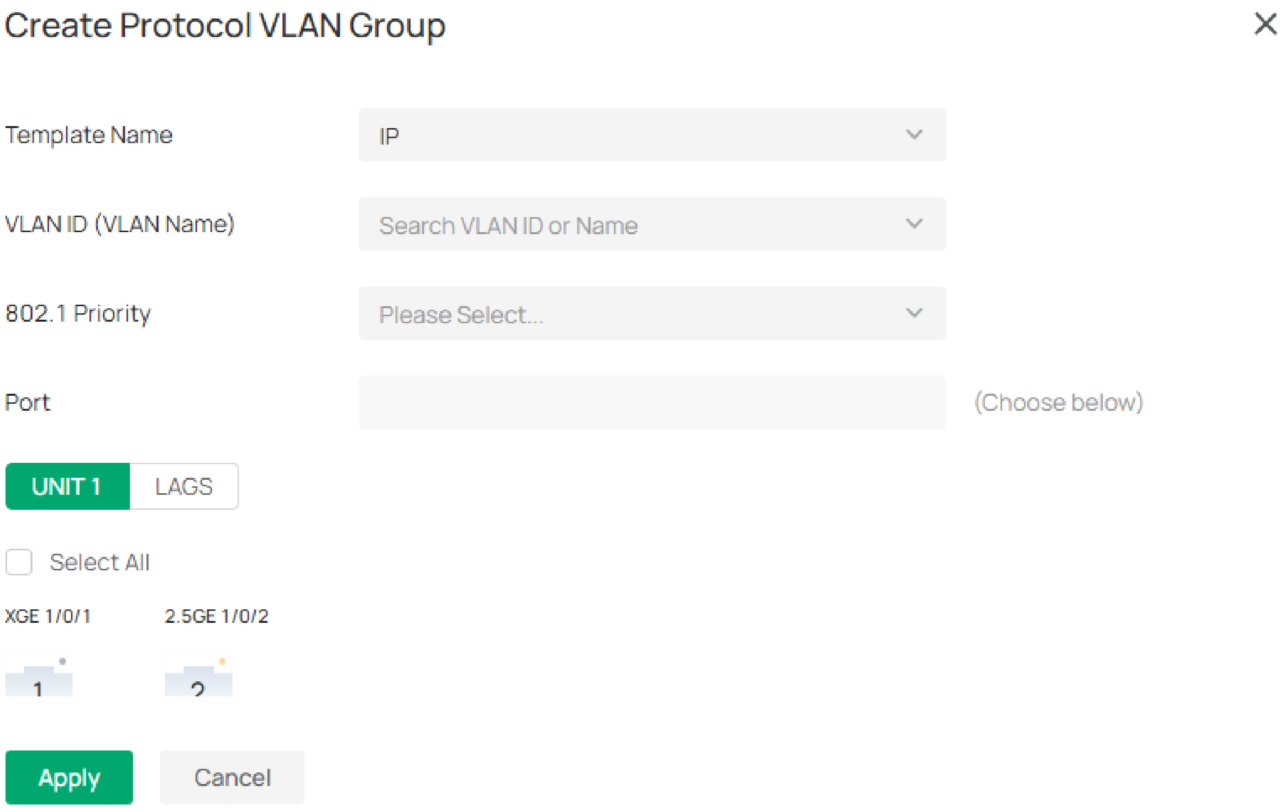
Frame Type ● Ethernet II ○ SNAP ○ LLC

Ether Type (4 hexadecimal integers, 0600-FFFF)

Template Name	Enter a protocol name to identify the protocol template.
Frame Type	Select the frame type of the new protocol template. Ethernet II: A common Ethernet frame format. Select to specify the Frame Type by entering the Ether Type. SNAP: An Ethernet 802.3 frame format based on IEEE 802.3 and IEEE 802.2 SNAP. Select to specify the Frame Type by entering the Ether Type. LLC: An Ethernet 802.3 frame format based on IEEE 802.3 and IEEE 802.2 LLC. Select to specify the Frame Type by entering the DSAP and SSAP.
Ether Type	Enter the Ethernet protocol type value for the protocol template. It is available when Ethernet II and SNAP is selected. It is the Ether Type field in the frame and is used to identify the data type of the frame.
DSAP	Enter the DSAP value for the protocol template. It is available when LLC is selected. It is the DSAP field in the frame and is used to identify the data type of the frame.

SSAP	Enter the SSAP value for the protocol template. It is available when LLC is selected. It is the SSAP field in the frame and is used to identify the data type of the frame.

3. In Protocol VLAN Group Config, click +Add on the upper right, and configure the parameters. Click Create.



Create Protocol VLAN Group

Template Name	IP	
VLAN ID (VLAN Name)	Search VLAN ID or Name	
802.1 Priority	Please Select...	
Port		(Choose below)

Template Name	Select an existing protocol template.
VLAN ID/Name	Enter the ID number or name of the 802.1Q VLAN that will be bound to the Protocol VLAN.
802.1p Priority	Specify the 802.1p priority for the packets that belong to the protocol VLAN. The OLT will determine the forwarding sequence according this value. The packets with larger value of 802.1p priority have the higher priority.
Port	Select the desired ports by clicking the port icons below.

4. 4. 4 GVRP VLAN

Overview

GVRP (GARP VLAN Registration Protocol) is a GARP (Generic Attribute Registration Protocol) application that allows registration and deregistration of VLAN attribute values and dynamic VLAN creation.

Without GVRP operating, configuring the same VLAN on a network would require manual configuration on each device. For a large and more complex network, such manual configuration would be time-consuming and fallible. GVRP can be used to implement dynamic VLAN configuration. With GVRP, a device can exchange VLAN configuration information with the adjacent GVRP device and dynamically create and manage the VLANs. This reduces VLAN configuration workload and ensures correct VLAN configuration.

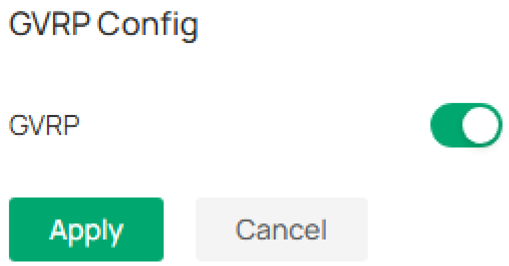
Configuration

Configuration Guidelines:

To dynamically create a VLAN on all ports in a network link, you must configure the same static VLAN on both ends of the link.

We call manually configured 802.1Q VLAN as static VLAN and VLAN created through GVRP as dynamic VLAN. Ports in a static VLAN can initiate the sending of GVRP registration message to other ports. A port registers VLANs only when it receives GVRP messages. As the messages can only be sent from one GVRP participant to another, two-way registration is required to configure a VLAN on all ports in a link. To implement two-way registration, you need to manually configure the same static VLAN on both ends of the link.

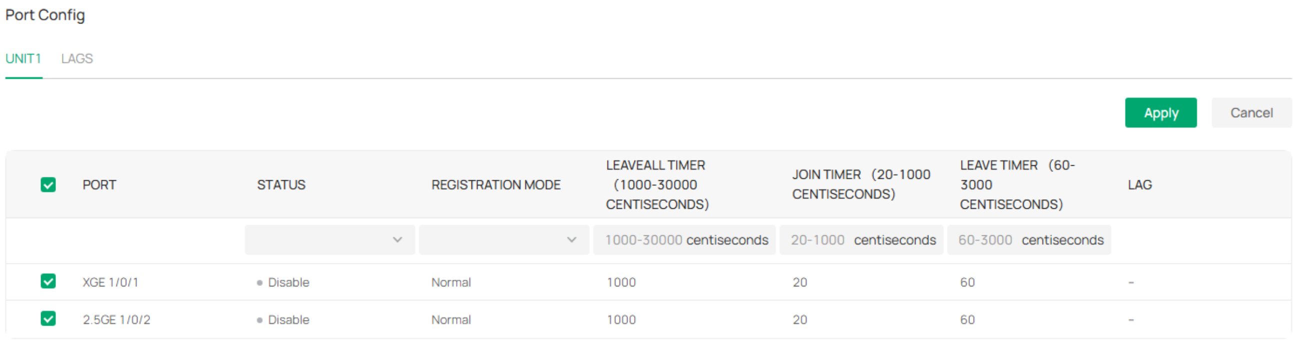
1. Go to L2 Features > VLAN > 802.1Q VLAN to create a 802.1Q VLAN (static VLAN) first. Go to L2 Features > VLAN > GVRP VLAN to enable GVRP globally. Click Apply.



GVRP Config

GVRP ●

2. In Port Config, select a port or multiple ports and configure the parameters. Click Apply.



Port Config

UNIT1 LAGS

Apply Cancel

☑	PORT	STATUS	REGISTRATION MODE	LEAVEALL TIMER (1000-30000 CENTISECONDS)	JOIN TIMER (20-1000 CENTISECONDS)	LEAVE TIMER (60-3000 CENTISECONDS)	LAG
				1000-30000 centiseconds	20-1000 centiseconds	60-3000 centiseconds	
☑	XGE 1/0/1	● Disable	Normal	1000	20	60	-
☑	2.5GE 1/0/2	● Disable	Normal	1000	20	60	-

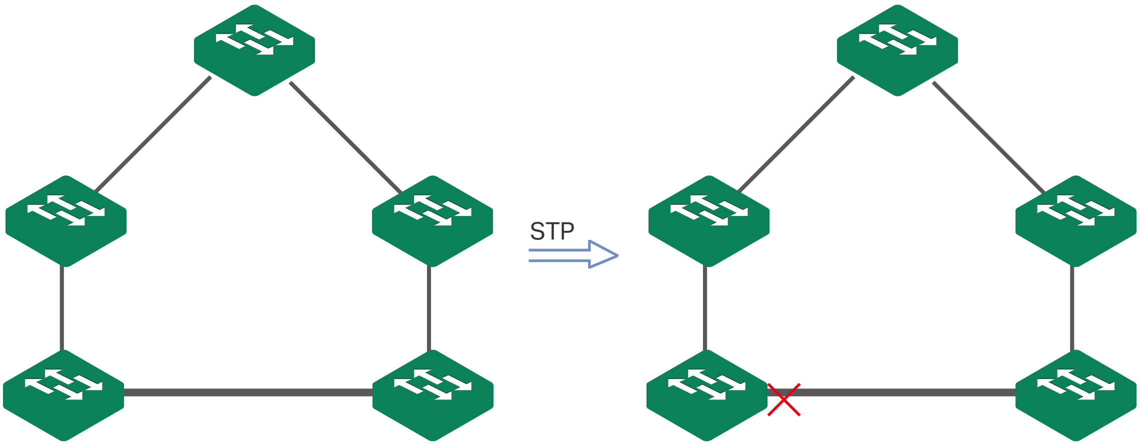
Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the LAG ID.
Status	Enable or disable GVRP on the port. By default, it is disabled.
Registration Mode	Select the GVRP registration mode for the port. Normal: In this mode, the port can dynamically register and deregister VLANs, and transmit both dynamic and static VLAN registration information. Fixed: In this mode, the port is unable to dynamically register and deregister VLANs, and can transmit only the static VLAN registration information. Forbidden: In this mode, the port is unable to dynamically register and deregister VLANs, and can transmit only the information of VLAN 1.
Leaveall Timer (1000-30000 Centiseconds)	When a GARP participant is enabled, the LeaveAll timer will start. When the LeaveAll timer expires, the GARP participant will send LeaveAll messages to request other GARP participants to re-register all its attributes. After that, the participant restarts the LeaveAll timer. The timer ranges from 1000 to 30000 centiseconds and should be an integral multiple of 5. The default value is 1000 centiseconds.
Join Timer (20-1000 Centiseconds)	Join timer controls the sending of Join messages. A GVRP participant starts the Join timer after sending the first Join message. If the participant does not receive any response, it will send the second Join message when the Join timer expires to ensures that the Join message can be sent to other participants. The timer ranges from 20 to 1000 centiseconds and should be an integral multiple of 5. The default value is 20 centiseconds.
Leavel Timer (60-3000 Centiseconds)	The Leave timer controls attribute deregistration. A participant will send a Leave message if it wants other participants to deregister some of its attributes. The participant receiving the message starts the Leave timer. If the participant does not receive any Join message of the corresponding attribute before the Leave timer expires, the participant deregisters the attribute. The timer ranges from 60 to 3000 centiseconds and should be an integral multiple of 5. The default value is 60 centiseconds.
LAG (Only for Unit)	Displays the LAG which the port belongs to.

4. 5 Configure STP

Overview

STP (Spanning Tree Protocol) is a layer 2 Protocol that prevents loops in the network. STP helps block specific ports of the OLTs to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology.

.



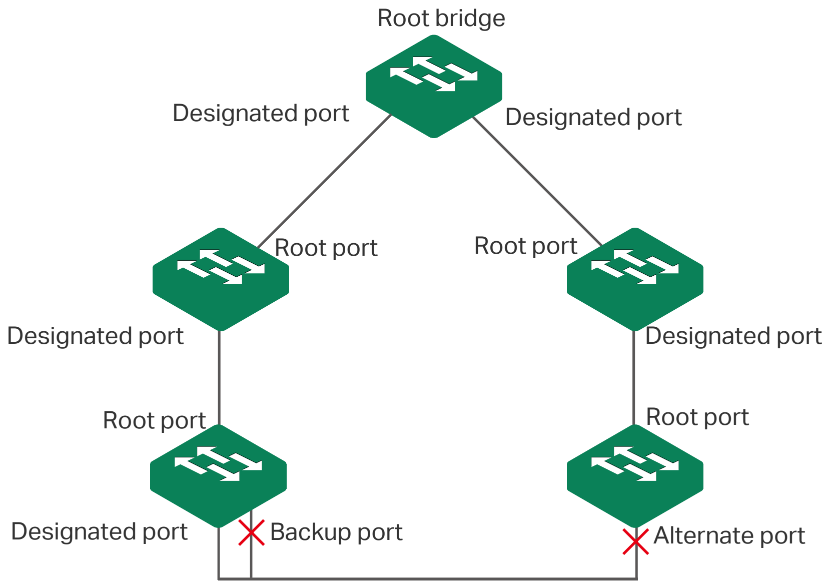
RSTP (Rapid Spanning Tree Protocol) provides the same features as STP. Besides, RSTP can provide much faster spanning tree convergence.

MSTP (Multiple Spanning Tree Protocol) also provides the fast spanning tree convergence as RSTP. In addition, MSTP enables VLANs to be mapped to different spanning trees (MST instances), and traffic in different VLANs will be transmitted along their respective paths, implementing load balancing.

4. 5. 1 Basic Concepts

STP/RSTP Concepts

Based on the networking topology below, this section will introduce some basic concepts in STP/ RSTP.



- **Root Bridge**

The root bridge is the root of a spanning tree. The device with te lowest bridge ID will be the root bridge, and there is only one root bridge in a spanning tree.

- **Bridge ID**

Bridge ID is used to select the root bridge. It is composed of a 2-byte priority and a 6-byte MAC address. The priority is allowed to be configured manually on the OLT, and the device with the lowest priority value will be elected as the root bridge. If the priority of the devices are the same, the device with the smallest MAC address will be selected as the root bridge.

- **Port Role**

  - Root Port

The root port is selected on non-root bridge that can provide the lowest root path cost. There is only one root port in each non-root bridge.

  - Designated Port

The designated port is selected in each LAN segment that can provide the lowest root path cost from that LAN segment to the root bridge.

  - Alternate Port

If a port is not selected as the designated port for it receives better BPDUs from another device, it will become an alternate port.

In RSTP/MSTP, the alternate port is the backup for the root port. It is blocked when the root port works normally. Once the root port fails, the alternate port will become the new root port.

In STP, the alternate port is always blocked.

  - Backup Port

If a port is not selected as the designated port for it receives better BPDUs from the device it belongs to, it will become an backup port.

In RSTP/MSTP, the backup port is the backup for the designated port. It is blocked when the designated port works normally. Once the root port fails, the backup port will become the new designated port.

In STP, the backup port is always blocked.

- Disable Port

The disconnected port with spanning tree function enabled .

Port Status

Generally, in STP, the port status includes: Blocking, Listening, Learning, Forwarding and Disabled.

- **Blocking**

  In this status, the port only receives BPDUs. The other packets are dropped.

- **Listening**

  In this status, the port receives and sends BPDUs. The other packets are dropped.

- **Learning**

  In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, but doesn't forward them.

- **Forwarding**

  In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, and forwards them.

- **Disabled**

  In this status, the port is not in the spanning tree, and drops all the packets it receives.

In RSTP/MSTP, the port status includes: Discarding, Learning and Forwarding. The Discarding status is the grouping of STP's Blocking, Listening and Disabled, and the Learning and Forwarding status correspond exactly to the Learning and Forwarding status specified in STP.

In TP-Link OLTS, the port status includes: Blocking, Learning, Forwarding and Disconnected.

- **Blocking**

  In this status, the port only receives BPDUs. The other packets are dropped.

- **Learning**

  In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, but doesn't forward them.

- **Forwarding**

  In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, and forwards them.

- **Disconnected**

  In this status, the port is enabled with spanning tree function but not connected to any device.

Path Cost

The path cost reflects the link speed of the port. The smaller the value, the higher link speed the port has.

The path cost can be manually configured on each port. If not, the path cost values are automatically calculated according to the link speed as shown below:

Link Speed	Path Cost Value
10Mb/s	2,000,000
100Mb/s	200,000
1Gb/s	20,000
10Gb/s	2,000

Root Path Cost

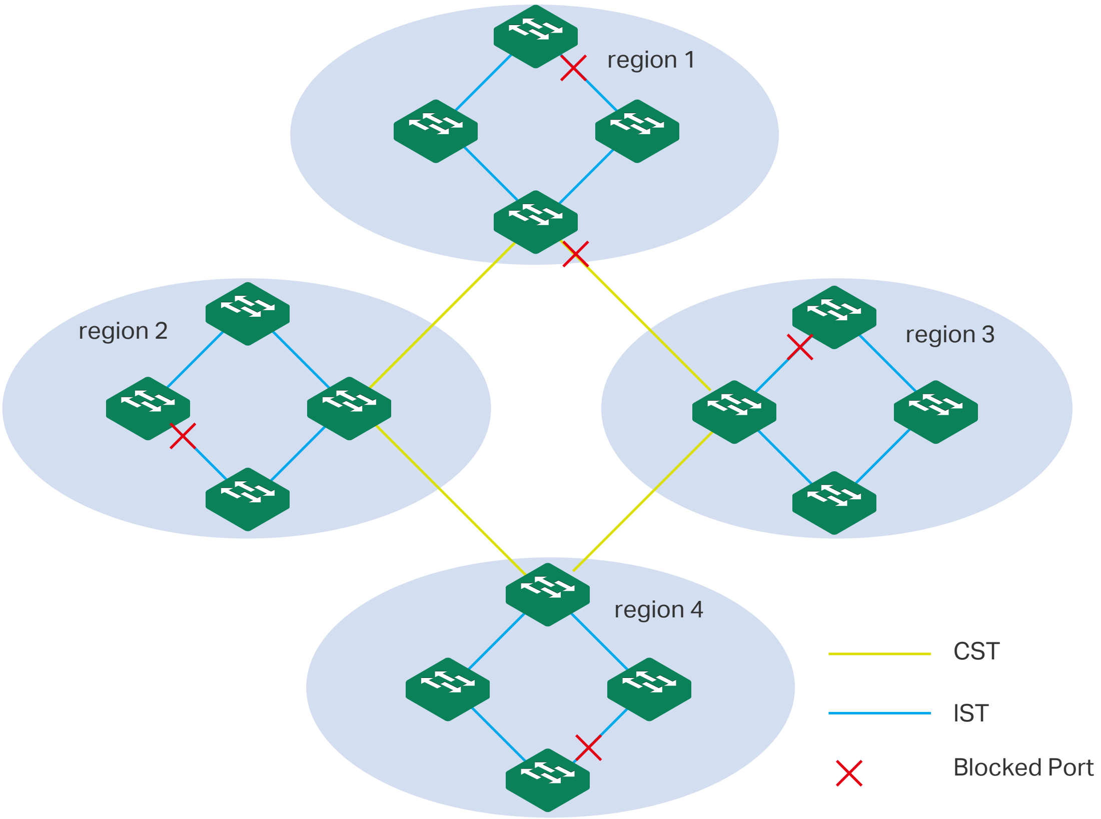
The root path cost is the accumulated path costs from the root bridge to the other devices. When root bridge sends its BPDU, the root path cost value is 0. When an OLT receives this BPDU, the root path cost wll be increased according to the path cost of the receive port. Then it create a new BPDU with the new root file cost and forwards it to the downstream device. The value of the accumulated root path cost increases as the BPDU spreads further.

BPDU

BPDU is a kind of packet that is used to generate and maintain the spanning tree. The BPDUs (Bridge Protocol Data Unit) contain a lot of information, like bridge ID, root path cost, port priority and so on. Devices share these information to help determine the spanning tree topology.

MSTP Concepts

MSTP, compatible with STP and RSTP, has the same basic elements used in STP and RSTP. Based on the networking topology, this section will introduce some concepts only used in MSTP

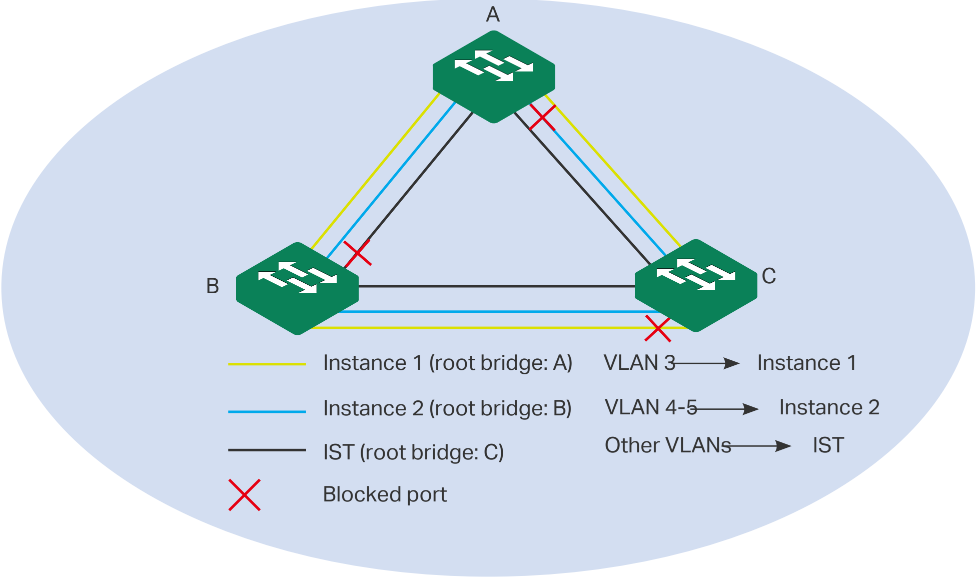


- **MST Region**

An MST region consists of multiple interconnected devices. The devices with the same following characteristics are considered as in the same region: same region name, same revision level, and same VLAN-Instance mapping.

- **MST Instance**

The MST instance is a spanning tree running in the MST region. Multiple MST instances can be established in one MST region and they are independent of each other. As is shown below, there are three instances in a region, and each instance has its own root bridge.



- **VLAN-Instance Mapping**

VLAN-Instance Mapping describes the mapping relationship between VLANs and instances. Multiple VLANs can be mapped to a same instance, but one VLAN can be mapped to only one instance.

- **IST**

The Internal Spanning Tree (IST), which is a special MST instance with an instance ID 0. By default, all the VLANs are mapped to IST.

- **CST**

The Common Spanning Tree (CST), that is the spanning tree connecting all MST regions.

- **CIST**

The Common and Internal Spanning Tree (CIST), comprising IST and CST. CIST is the spanning tree that connects all the devices in the network.

4. 5. 2 STP/RSTP Configuration

Overview

Both STP and RSTP helps block specific ports of the OLTs to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP (Rapid Spanning Tree Protocol) provides the same features as STP, but it can provide much faster spanning tree convergence

Configuration

To configure STP/RSTP, follow these steps:

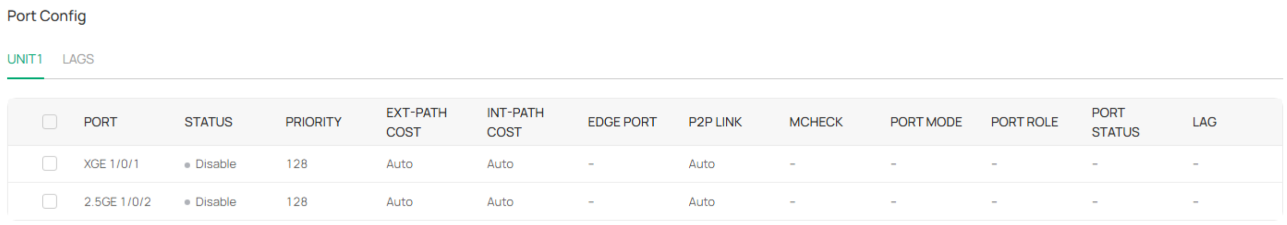
1) Configure STP/RSTP parameters on ports.

2) Configure STP/RSTP globally.

3) Verify the STP/RSTP configurations.

Configure on Ports

Go to L2 Features > STP > Port Config to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Config

UNIT1 LAGS

□	PORT	STATUS	PRIORITY	EXT-PATH COST	INT-PATH COST	EDGE PORT	P2P LINK	MCHECK	PORT MODE	PORT ROLE	PORT STATUS	LAG
□	XGE 1/0/1	● Disable	128	Auto	Auto	-	Auto	-	-	-	-	-
□	2.5GE 1/0/2	● Disable	128	Auto	Auto	-	Auto	-	-	-	-	-

Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the LAG ID.
Status	Enable or disable spanning tree function on the desired port.
Priority	Specify the Priority for the desired port. The value should be an integral multiple of 16, ranging from 0 to 240. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the OLT will compare the port priorities between these port and select a root port with the highest priority.
Ext-Path Cost	Enter the value of the external path cost. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed. For STP/RSTP, external path cost indicates the path cost of the port in spanning tree. The port with the lowest root path cost will be elected as the root port of the OLT. For MSTP, external path cost indicates the path cost of the port in CST.
Int-Path Cost	Enter the value of the internal path cost. The default setting is Auto, which means the port calculates the internal path cost automatically according to the port's link speed. This parameter is only used in MSTP and you need not to configure it if the spanning tree mode is STP/RSTP. For MSTP, internal path cost is used to calculate the path cost in IST. The port with the lowest root path cost will be elected as the root port of the OLT in IST.

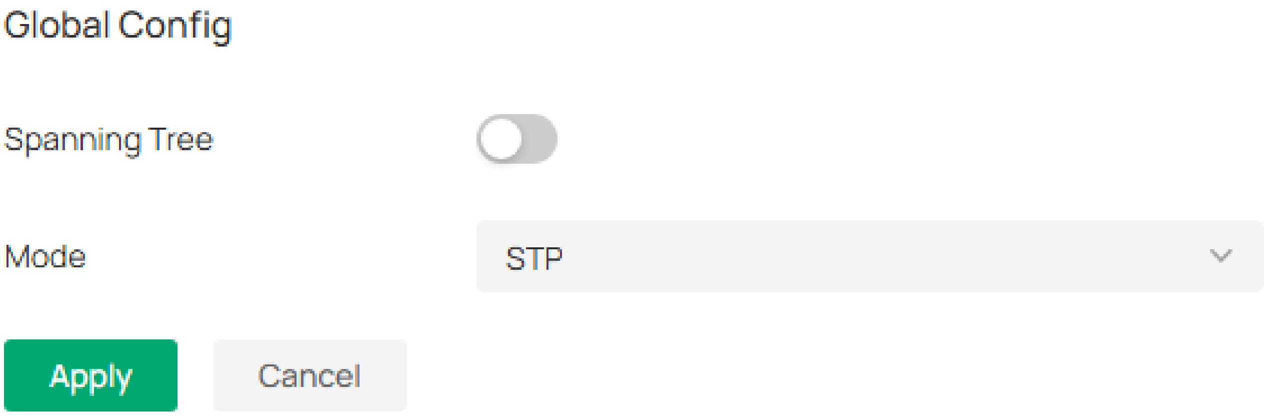
Edge Port	Enable: The port is set as the edge port Disable: The port is not the edge port. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.
P2P Link	Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. By default, it is Auto. Auto: The OLT automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. Open (Force): A port is set as the one that is connected to a P2P link. You should check the link first. Close (Force): A port is set as the one that is not connected to a P2P link. You should check the link first.
MCheck	Select whether to perform MCheck operations on the port. If a port on an RSTP-enabled/MSTP-enabled device is connected to an STP-enabled device, the port will switch to STP compatible mode and send packets in STP format. MCheck is used to switch the mode of the port back to RSTP/MSTP after the port is disconnected from the STP-enabled device. Note that the MCheck configuration can take effect only once, after that the MCheck status of the port will switch to Disabled.
Port Mode	Displays the spanning tree mode of the port. STP: The spanning tree mode of the port is STP. RSTP: The spanning tree mode of the port is RSTP. MSTP: The spanning tree mode of the port is MSTP.
Port Role	Displays the role that the port plays in the spanning tree. Root Port: Indicates that the port is the root port in the spanning tree. It has the lowest path cost from the root bridge to this OLT and is used to communicate with the root bridge. Designated Port: Indicates that the port is the designated port in the spanning tree. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. Alternate Port: Indicates that the port is the alternate port in the spanning tree. It is the backup of the root port or master port. Backup Port: Indicates that the port is the backup port in the spanning tree. It is the backup of the designated port. Disabled: Indicates that the port is not in the spanning tree.

Port Status	Displays the port status. Forwarding: The port only receives BPDUs, and forwards user data. Learning: The port receives and sends BPDUs. It also receives user traffic, but doesn't forward the traffic. Blocking: The port only receives BPDUs. Disconnected: The port has the spanning tree function enabled but is not connected to any device.
LAG (Only for Unit)	Displays the LAG which the port belongs to.

Note: The member ports of an LAG follow the configurations of the LAG and not their own. The individual configurations of the ports can take effect only after the ports leave the LAG.

- **Configure Globally**

1. Go to L2 Features > STP > STP Config to load the following page. In Global Config, enable Spanning Tree and choose the desired Mode (STP or RSTP). Click Apply.



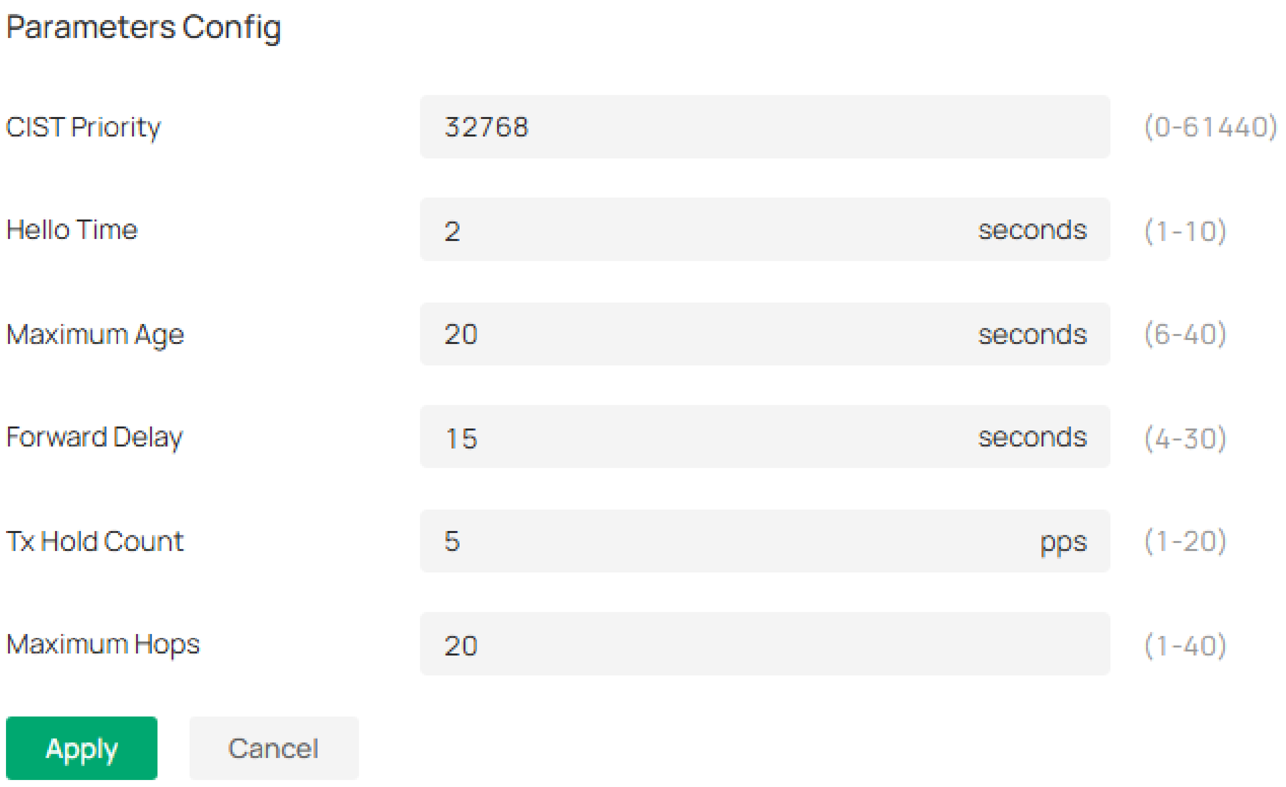
Global Config

Spanning Tree

Mode STP

Spanning Tree	Toggle to enable Spanning Tree feature.
Mode	Select the protocol globally. STP: STP (Spanning Tree Protocol) is a layer 2 Protocol that prevents loops in the network. RSTP: RSTP (Rapid Spanning Tree Protocol) provides the same features as STP, while RSTP can provide much faster spanning tree convergence. MSTP: MSTP (Multiple Spanning Tree Protocol) also provides the fast spanning tree convergence as RSTP. In addition, MSTP enables VLANs to be mapped to different spanning trees (MST instances), and traffic in different VLANs will be transmitted along their respective paths, implementing load balancing.

2. In Parameters Config, configure the parameters. Click Apply.



Parameters Config

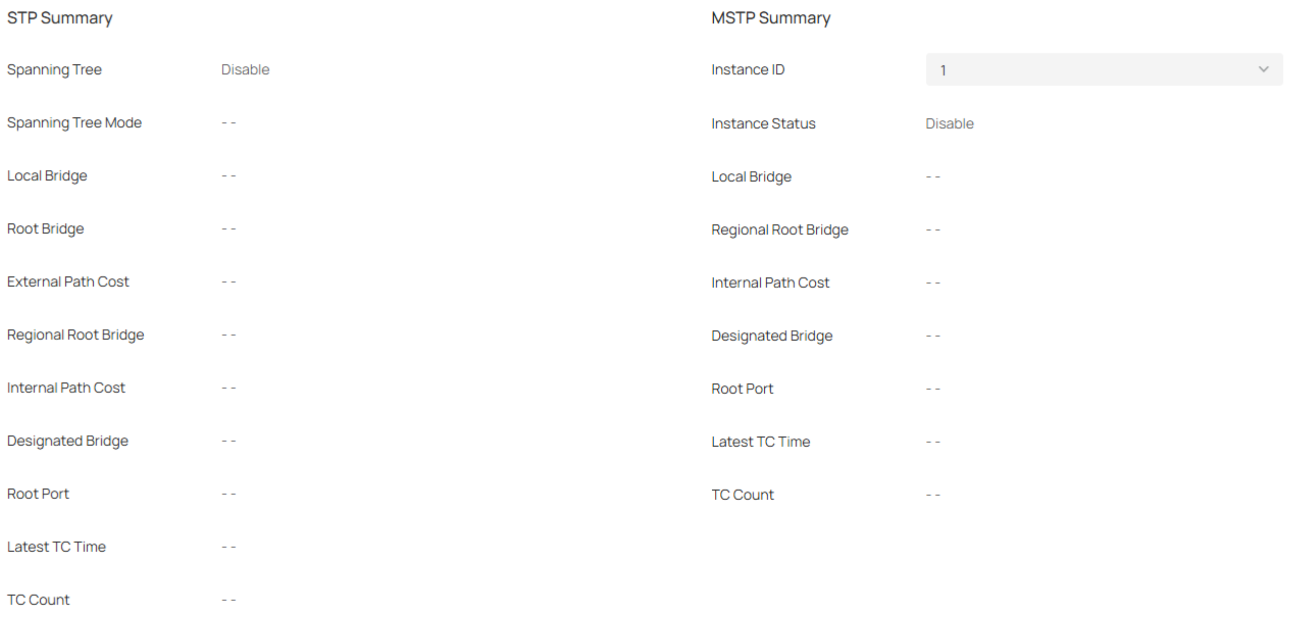
CIST Priority	32768	(0-61440)
Hello Time	2 seconds	(1-10)
Maximum Age	20 seconds	(6-40)
Forward Delay	15 seconds	(4-30)
Tx Hold Count	5 pps	(1-20)
Maximum Hops	20	(1-40)

CIST Priority	Specify the CIST priority for the OLT. CIST priority is a parameter used to determine the root bridge for spanning tree. The OLT with the lower value has the higher priority. In STP/RSTP, CIST priority is the priority of the OLT in spanning tree. The OLT with the highest priority will be elected as the root bridge. In MSTP, CISP priority is the priority of the OLT in CIST. The OLT with the higher priority will be elected as the root bridge in CIST.
Hello Time	Specify the interval between BPDUs' sending. The default value is 2.The root bridge sends configuration BPDUs at an interval of Hello Time. It works with the MAX Age to test the link failures and maintain the spanning tree.
Max Age	Specify the maximum time that the OLT can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The default value is 20.
Forward Delay	Specify the interval between the port state transition from listening to learning. The default value is 15. It is used to prevent the network from causing temporary loops during the regeneration of spanning tree. The interval between the port state transition from learning to forwarding is also the Forward Delay.
Tx Hold Count	Specify the maximum number of BPDU that can be sent in a second. The default value is 5.

Max Hops	Specify the maximum BPDU counts that can be forwarded in a MST region. The default value is 20. An OLT receives BPDU, then decrements the hop count by one and generates BPDUs with the new value. When the hop reaches zero, the OLT will discard the BPDU. This value can control the scale of the spanning tree in the MST region. Max Hops is a parameter configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.

Verify

Go to L2 Features > STP > STP Summary to load the following page. In STP Summary, the summary information of the spanning tree is displayed.



STP Summary

Spanning Tree	Disable
Spanning Tree Mode	- -
Local Bridge	- -
Root Bridge	- -
External Path Cost	- -
Regional Root Bridge	- -
Internal Path Cost	- -
Designated Bridge	- -
Root Port	- -
Latest TC Time	- -
TC Count	- -

MSTP Summary

Instance ID	1
Instance Status	Disable
Local Bridge	- -
Regional Root Bridge	- -
Internal Path Cost	- -
Designated Bridge	- -
Root Port	- -
Latest TC Time	- -
TC Count	- -

Spanning Tree	Displays the status of the spanning tree feature.
Spanning Tree Mode	Displays the spanning tree mode.
Local Bridge	Displays the bridge ID of the local bridge. The local bridge is the current OLT.
Root Bridge	Displays the bridge ID of the root bridge.
External Path Cost	Displays the root path cost from the OLT to the root bridge.
Regional Root Bridge	It is the root bridge of IST. It is not displayed when you choose the spanning tree mode as STP/RSTP.
Internal Path Cost	The internal path cost is the root path cost from the OLT to the root bridge of IST. It is not displayed when you choose the spanning tree mode as STP/RSTP.
Designated Bridge	Displays the bridge ID of the designated bridge. The designated bridge is the OLT that has designated ports.
Root Port	Displays the root port of the current OLT.

Latest TC Time	Displays the latest time when the topology is changed.
TC Count	Displays how many times the topology has changed.

4. 5. 3 MSTP Configuration

Overview

MSTP (Multiple Spanning Tree Protocol) provides the fast spanning tree convergence as RSTP. In addition, MSTP enables VLANs to be mapped to different spanning trees (MST instances), and traffic in different VLANs will be transmitted along their respective paths, implementing load balancing.

Configuration

To configure MSTP, follow these steps:

1) Configure MSTP parameters on ports.

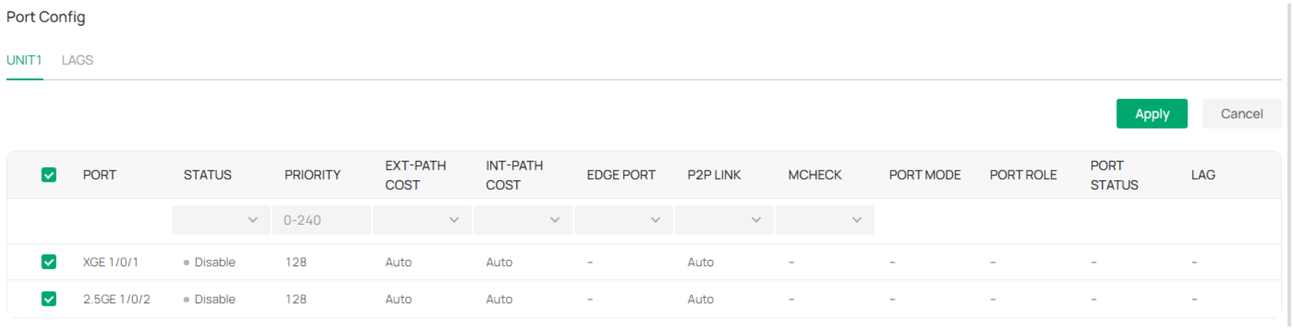
2) Configure MSTP region.

3) Configure MSTP globally.

4) Verify the MSTP configurations.

- **Configure on Ports**

Go to L2 Features > STP > Port Config to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Config

UNIT1 LAGS

Apply Cancel

☑	PORT	STATUS	PRIORITY	EXT-PATH COST	INT-PATH COST	EDGE PORT	P2P LINK	MCHECK	PORT MODE	PORT ROLE	PORT STATUS	LAG
			0-240									
☑	XGE 1/0/1	● Disable	128	Auto	Auto	-	Auto	-	-	-	-	-
☑	2.5GE 1/0/2	● Disable	128	Auto	Auto	-	Auto	-	-	-	-	-

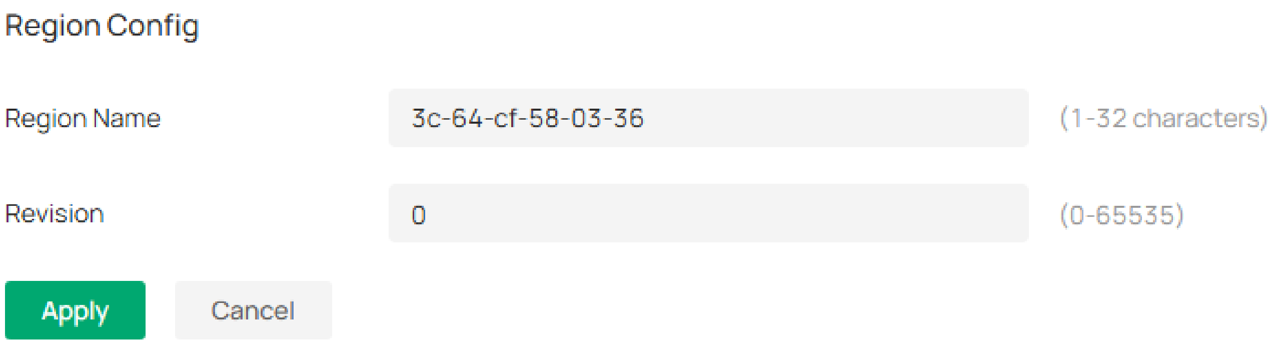
Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the LAG ID.
Status	Enable or disable spanning tree function on the desired port.
Priority	Specify the Priority for the desired port. The value should be an integral multiple of 16, ranging from 0 to 240. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the OLT will compare the port priorities between these port and select a root port with the highest priority.

Ext-Path Cost	Enter the value of the external path cost. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed. For STP/RSTP, external path cost indicates the path cost of the port in spanning tree. The port with the lowest root path cost will be elected as the root port of the OLT. For MSTP, external path cost indicates the path cost of the port in CST.
Int-Path Cost	Enter the value of the internal path cost. The default setting is Auto, which means the port calculates the internal path cost automatically according to the port's link speed. This parameter is only used in MSTP and you need not to configure it if the spanning tree mode is STP/RSTP. For MSTP, internal path cost is used to calculate the path cost in IST. The port with the lowest root path cost will be elected as the root port of the OLT in IST.
Edge Port	Enable: The port is set as the edge port Disable: The port is not the edge port. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.
P2P Link	Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. By default, it is Auto. Auto: The OLT automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. Open (Force): A port is set as the one that is connected to a P2P link. You should check the link first. Close (Force): A port is set as the one that is not connected to a P2P link. You should check the link first.
MCheck	Select whether to perform MCheck operations on the port. If a port on an RSTP-enabled/MSTP-enabled device is connected to an STP-enabled device, the port will switch to STP compatible mode and send packets in STP format. MCheck is used to switch the mode of the port back to RSTP/MSTP after the port is disconnected from the STP-enabled device. Note that the MCheck configuration can take effect only once, after that the MCheck status of the port will switch to Disabled.
Port Mode	Displays the spanning tree mode of the port. STP: The spanning tree mode of the port is STP. RSTP: The spanning tree mode of the port is RSTP. MSTP: The spanning tree mode of the port is MSTP.

Port Role	Displays the role that the port plays in the spanning tree. Root Port: Indicates that the port is the root port in the spanning tree. It has the lowest path cost from the root bridge to this OLT and is used to communicate with the root bridge. Designated Port: Indicates that the port is the designated port in the spanning tree. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. Alternate Port: Indicates that the port is the alternate port in the spanning tree. It is the backup of the root port or master port. Backup Port: Indicates that the port is the backup port in the spanning tree. It is the backup of the designated port. Disabled: Indicates that the port is not in the spanning tree.
Port Status	Displays the port status. Forwarding: The port receives and sends BPDUs, and forwards user data. Learning: The port receives and sends BPDUs. It also receives user traffic, but doesn't forward the traffic. Blocking: The port only receives and sends BPDUs. Disconnected: The port has the spanning tree function enabled but is not connected to any device.
LAG (Only for Unit)	Displays the LAG which the port belongs to.

- **Configure MSTP Region**

1. Go to L2 Features > STP > MSTP Instance to load the following page. In Region Config, configure the parameters. Click Apply.



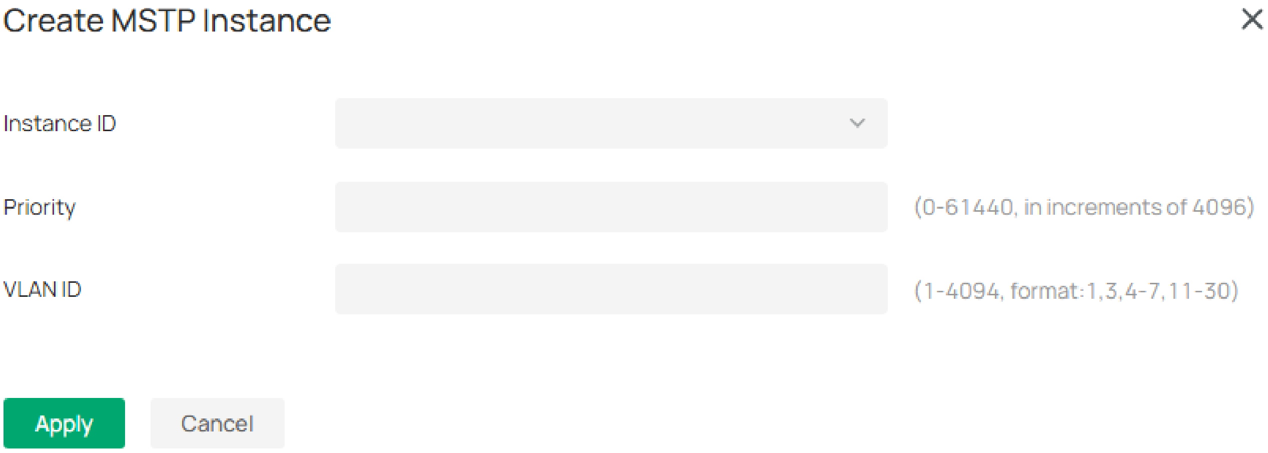
Region Config

Region Name: 3c-64-cf-58-03-36 (1-32 characters)

Revision: 0 (0-65535)

Region Name	Specify the name for an MST region using up to 32 characters. By default, it is the MAC address of the OLT. An MST region consists of multiple interconnected devices. The OLT with the same following characteristics are considered as in the same region: same region name, same revision level, and same VLAN-Instance mapping.
Revision	Enter the revision level of the OLT, By default, it is 0. An MST region consists of multiple interconnected devices. The OLT with the same following characteristics are considered as in the same region: same region name, same revision level, and same VLAN-Instance mapping.

2. In Instance Config, click +Add on the upper right and configure the parameters. Click Create.



Create MSTP Instance

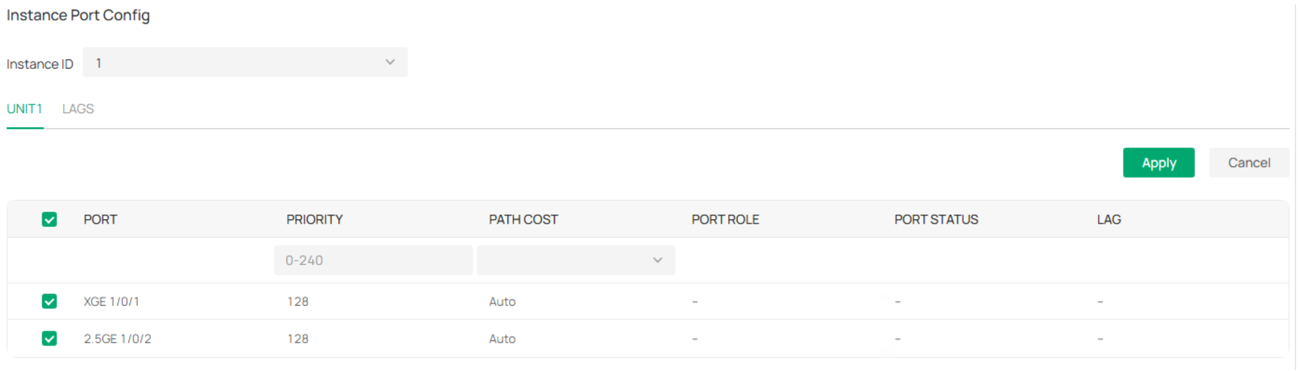
Instance ID

Priority (0-61440, in increments of 4096)

VLAN ID (1-4094, format:1,3,4-7,11-30)

Instance ID	Specify the instance ID.
Priority	Specify the priority for the OLT in the corresponding instance. The value should be an integral multiple of 4096, ranging from 0 to 61440. It is used to determine the root bridge for the instance. OLTs with a lower value have higher priority, and the OLT with the highest priority will be elected as the root bridge in the corresponding instance.
VLAN ID	Enter the VLAN ID. Add: Map the VLAN to the desired instance. Delete: Unbind the VLAN-instance mapping.

3. In Instance Port Config, select one or multiple ports to configure the parameters. Click Apply.



Instance Port Config

Instance ID 1

UNIT1 LAGS

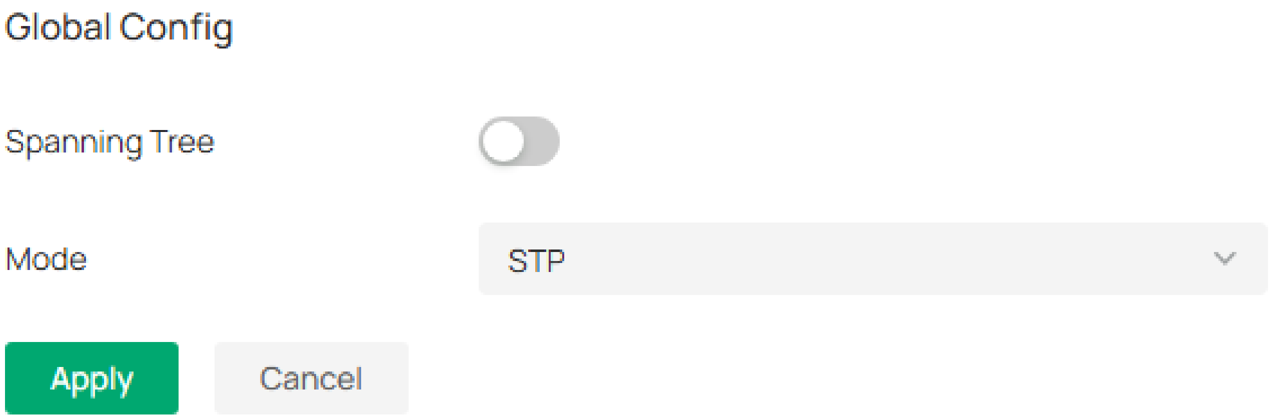
☑	PORT	PRIORITY	PATH COST	PORT ROLE	PORT STATUS	LAG
		0-240				
☑	XGE 1/0/1	128	Auto	-	-	-
☑	2.5GE 1/0/2	128	Auto	-	-	-

Instance ID	Select the ID number of the instance that you want to configure.
Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the LAG ID.
Priority	Specify the Priority for the port in the corresponding instance. The value should be an integral multiple of 16, ranging from 0 to 240. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the OLT will compare the port priorities between these ports and select a root port with the highest priority.
Path Cost	Enter the value of the path cost in the corresponding instance. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed. The port with the lowest root path cost will be elected as the root port of the OLT.
Port Role	Displays the role that the port plays in the desired instance. Root Port: Indicates that the port is the root port in the desired instance. It has the lowest path cost from the root bridge to this OLT and is used to communicate with the root bridge. Designated Port: Indicates that the port is the designated port in the desired instance. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. Alternate Port: Indicates that the port is the alternate port in the desired instance. It is the backup of the root port or master port. Backup Port: Indicates that the port is the backup port in the desired instance. It is the backup of the designated port. Master Port: Indicates the port provides the lowest root path cost from the region to the root bridge in CIST. In CIST, each region is regarded as an OLT, and the master port is the root port of the corresponding region. Disabled: Indicates that the port is not in the spanning tree.

Port Status	Displays the port status. Forwarding: The port receives and sends BPDUs, and forwards user traffic. Learning: The port receives and sends BPDUs. It also receives user traffic, but doesn’t forward the traffic. Blocking: The port only receives and sends BPDUs. Disconnected: The port has the spanning tree function enabled but is not connected to any device.
LAG (Only for Unit)	Displays the LAG which the port belongs to.

- **Configure Globally**

1. Go to L2 Features > STP > STP Config to load the following page. In Global Config, enable Spanning Tree and choose MSTP Mode. Click Apply.



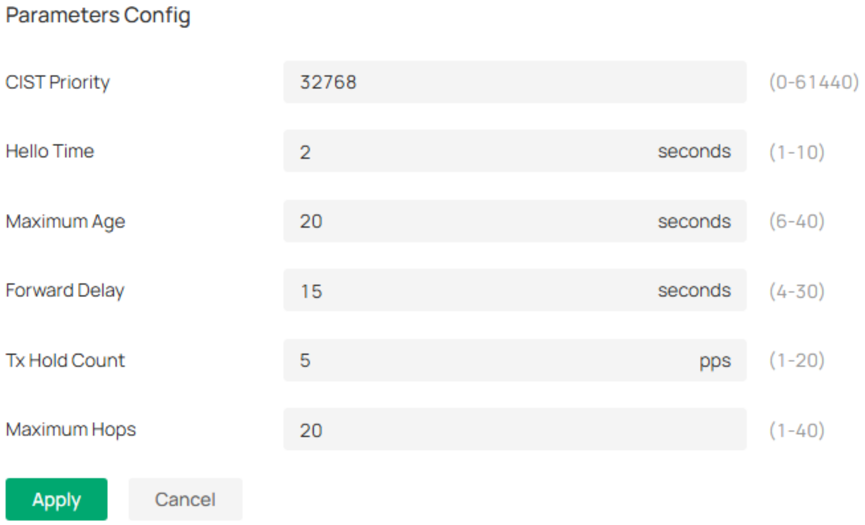
Global Config

Spanning Tree ○

Mode STP

Spanning Tree	Toggle to enable Spanning Tree feature.
Mode	Select the protocol globally. STP: STP (Spanning Tree Protocol) is a layer 2 Protocol that prevents loops in the network. RSTP: RSTP (Rapid Spanning Tree Protocol) provides the same features as STP, while RSTP can provide much faster spanning tree convergence. MSTP: MSTP (Multiple Spanning Tree Protocol) also provides the fast spanning tree convergence as RSTP. In addition, MSTP enables VLANs to be mapped to different spanning trees (MST instances), and traffic in different VLANs will be transmitted along their respective paths, implementing load balancing.

2. In Parameters Config, configure the parameters. Click Apply.



Parameters Config

CIST Priority	32768	(0-61440)
Hello Time	2 seconds	(1-10)
Maximum Age	20 seconds	(6-40)
Forward Delay	15 seconds	(4-30)
Tx Hold Count	5 pps	(1-20)
Maximum Hops	20	(1-40)

CIST Priority

Specify the CIST priority for the OLT. CIST priority is a parameter used to determine the root bridge for spanning tree. The OLT with the lower value has the higher priority.

In STP/RSTP, CIST priority is the priority of the OLT in spanning tree. The OLT with the highest priority will be elected as the root bridge.

In MSTP, CISP priority is the priority of the OLT in CIST. The OLT with the higher priority will be elected as the root bridge in CIST.

Hello Time

Specify the interval between BPDUs' sending. The default value is 2.The root bridge sends configuration BPDUs at an interval of Hello Time. It works with the MAX Age to test the link failures and maintain the spanning tree.

Max Age

Specify the maximum time that the OLT can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The default value is 20.

Forward Delay

Specify the interval between the port state transition from listening to learning. The default value is 15.

It is used to prevent the network from causing temporary loops during the regeneration of spanning tree. The interval between the port state transition from learning to forwarding is also the Forward Delay.

Tx Hold Count

Specify the maximum number of BPDU that can be sent in a second. The default value is 5.

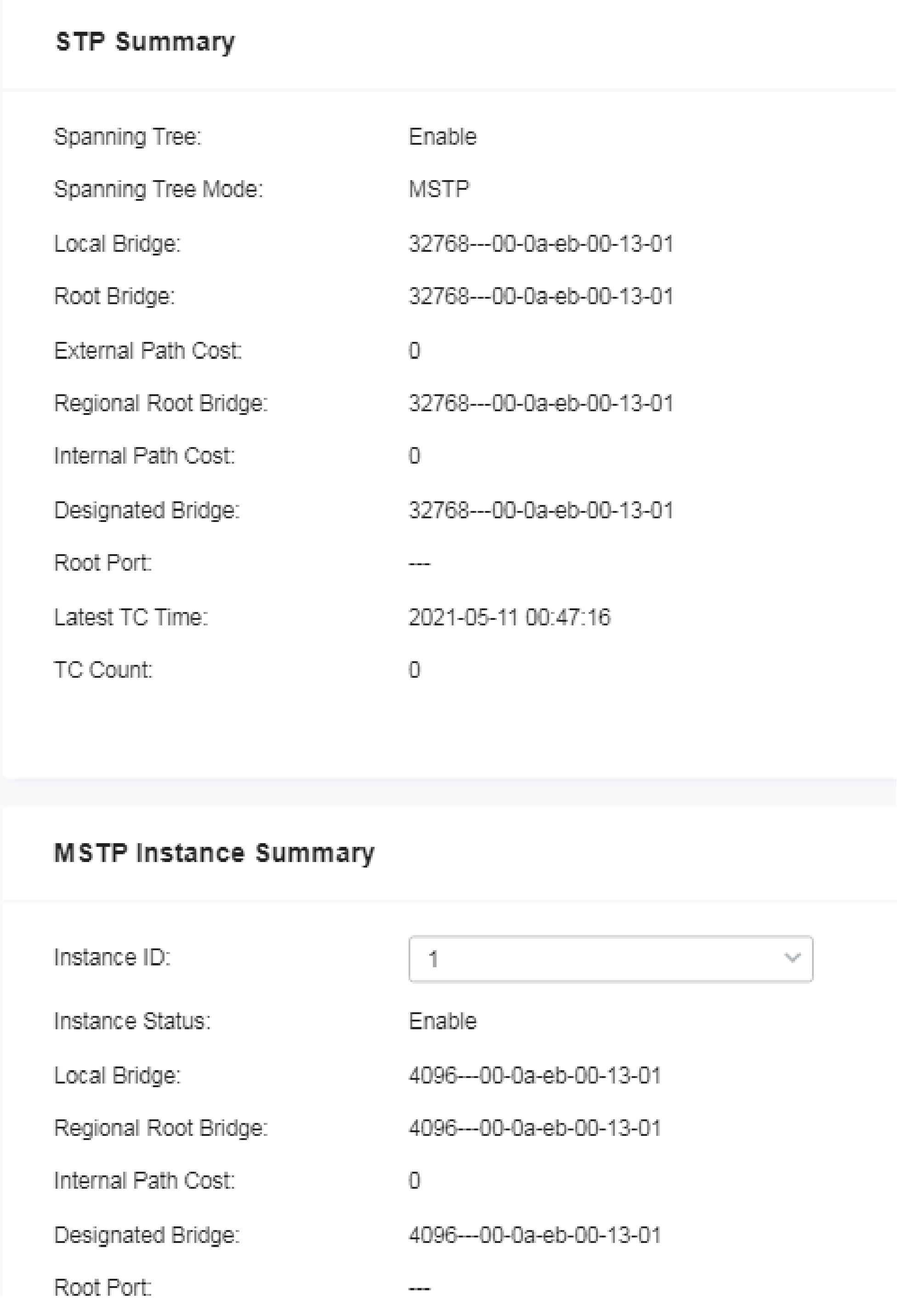
Max Hops

Specify the maximum BPDU counts that can be forwarded in a MST region. The default value is 20. An OLT receives BPDU, then decrements the hop count by one and generates BPDUs with the new value. When the hop reaches zero, the OLT will discard the BPDU. This value can control the scale of the spanning tree in the MST region.

Max Hops is a parameter configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.

- **Verify**

Go to L2 Features > STP > STP Summary to load the following page. The STP Summary shows the summary information of CIST, and n MSTP Instance Summary, the summary information of the spanning tree is displayed.



STP Summary

Spanning Tree:	Enable
Spanning Tree Mode:	MSTP
Local Bridge:	32768---00-0a-eb-00-13-01
Root Bridge:	32768---00-0a-eb-00-13-01
External Path Cost:	0
Regional Root Bridge:	32768---00-0a-eb-00-13-01
Internal Path Cost:	0
Designated Bridge:	32768---00-0a-eb-00-13-01
Root Port:	---
Latest TC Time:	2021-05-11 00:47:16
TC Count:	0

MSTP Instance Summary

Instance ID:	1
Instance Status:	Enable
Local Bridge:	4096---00-0a-eb-00-13-01
Regional Root Bridge:	4096---00-0a-eb-00-13-01
Internal Path Cost:	0
Designated Bridge:	4096---00-0a-eb-00-13-01
Root Port:	---

Spanning Tree	Displays the status of the spanning tree feature.
Spanning Tree Mode	Displays the spanning tree mode.

Local Bridge	Displays the bridge ID of the local bridge. The local bridge is the current OLT.
Root Bridge	Displays the bridge ID of the root bridge in CIST.
External Path Cost	Displays the external root path cost from the OLT to the root bridge in CIST.
Regional Root Bridge	It is the root bridge of IST.
Internal Path Cost	The internal path cost is the root path cost from the OLT to the root bridge of IST.
Designated Bridge	Displays the bridge ID of the designated bridge in CIST.
Root Port	Displays the root port in CIST.
Latest TC Time	Displays the latest time when the topology is changed.
TC Count	Displays how many times the topology has changed.
Instacne ID	Displays the status of the spanning tree feature.
Instance Status	Displays the spanning tree mode.
Local Bridge	Displays the bridge ID of the local bridge. The local bridge is the current OLT.
Regional Root Bridge	Displays the bridge ID of the root bridge.
Internal Path Cost	Displays the root path cost from the OLT to the root bridge.
Designated Bridge	It is the root bridge of IST. It is not displayed when you choose the spanning tree mode as STP/RSTP.
Root Port	Displays the root port of the current OLT.
Latest TC Time	Displays the latest time when the topology is changed.
TC Count	Displays how many times the topology has changed.

4. 5. 4 STP Security

Overview

STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains Loop Protect, Root Protect, BPDU Protect, BPDU Filter and TC Protect functions.

- **Loop Protect**

  Loop Protect function is used to prevent loops caused by link congestions or link failures. It is recommended to enable this function on root ports and alternate ports.

  If the OLT cannot receive BPDUs because of link congestions or link failures, the root port will become a designated port and the alternate port will transit to forwarding status, so loops will occur.

  With Loop Protect function enabled, the port will temporarily transit to blocking state when the port does not receive BPDUs. After the link restores to normal, the port will transit to its normal state, so loops can be prevented.

- **Root Protect**

  Root Protect function is used to ensure that the desired root bridge will not lose its position. It is recommended to enable this function on the designated ports of the root bridge.

  Generally, the root bridge will lose its position once receiving higher-priority BPDUs caused by wrong configurations or malicious attacks. In this case, the spanning tree will be regenerated, and traffic needed to be forwarded along high-speed links may be lead to low-speed links.

  With root protect function enabled, when the port receives higher-priority BDPUs, it will temporarily transit to blocking state. After two times of forward delay, if the port does not receive any higher-priority BDPUs, it will transit to its normal state.

- **BPDU Protect**

  BPDU Protect function is used to prevent the port from receiving BPUDs. It is recommended to enable this function on edge ports.

  Normally edge ports do not receive BPDUs, but if a user maliciously attacks the OLT by sending BPDUs, the system automatically configures these ports as non-edge ports and regenerates the spanning tree.

  With BPDU protect function enabled, the edge port will be shutdown when it receives BPDUs, and reports these cases to the administrator. Only the administrator can restore it.

- **BPDU Filter**

  BPDU filter function is to prevent BPDU flooding in the network. It is recommended to enable this function on edge ports.

  If an OLT receives malicious BPDUs, it forwards these BPDUs to the other devices in the network, and the spanning tree will be continuously regenerated. In this case, the OLT occupies too much CPU or the protocol status of BPDUs is wrong.

With the BPDU Filter function enabled, the port does not forward BPDUs from the other devices.

- **TC Protect**

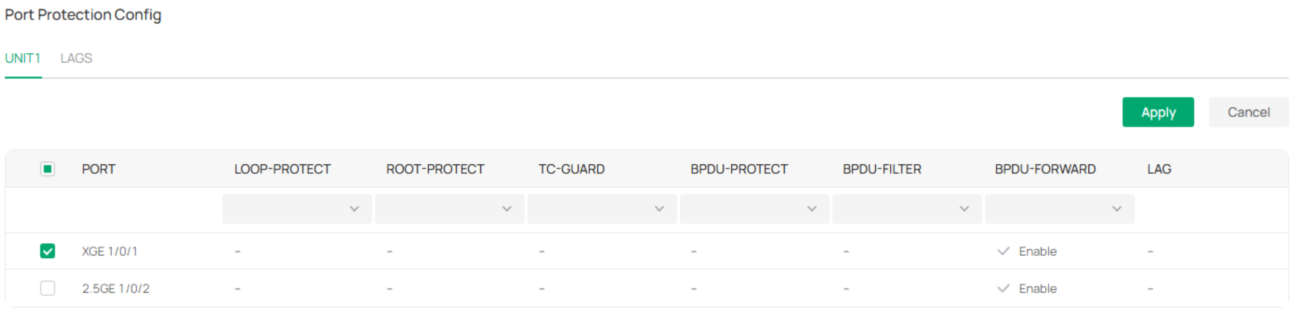
  TC Protect function is used to prevent the OLT from frequently removing MAC address entries. It is recommended to enable this function on the ports of non-root OLTs.

  An OLT removes MAC address entries upon receiving TC-BPDUs (the packets used to announce changes in the network topology). If a user maliciously sends a large number of TC-BPDUs to an OLT in a short period, the OLT will be busy with removing MAC address entries, which may decrease the performance and stability of the network.

  With TC protect function enabled, if the number of the received TC-BPDUs exceeds the maximum number you set in the TC threshold, the OLT will not remove MAC address entries in the TC protect cycle.

Configuration

Go to L2 Features > STP > STP Security to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Protection Config

UNIT1 LAGS

Apply Cancel

■	PORT	LOOP-PROTECT	ROOT-PROTECT	TC-GUARD	BPDU-PROTECT	BPDU-FILTER	BPDU-FORWARD	LAG
☑	XGE 1/0/1	-	-	-	-	-	✓ Enable	-
☐	2.5GE 1/0/2	-	-	-	-	-	✓ Enable	-

Port (Only for Unit)	Displays the port number.
LAG (Only for LAGS)	Displays the LAG ID.
Loop Protect	Enable or disable Loop Protect. It is recommended to enable this function on root ports and alternate ports. When there are link congestions or link failures in the network, the OLT will not receive BPDUs from the upstream device in time. Loop Protect is used to avoid loop caused by the recalculation in this situation. With Loop Protect function enabled, the port will temporarily transit to a blocking state after it does not receive BPDUs in time.

Root Protect	Enable or disable Root Protect. It is recommended to enable this function on the designated ports of the root bridge. OLTs with faulty configurations may produce a higher-priority BPDUs than the root bridge's, and this situation will cause recalculation of the spanning tree. Root Protect is used to ensure that the desired root bridge will not lose its position in the scenario above. With root protect enabled, the port will temporarily transit to blocking state when it receives higher-priority BDPUs. After two forward delays, if the port does not receive any other higher-priority BDPUs, it will transit to its normal state.
TC Guard	Enable or disable the TC Guard function. It is recommended to enable this function on the ports of non-root OLTs. TC Guard function is used to prevent the OLT from frequently changing the MAC address table. With TC Guard function enabled, when the OLT receives TC-BPDUs, it will not process the TC-BPDUs at once. The OLT will wait for a fixed time and process the TC-BPDUs together after receiving the first TC-BPDU, then it will restart timing.
BPDU Protect	Enable or disable the BPDU Protect function. It is recommended to enable this function on edge ports. Edge ports in spanning tree are used to connect to the end devices and it doesn't receive BPDUs in the normal situation. If edge ports receive BPDUs, it may be an attack. BPDU Protect is used to protect the OLT from the attack talked above. With BPDU protect function enabled, the edge ports will be shutdown when they receives BPDUs, and will report these cases to the administrator. Only the administrator can restore the state of the ports.
BPDU Filter	Enable or disable BPDU Filter. It is recommended to enable this function on edge ports. With the BPDU Filter function enabled, the port does not forward BPDUs from the other devices.
BPDU Forward	Enable or disable BPDU Forward. This function only takes effect when the spanning tree function is disabled globally. With BPDU forward enabled, the port can still forward spanning tree BPDUs when the spanning tree function is disabled.
LAG (Only for Unit)	Displays the LAG which the port belongs to.

4. 6 Configure LLDP

Overview

LLDP (Link Layer Discovery Protocol) is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol is a standard IEEE 802.1ab defined protocol and runs over the Layer 2 (the data-link layer) , which allows for interoperability between network devices of different vendors.

With LLDP enabled, the OLT can get its neighbors' information, and network administrators can use the NMS (Network Management System) to gather these information, helping them to know about the network topology, examine the network connectivity and troubleshoot the network faults.

LLDP-MED (LLDP for Media Endpoint Discovery) is an extension of LLDP and is used to advertise information between network devices and media endpoints. It is specially used together with Auto VoIP (Voice over Internet Protocol) to allow VoIP device to access the network. VoIP devices can use LLDP-MED for auto-configuration to minimize the configuration effort.

4. 6. 1 LLDP Configuration

Overview

LLDP allows the local device to encapsulate its management address, device ID, interface ID and other information into a LLDPDU (Link Layer Discovery Protocol Data Unit) and periodically advertise this LLDPDU to its neighbor devices. The neighbors store the received LLDPDU in a standard MIB (Management Information Base), making it possible for the information to be accessed by a NMS (Network Management System) using a management protocol such as the SNMP (Simple Network Management Protocol).

Configuration

To configure LLDP, follow these steps:

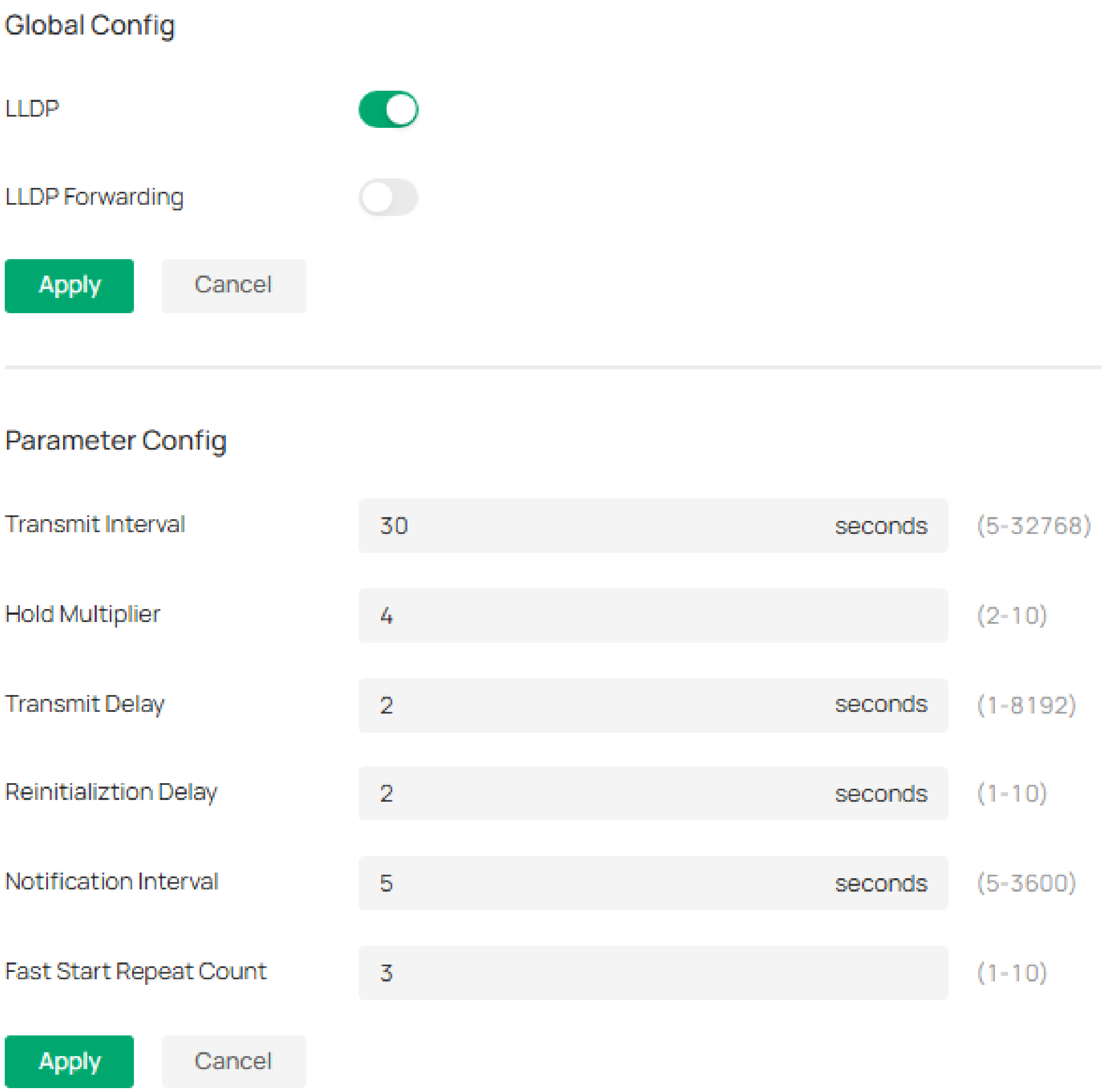
1) Configure LLDP feature globally.

2) Configure LLDP on ports.

3) View the LLDP settings.

- **Configure Globally**

1. Go to L2 Features > LLDP > LLDP Config > Global Config to load the following page. In the Global Config section, enable LLDP. You can also enable the OLT to forward LLDP messages when LLDP function is disabled. Click Apply.



Global Config

LLDP ●

LLDP Forwarding ○

Parameter Config

Transmit Interval	30 seconds	(5-32768)
Hold Multiplier	4	(2-10)
Transmit Delay	2 seconds	(1-8192)
Reinitializtion Delay	2 seconds	(1-10)
Notification Interval	5 seconds	(5-3600)
Fast Start Repeat Count	3	(1-10)

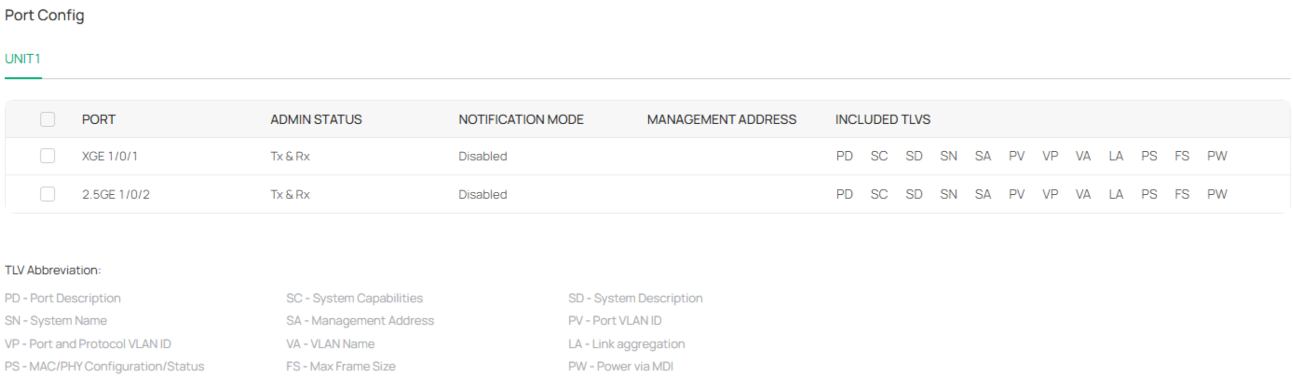
2. In the Parameter Config section, configure the parameters. Click Apply.

LLDP	Enable LLDP function globally.
LLDP Forwarding	(Optional) Enable the OLT to forward LLDP messages when LLDP function is disabled.
Transmit Interval	Enter the interval between successive LLDP packets that are periodically sent from the local device to its neighbors. The default is 30 seconds.
Hold Multiplier	This parameter is a multiplier on the Transmit Interval that determines the actual TTL (Time To Live) value used in an LLDP packet. TTL is the duration that the neighbor device should hold the received LLDP packet before discarding it. The default value is 4. TTL= Hold Multiplier * Transmit Interval.

Transmit Delay	Specify the amount of time that the local device waits before sending another LLDP packet to its neighbor. When the local information changes, the local device will send LLDP packets to inform its neighbors. If frequent changes occur to the local device, LLDP packets will flood. After specifying a transmit delay time, the local device will wait for a delay time to send LLDP packets when changes occur to avoid frequent LLDP packet forwarding. The default is 2 seconds..
Reinitialization Delay	Specify the amount of delay from when Admin Status of ports becomes “Disable’ until reinitialization will be attempted. The default value is 2 seconds.
Notification Interval	Enter the interval between successive in seconds Trap messages that are periodically sent from the local device to the NMS. The default value is 5.
Fast Start Repeat Count	Specify the number of LLDP packets that the local port sends when its Admin Status changes from Disable (or Rx_Only) to Tx&RX (or Tx_Only). The default value is 3. In this case, the local device will shorten the Transmit Interval of LLDP packets to 1 second to make it quickly discovered by its neighbors. After the specified number of LLDP packets are sent, the Transmit Interval will be restored to the specified value.

- **Configure on Ports**

Go to L2 Features > LLDP > LLDP Config > Port Config to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Config

UNIT1

☐	PORT	ADMIN STATUS	NOTIFICATION MODE	MANAGEMENT ADDRESS	INCLUDED TLVS
☐	XGE 1/0/1	Tx & Rx	Disabled		PD SC SD SN SA PV VP VA LA PS FS PW
☐	2.5GE 1/0/2	Tx & Rx	Disabled		PD SC SD SN SA PV VP VA LA PS FS PW

TLV Abbreviation:

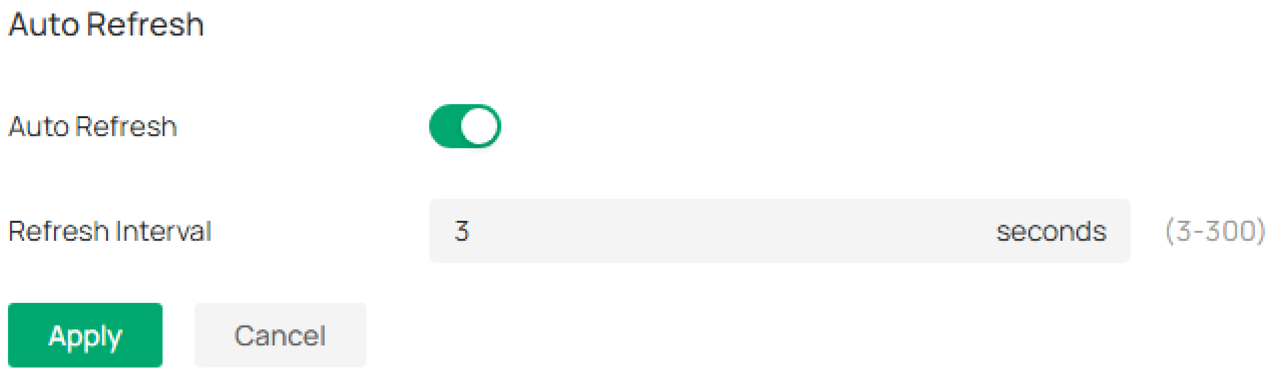
PD - Port Description	SC - System Capabilities	SD - System Description
SN - System Name	SA - Management Address	PV - Port VLAN ID
VP - Port and Protocol VLAN ID	VA - VLAN Name	LA - Link aggregation
PS - MAC/PHY Configuration/Status	FS - Max Frame Size	PW - Power via MDI

Port	Displays the port ID.
Admin Status	Set Admin Status for the port to deal with LLDP packets. Tx&Rx: The port transmits LLDP packets and receives LLDP packets. Rx_Only: The port only receives LLDP packets. Tx_Only: The port only transmits LLDP packets. Disable: The port will not transmit LLDP packets or drop the received LLDP packets.
Notification Mode	(Optional) Enable the OLT to send trap messages to the NMS when the information of the neighbor device connected to this port changes.

Management Address	Specify the Management IP address of the port to be notified to the neighbor. Value 0.0.0.0 means the port will notify its default management address to the neighbor.
Included TLVs (Type/Length/Value)	Configure the TLVs included in the outgoing LLDP packets. PD: Used to advertise the port description defined by the IEEE 802 LAN station. SC: Used to advertise the supported functions and whether or not these functions are enabled. SD: Used to advertise the system's description including the full name and version identification of the system's hardware type, software operating system, and networking software. SN: Used to advertise the system name. SA: Used to advertise the local device's management address to make it possible to be managed by SNMP. PV: Used to advertise the 802.1Q VLAN ID of the port. VP: Used to advertise the protocol VLAN ID of the port. VA: Used to advertise the name of the VLAN which the port is in. LA: Used to advertise whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the port ID when it is in an aggregation. PS: Used to advertise the port's attributes including the duplex and bit-rate capability of the sending IEEE 802.3 LAN node that is connected to the physical medium, the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node and whether these settings are the result of auto-negotiation during link initiation or of manual set override action. FS: Used to advertise the maximum frame size capability of the implemented MAC and PHY. PW: Used to advertise the port's PoE (Power over Ethernet) support capabilities.

- **View Local Info**

1. Go to L2 Features > LLDP > LLDP Config > Local Info to load the following page. In Auto Refresh, enable Auto Refresh feature and set the Refresh Interval based on needs.



Auto Refresh

Auto Refresh: enabled

Refresh Interval: 3 seconds (3-300)

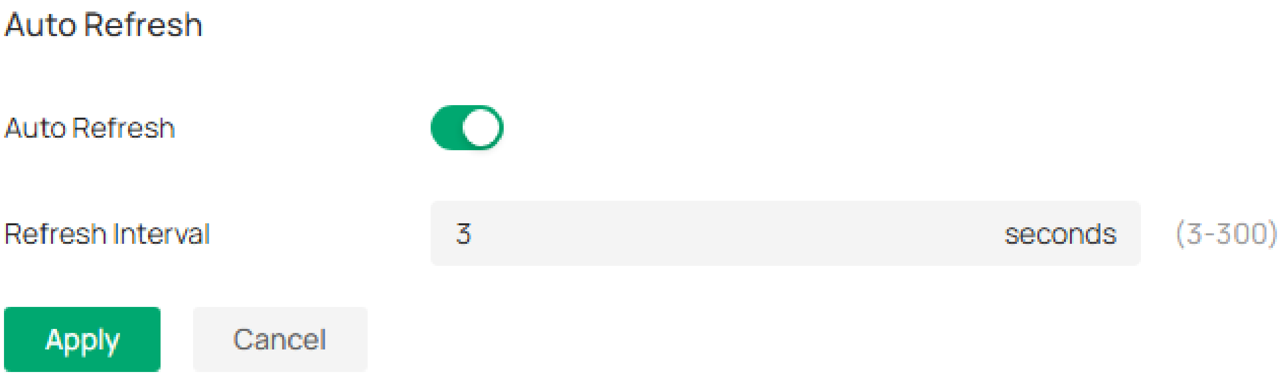
2. In Local Info, select the desired port and view its associated local device information.

Local Interface	Displays the local port ID.
Chassis ID Subtype	Displays the Chassis ID type.
Chassis ID	Displays the value of the Chassis ID.
Port ID Subtype	Displays the Port ID type.
Port ID	Displays the value of the Port ID.
TTL	Specify the amount of time in seconds the neighbor device should hold the received information before discarding it.
Port Description	Displays the description of the local port.
System Name	Displays the system name of the local device.
System Description	Displays the system description of the local device.
System Capabilities Supported	Displays the supported capabilities of the local system.
System Capabilities Enabled	Displays the primary functions of the local device.
Management Address Type	Displays the management IP address type of the local device.
Management Address	Displays the management IP address of the local device.
Management Address Interface Type	Displays the interface numbering type that is used to define the interface ID.
Management Address Interface ID	Displays the interface ID that is used to identify the specific interface associated with the MAC address of the local device.
Management Address OID	Displays the OID (Object Identifier) of the local device. A value of 0 means that the OID is not provided.
Port VLAN ID(PVID)	Displays the PVID of the local port.
Port And Protocol VLAN ID(PPVID)	Displays the PPVID of the local port.
Port And Protocol Supported	Displays whether the local device supports port and protocol VLAN feature.
Port And Protocol VLAN Enabled	Displays the status of the port and protocol VLAN feature.

VLAN Name of VLAN 1	Displays the VLAN name of VLAN 1 for the local device.
Protocol Identify	Displays the particular protocol that the local device wants to advise.
Auto-negotiation Supported	Displays whether the local device supports auto-negotiation.
Auto-Negotiation Enable	Displays the status of auto-negotiation for the local device.
OperMau	Displays the OperMau (Optional Mau) field of the TLV configured by the local device.
Link Aggregation Supported	Displays whether the local device supports link aggregation.
Link Aggregation Enabled	Displays the status of link aggregation fot the local device.
Aggregation Port ID	Displays the aggregation port ID of the local device.
Power Port Class	Displays the power port class of the local device.
PSE Power Supported	Displays whether the local device supports PSE power.
PSE Power Enabled	Displays the status of PSE power for the local device.
PSE Pairs Control Ability	Displays whether the PSE pairs can be controlled for the local device.
Maximum Frame Size	Displays the maximum frame size supported by the local device.

- **View Neighbor Info**

1. Go to L2 Features > LLDP > LLDP Config > Neighbor Info to load the following page. In Auto Refresh, enable Auto Refresh feature and set the Refresh Interval based on needs.



Auto Refresh

Auto Refresh ●

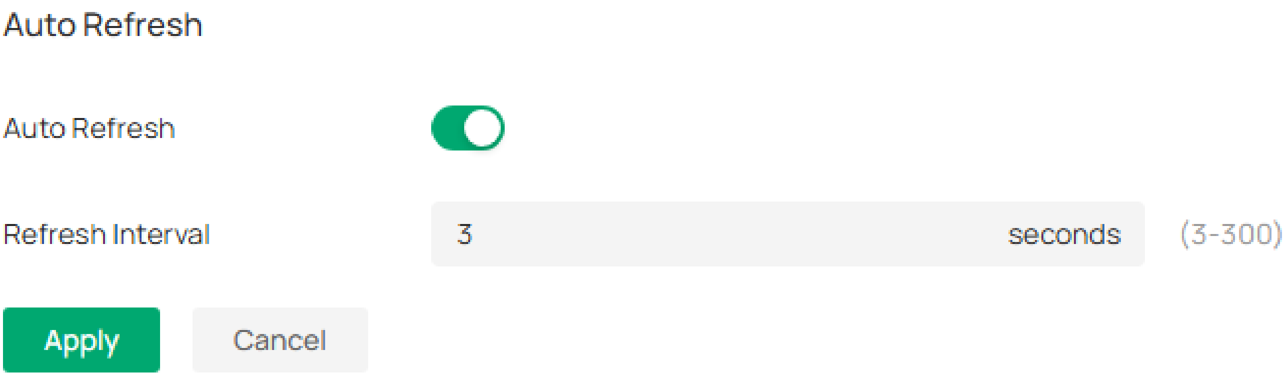
Refresh Interval: 3 seconds (3-300)

2. In Neighbor Info, select the desired port and view its associated neighbor device information.

System Name	Displays the system name of the neighbor device.
Chassis ID	Displays the Chassis ID of the neighbor device.
System Description	Displays the system description of the neighbor device.
Neighbor Port	Displays the port ID of the neighbor device which is connected to the local port.
Information	Click to view the details of the neighbor device.

- **View LLDP Statistics**

1. Go to L2 Features > LLDP > LLDP Config > Statistics Info to load the following page. In Auto Refresh, enable Auto Refresh feature and set the Refresh Interval based on needs.

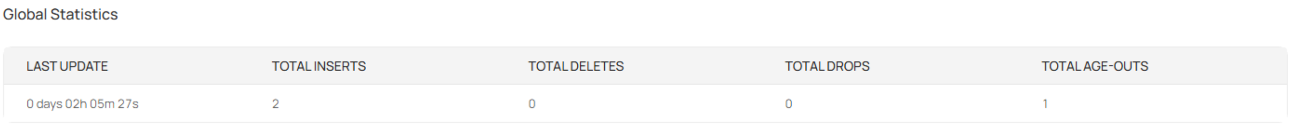


Auto Refresh

Auto Refresh: On

Refresh Interval: 3 seconds (3-300)

2. In Global Statistics, view the global statistics of the local device.

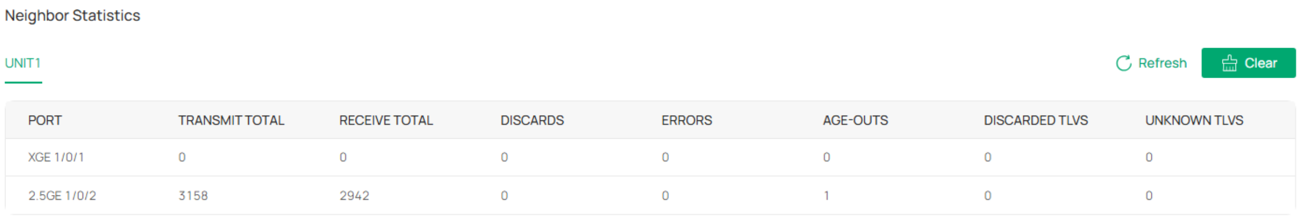


Global Statistics

LAST UPDATE	TOTAL INSERTS	TOTAL DELETES	TOTAL DROPS	TOTAL AGE-OUTS
0 days 02h 05m 27s	2	0	0	1

Last Update	Displays the time since last statistics update.
Total Inserts	Displays the total number of neighbors during latest update time.
Total Deletes	Displays the number of neighbors deleted by the local device. The port will delete neighbors when the port is disabled or the TTL of the LLDP packets sent by the neighbor is 0.
Total Drops	Displays the number of neighbors dropped by the local device. Each port can learn a maximum of 80 neighbor devices, and the subsequent neighbors will be dropped when the limit is reached.
Total Ageouts	Displays the latest number of neighbors that have aged out on the local device.

3. In Neighbor Statistics, view the statistics of the corresponding port.



Neighbor Statistics

PORT	TRANSMIT TOTAL	RECEIVE TOTAL	DISCARDS	ERRORS	AGE-OUTS	DISCARDED TLVS	UNKNOWN TLVS
XGE 1/0/1	0	0	0	0	0	0	0
2.5GE 1/0/2	3158	2942	0	0	1	0	0

Port	Displays the port ID.
Transmit Total	Displays the total number of the LLDP packets sent via the port.
Receive Total	Displays the total number of the LLDP packets received via the port.
Discards	Displays the total number of the LLDP packets discarded by the port.
Errors	Displays the total number of the error LLDP packets received via the port.
Ageouts	Displays the number of the aged out neighbors that are connected to the port.
TLV Discards	Displays the total number of the TLVs discarded by the port when receiving LLDP packets.
TLV Unknowns	Displays the total number of the unknown TLVs included in the received LLDP packets.

4. 6. 2 LLDP-MED Configuration

Overview

LLDP-MED allows the network device to send its information including Auto VoIP information, PoE (Power over Ethernet) capacity to the media endpoint devices (for example, IP phones) for auto-configuration. The media endpoint devices receive the Auto VoIP information and finish the auto-configuration, then send the voice traffic with the desired configuration, which can provide preferential treatment to the voice traffic.

Configuration

To configure LLDP-MED, follow these steps:

1) Configure LLDP feature.

2) Configure LLDP-MED fast repeat count globally.

3) Enable and Configure the LLDP-MED feature on the port.

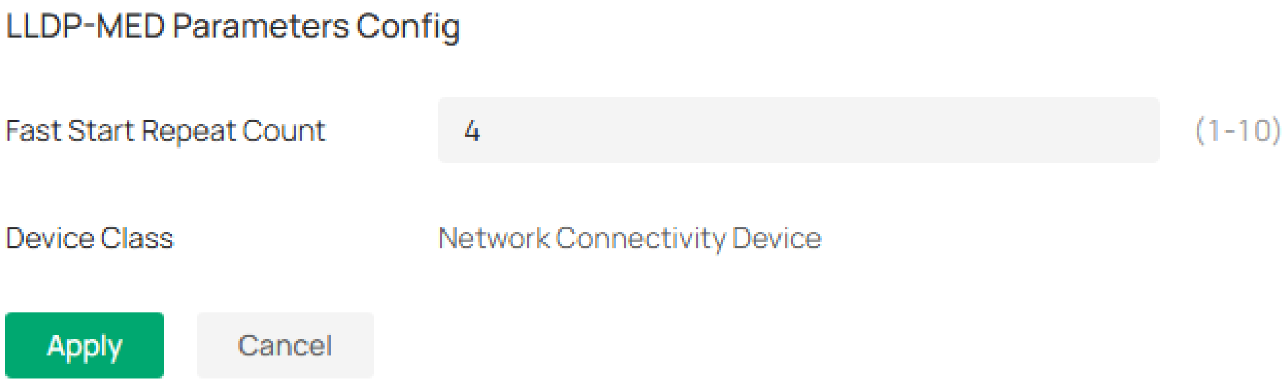
4) View the LLDP-MED settings.

- **Configure LLDP**

Go to L2 Features > LLDP > LLDP Config > Global Config to configure the LLDP feature. For details, refer to 44. 6. 1 LLDP Configuration.

- **Configure Fast Start Repeat Count**

Go to L2 Features > LLDP > LLDP Config >LLDP-MED Config > Global Config to load the following page. Configure the parameters. Click Apply.



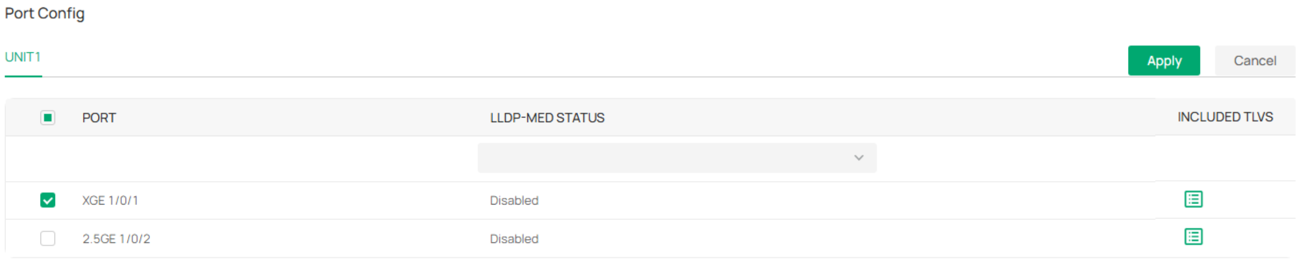
LLDP-MED Parameters Config

Fast Start Repeat Count	4	(1-10)
Device Class	Network Connectivity Device	

Fast Start Repeat Count	Specify the number of successive LLDP-MED packets that the OLT sends when it receives the LLDP-MED packets from the neighbor endpoints. The default is 4. When the OLT receives LLDP-MED packets from the neighbor endpoints for the first time, it will send the specified number of LLDP-MED packets carrying LLDP-MED information. After that, the Transmit Interval will be restored to the specified value you set in Parameter Config in LLDP Config > Global Config.
Device Class	Display the current device class. LLDP-MED defines two device classes, Network Connectivity Device and Endpoint Device. An OLT is a Network Connectivity device.

- **Configure on Ports**

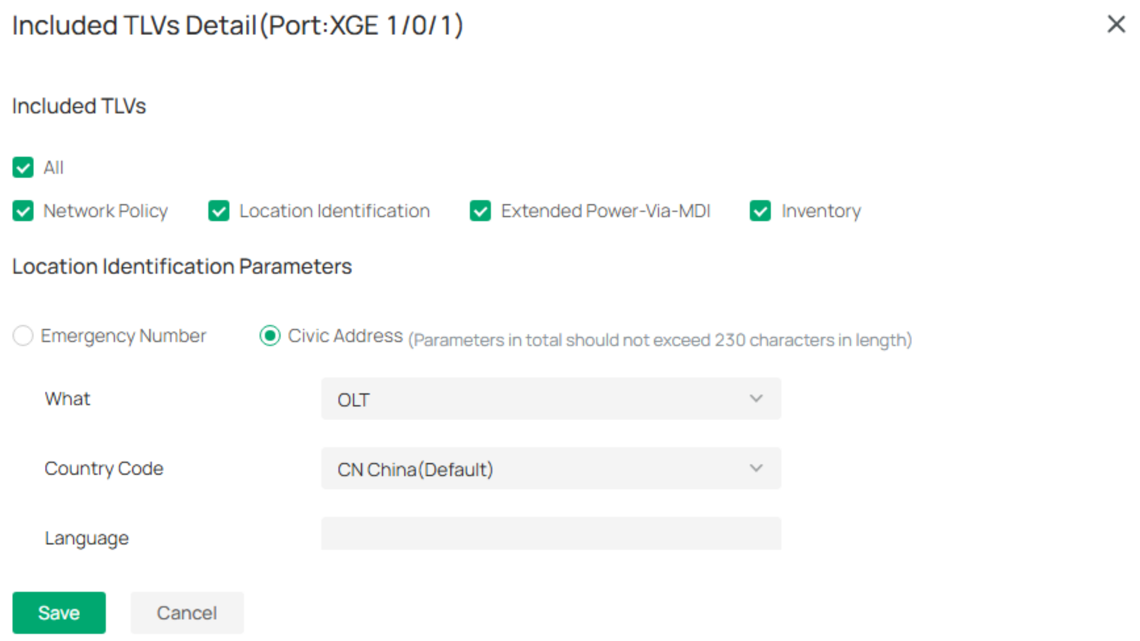
1. Go to L2 Features > LLDP > LLDP-MED Config > Port Config to load the following page. Choose the desired port to enable it in LLDP-MED Status. Click Apply.



Port Config

■	PORT	LLDP-MED STATUS	INCLUDED TLVS
☑	XGE 1/0/1	Disabled	☰
☐	2.5GE 1/0/2	Disabled	☰

2. Click ☰ in the Included TLVS Column to load the following page and configure the parameter. Click Save.



Included TLVs Detail(Port:XGE 1/0/1) ×

Included TLVs

☑ All

☑ Network Policy ☑ Location Identification ☑ Extended Power-Via-MDI ☑ Inventory

Location Identification Parameters

○ Emergency Number ● Civic Address (Parameters in total should not exceed 230 characters in length)

What: OLT

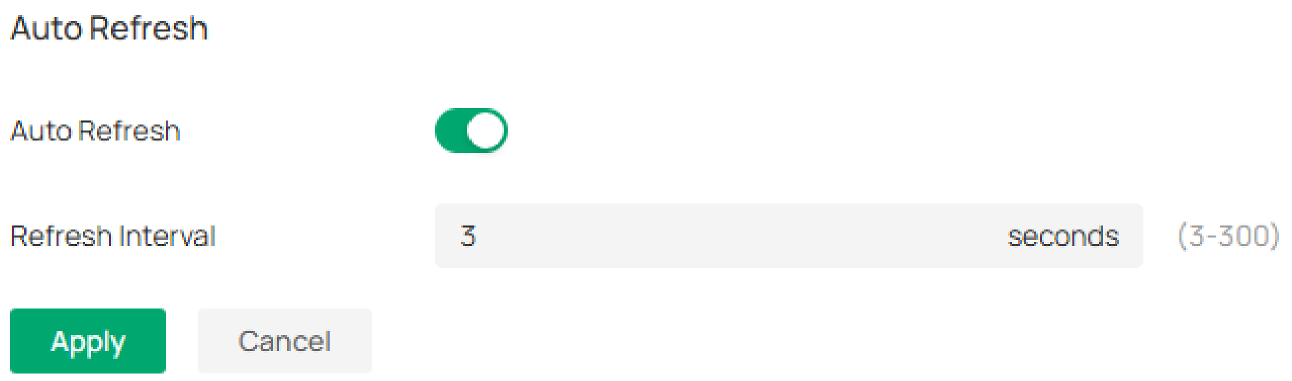
Country Code: CN China(Default)

Language:

Included TLVs	Network Policy: Used to advertise VLAN configuration and the associated Layer 2 and Layer 3 attributes of the port to the Endpoint devices. Location Identification: Used to assign the location identifier information to the Endpoint devices. If this option is selected, you can configure the emergency number and the detailed address of the endpoint device in the Location Identification Parameters section. Extended Power-Via-MDI: Used to advertise the detailed PoE information including power supply priority and supply status between LLDP-MED Endpoint devices and Network Connectivity devices. Inventory: Used to advertise the inventory information. The Inventory TLV set contains seven basic Inventory management TLVs: Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV and Asset ID TLV.
Emergency Number (Only for Local Identification)	Configure the emergency number to call CAMA or PSAP. The number should contain 10-25 characters.
Civic Address (Only for Local Identification)	Configure the address of the audio device in the IETF defined address format, and enter the address details accordingly. What: Specify the role type of the local device, DHCP Server, OLT or LLDP-MED Endpoint.

- View Local Info

1. Go to L2 Features > LLDP > LLDP-MED Config > Local Info to load the following page. In Auto Refresh, enable Auto Refresh feature and set the Refresh Interval based on needs.



Auto Refresh

Auto Refresh

Refresh Interval 3 seconds (3-300)

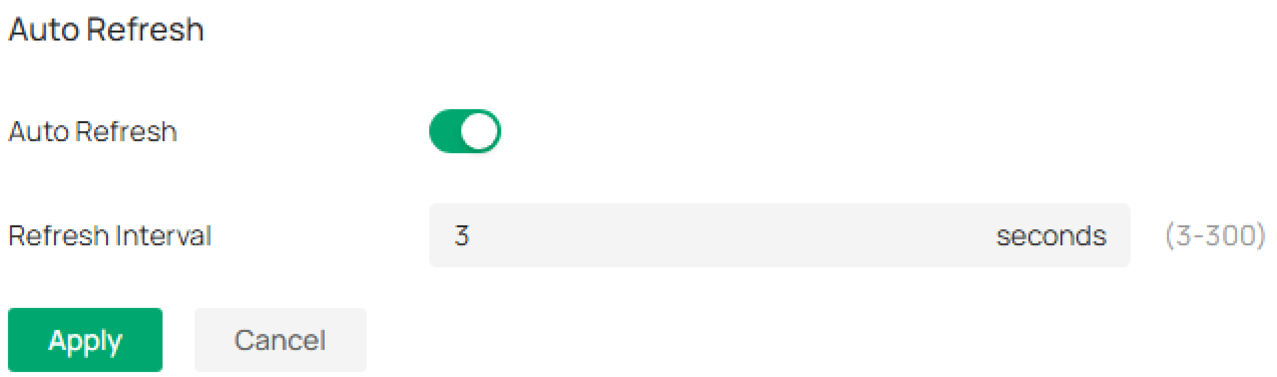
2. In Local Info, select the desired port and view the LLDP-MED local information.

Local Interface	Displays the local port ID.
Device Type	Displays the local device type defined by LLDP-MED.
Application Type	Displays the supported applications of the local device.
Unknown Policy Flag	Displays the unknown location settings included in the network policy TLV.
VLAN tagged	Displays the VLAN Tag type of the applications, tagged or untagged.
Media Policy VLAN ID	Displays the 802.1Q VLAN ID of the port.
Media Policy Layer 2 Priority	Displays the Layer 2 priority used in the specific application.
Media Policy DSCP	Displays the DSCP value used in the specific application.
Location Data Format	Displays the Location ID data format of the local device.
What	Displays the type of the local device.
Country Code	Displays the country code of the local device.
Power Type	Displays the whether the local device is a PSE device or PD device.
Power Source	Displays the power source of the local device.
Power Priority	Displays the power priority of the local device, which represents the priority of power that is received by the PD devices, or the priority of power that the PSE devices supply.
Power Value	Displays the power required by the PD device or supplied by the PSE device.
Hardware Revision	Displays the hardware revision of the local device.
Firmware Revision	Displays the firmware revision of the local device.

Software Revision	Displays the software revision of the local device.
Serial Number	Displays the serial number of the local device.
Manufacturer Name	Displays the manufacturer name of the local device.
Model Name	Displays the model name of the local device.
Asset ID	Displays the asset ID of the local device.
Auto-negotiation Supported	Displays whether the local device supports auto-negotiation.
Auto-Negotiation Enable	Displays the status of auto-negotiation for the local device.
OperMau	Displays the OperMau (Optional Mau) field of the TLV configured by the local device.
Link Aggregation Supported	Displays whether the local device supports link aggregation.
Link Aggregation Enabled	Displays the status of link aggregation for the local device.
Aggregation Port ID	Displays the aggregation port ID of the local device.
Power Port Class	Displays the power port class of the local device.
PSE Power Supported	Displays whether the local device supports PSE power.
PSE Power Enabled	Displays the status of PSE power for the local device.
PSE Pairs Control Ability	Displays whether the PSE pairs can be controlled for the local device.
Maximum Frame Size	Displays the maximum frame size supported by the local device.

- **View Neighbor Info**

1. Go to L2 Features > LLDP > LLDP Config > Neighbor Info to load the following page. In Auto Refresh, enable Auto Refresh feature and set the Refresh Interval based on needs.



Auto Refresh

Auto Refresh ●

Refresh Interval 3 seconds (3-300)

2. In Neighbor Info, select the desired port and view the LLDP-MED information.

Device Type	Displays the LLDP-MED device type of the neighbor device.
Application Type	Displays the application type of the neighbor device.
Location Data Format	Displays the location type of the neighbor device.
Power Type	Displays the power type of the neighbor device.
Information	View more LLDP-MED details of the neighbor device.

Chapter 5

Configure L3 Features

This chapter guides you on how to configure L3 features. The chapter includes the following sections:

5. 1 Configure ARP

Overview

ARP (Address Resolution Protocol) is used to map IP addresses to MAC addresses. Taking an IP address as input, ARP learns the associated MAC address, and stores the IP-MAC address association in an ARP entry for rapid retrieval.

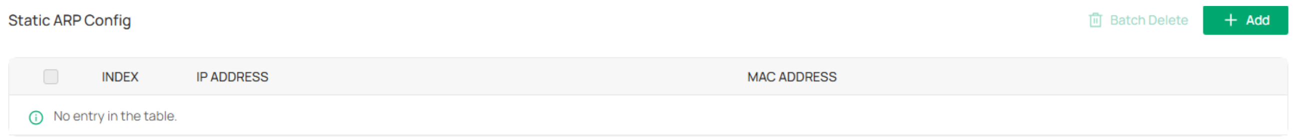
5. 1. 1 Add Static ARP Entries Manually

Overview

You can manually add ARP entries by specifying the IP addresses and MAC addresses.

Configuration

Go to L3 Feature > ARP > Static ARP to load the following page. Click +Add on the upper right and configure the parameters. Click Create.



Static ARP Config

□	INDEX	IP ADDRESS	MAC ADDRESS

ⓘ No entry in the table.

IP address	Specify the IP address of the static ARP entry.
MAC address	Specify the MAC address.of the static ARP entry.

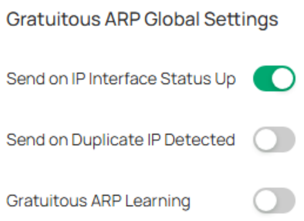
5. 1. 2 Configure Gratuitous ARP

Overview

Gratuitous ARP is a special kind of ARP. Both the source and destination addresses of the gratuitous ARP packet are the sender its own IP address. It is used to detect duplicate IP address. If an interface sends a gratuitous ARP packet and no replies are received, then the sender knows its IP address is not used by other devices.

Configuration

1. Go to L3 Feature > ARP > Gratuitous ARP to load the following page. In Gratuitous ARP Global Settings, configure the global settings for gratuitous ARP. Click Apply.



Gratuitous ARP Global Settings

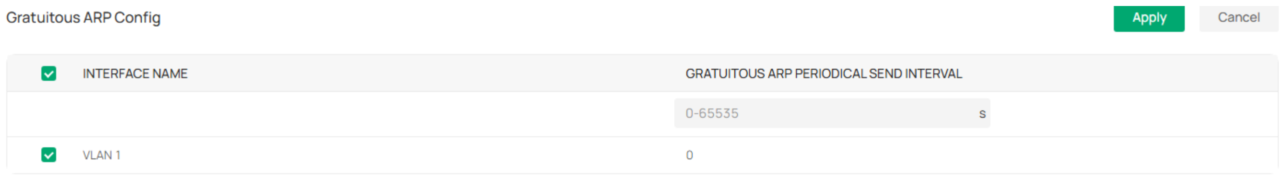
Send on IP Interface Status Up ☑

Send on Duplicate IP Detected ☐

Gratuitous ARP Learning ☐

Send on IP Interface Status Up	With this option enabled, the interface will send gratuitous ARP request packets when its status becomes up. This is used to announce the interface's IP address to the other hosts. It is enabled by default.
Send on Duplicate IP Detected	With this option enabled, the interface will send gratuitous ARP request packets when a gratuitous ARP request packet is received for which the IP address is the same as the interface's. In this case, the OLT knows that another host is using the same IP address as its own. To claim the IP address for the correct owner, the interface sends gratuitous ARP packets. It is disabled by default.
Gratuitous ARP Learning	Normally, the OLT only updates the MAC address table by learning from the ARP reply packet or normal ARP request packet. With this option enabled, the OLT will also update the MAC address table by learning from the received gratuitous ARP packets. It is disabled by default.

2. In Gratuitous ARP Config, select one or multiple interfaces to configure the parameters. Click Apply.



Gratuitous ARP Config

☑	INTERFACE NAME	GRATUITOUS ARP PERIODICAL SEND INTERVAL
		0-65535 s
☑	VLAN 1	0

Interface Name	Displays the Interface ID of the Layer 3 interface.
Gratuitous ARP Periodical Send Interval	Enter the interval of sending gratuitous ARP request packets for the interface. A value of 0 means the interface will not send gratuitous ARP request packets periodically.

5. 1. 3 Configure Proxy ARP

Overview

Normally, the ARP packets can only be transmitted in one broadcast domain, which means if two devices in the same network segment are connected to different Layer 3 interfaces, they cannot communicate with each other because they cannot learn each other's MAC address using ARP packets.

Proxy ARP solves this problem. when a host sends an ARP request to another device that is not in the same broadcast domain but on the same network segment, the Layer 3 interface with Proxy ARP enabled will respond the ARP request with its own MAC address if the destination IP is reachable.

After that, the ARP request sender sends packets to the OLT, and the OLT forwards the packets to the intended device.

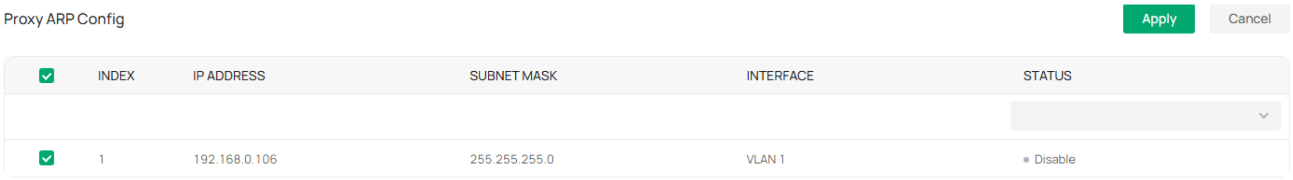
Local Proxy ARP is similar with Proxy ARP. When two hosts are in the same VLAN and connected to VLAN interface 1, but two ports are isolated on Layer 2, both of the hosts cannot receive each other's ARP request. So they cannot communicate with each other because they cannot learn each other's MAC address using ARP packets.

To solve this problem, you can enable Local Proxy ARP on the Layer 3 interface and the interface will respond the ARP request sender with its own MAC address. After that, the ARP request sender sends packets to the Layer 3 interface, and the interface forwards the packets to the intended device.

Configuration

■ Configure Proxy ARP

1. Go to L3 Feature > ARP > Proxy ARP to load the following page. In Proxy ARP Config, select one or multiple entries to configure the parameters. Click Apply.

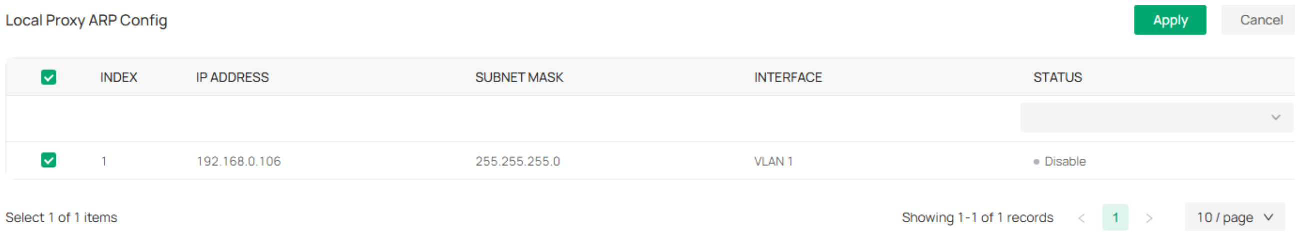


Proxy ARP Config

☑	INDEX	IP ADDRESS	SUBNET MASK	INTERFACE	STATUS
☑	1	192.168.0.106	255.255.255.0	VLAN 1	● Disable

IP Address	Displays the IP address of the Layer 3 interface
Subnet Mask	Displays the subnet mask of the IP address.
Interface	Displays the interface name of the entry.
Status	Enable proxy ARP feature on the interface. The interface will respond the ARP request sender with its own MAC address.

2. In Local Proxy ARP Config, select one or multiple entries to configure the parameters. Click Apply.



Local Proxy ARP Config

☑	INDEX	IP ADDRESS	SUBNET MASK	INTERFACE	STATUS
☑	1	192.168.0.106	255.255.255.0	VLAN 1	● Disable

Select 1 of 1 items

Showing 1-1 of 1 records

IP Address	Displays the IP address of the Layer 3 interface
Subnet Mask	Displays the subnet mask of the IP address.
Interface	Displays the interface ID of the entry.
Status	Enable proxy ARP feature on the interface. The interface will respond the ARP request sender with its own MAC address.

5. 2 Configure Static Routing

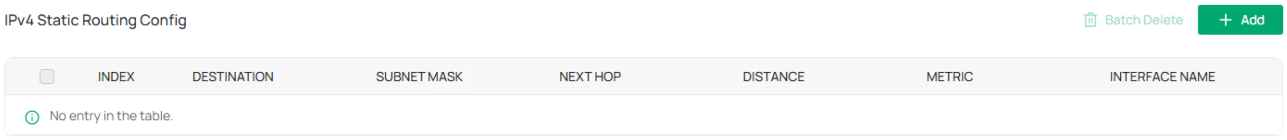
Overview

Static routing entries are manually added none-aging routing entries. In a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. In a complex large-scale network, static routes ensure stable connectivity for important applications because the static routes remain unchanged even when the topology changes.

The OLT supports IPv4 static routing and IPv6 static routing configuration.

■ Configure IPv4 Static Routing

Go to L3 Feature > Static Routing > IPv4 Static Routing to load the following page. Click +Add on the upper right and configure the parameters. Click Create.



IPv4 Static Routing Config

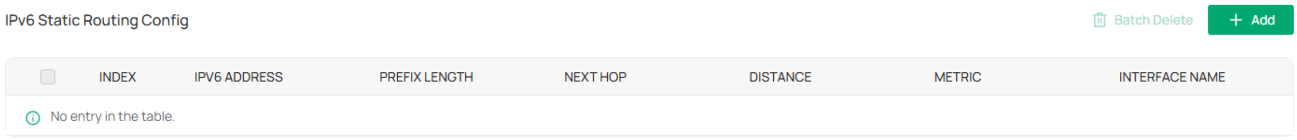
□	INDEX	DESTINATION	SUBNET MASK	NEXT HOP	DISTANCE	METRIC	INTERFACE NAME

ⓘ No entry in the table.

Destination	Specify the destination IPv4 address of the packets.
Subnet Mask	Specify the subnet mask of the destination IPv4 address.
Next Hop	Specify the IPv4 address to which the packet should be sent next.
Distance	Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv4 routing table. The valid value ranges from 1 to 255 and the default value is 1.

■ Configure IPv6 Staic Routing

Go to L3 Feature > Static Routing > IPv6 Static Routing to load the following page. Click +Add on the upper right and configure the parameters. Click Create.



IPv6 Static Routing Config

□	INDEX	IPV6 ADDRESS	PREFIX LENGTH	NEXT HOP	DISTANCE	METRIC	INTERFACE NAME

ⓘ No entry in the table.

IPv6 Address	Specify the destination IPv6 address of the packets.
Prefix Length	Specify the prefix length of the IPv6 address.
Next Hop	Specify the IPv6 address to which the packet should be sent next.

Distance	Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table. The valid value ranges from 1 to 255 and the default value is 1

5. 3 Configure DHCP Service

Overview

DHCP (Dynamic Host Configuration Protocol) is widely used to automatically assign IP addresses and other network configuration parameters to network devices, enhancing the utilization of IP address.

The supported DHCP features of the OLT include DHCP Server, DHCP Relay, and DHCP L2 Relay, and they support PON port configuration.

For the client under the PON port, DHCP Server will assign the IP of the interface under the svlan that matches the client under the PON port by default, DHCP Relay will use the svlan that matches the client under the PON port as the relay-agent-interface or vlan-relay vlanID, and DHCP L2 Relay will forward and execute op82 policy in the vlan that matches the client under the PON port.

5. 3. 1 DHCP Server

Overview

DHCP Server is used to dynamically assign IP addresses, default gateway and other parameters to DHCP clients. As the following figure shows, the OLT acts as a DHCP server and assigns IP addresses to the clients.

Configuration

To configure DHCP Server, follow these steps:

1) Enable the DHCP Server feature on the OLT.

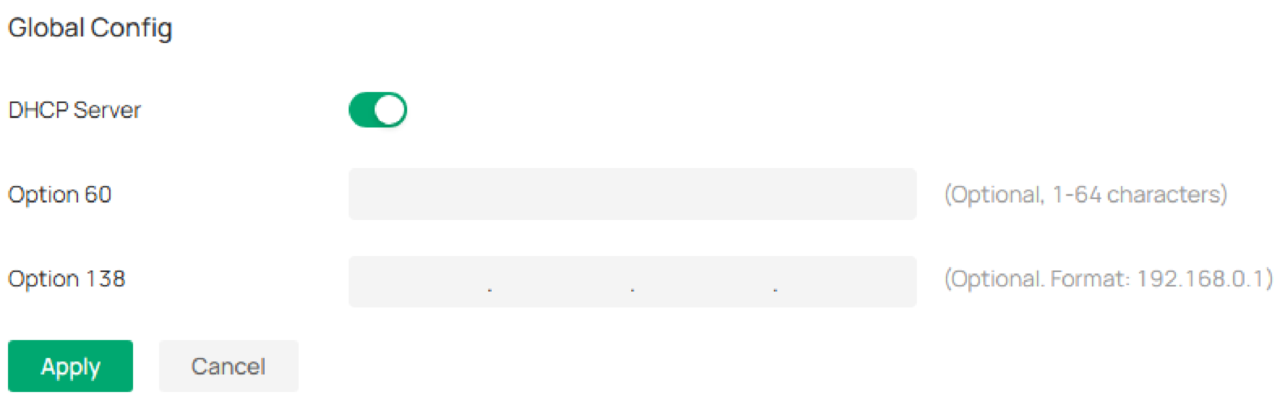
2) Configure DHCP Server Pool.

3) (Optional) Manually assign static IP addresses for some clients.

4) View Statistics.

- **Enable DHCP Server**

1. Go to L3 Feature > DHCP Service > DHCP Server > DHCP Server to load the following page. In Global Config, enable DHCP Server. Click Apply.



Global Config

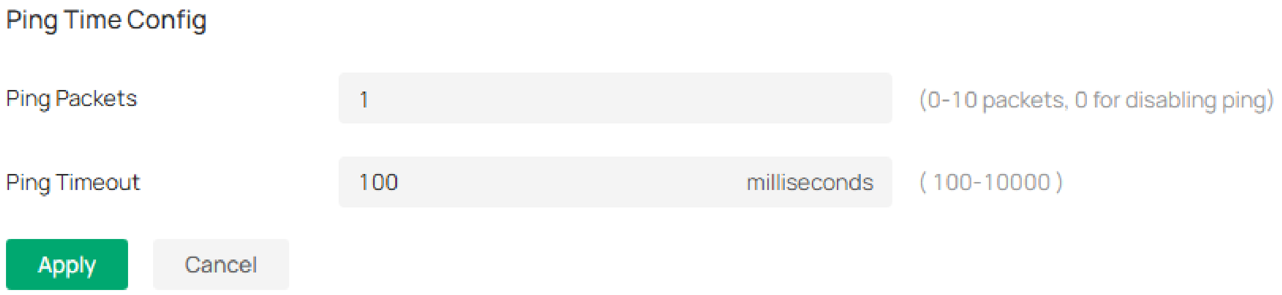
DHCP Server: ●

Option 60: (Optional, 1-64 characters)

Option 138: . . . (Optional. Format: 192.168.0.1)

DHCP Server	Enable DHCP Server.
Option 60	(Optional) Specify the Option 60 for device identification. Mostly it is used for the scenarios that the devices apply for different IP addresses from different servers according to the needs. If a device requests Option 60, the server will respond a packet containing the Option 60 configured here. And then the device will compare the received Option 60 with its own. If they are the same, the device will accept the IP address assigned by the server. Otherwise, the assigned IP address will not be accepted.
Option 138	(Optional) Specify the Option 138, which should be configured as the management IP address of an AC (Access Control) device. If the devices in the local network request this option, the server will respond a packet containing this option to inform the devices of the AC's IP address.

2. In Ping Time Config, configure the ping-related parameters. Click Apply.



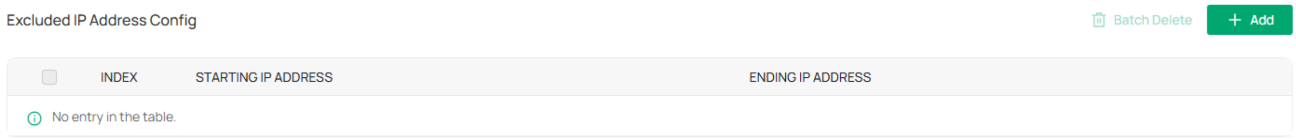
Ping Time Config

Ping Packets: 1 (0-10 packets, 0 for disabling ping)

Ping Timeout: 100 milliseconds (100-10000)

Ping Packets	Enter the number of ping packets the server can broadcast to test whether the IP address is occupied. The valid values are from 1 to 10, and the default is 1. When the OLT is configured as a DHCP server to dynamically assign IP addresses to clients, the OLT will deploy ping tests to avoid IP address conflicts resulted from assigning IP addresses repeatedly.
Ping Timeout	Specify the timeout period for ping tests in milliseconds. It ranges from 100 to 10000 ms, and the default is 100 ms. The DHCP server broadcasts an ICMP Echo Request (ping packet) to test whether an IP address is occupied or not. If there is no response within the timeout period, the server will broadcast the ping packet again. If the number of ping packets reaches the specified number without response, the server will assign the IP address. Otherwise, the server will record the IP address as a conflicted one and assign another IP address to the client.

3. (Optional) In Excluded IP Address Config, you can add IP addresses that will be not assigned. Click +Add on the upper right and configure the parameters. Click Create.



Excluded IP Address Config

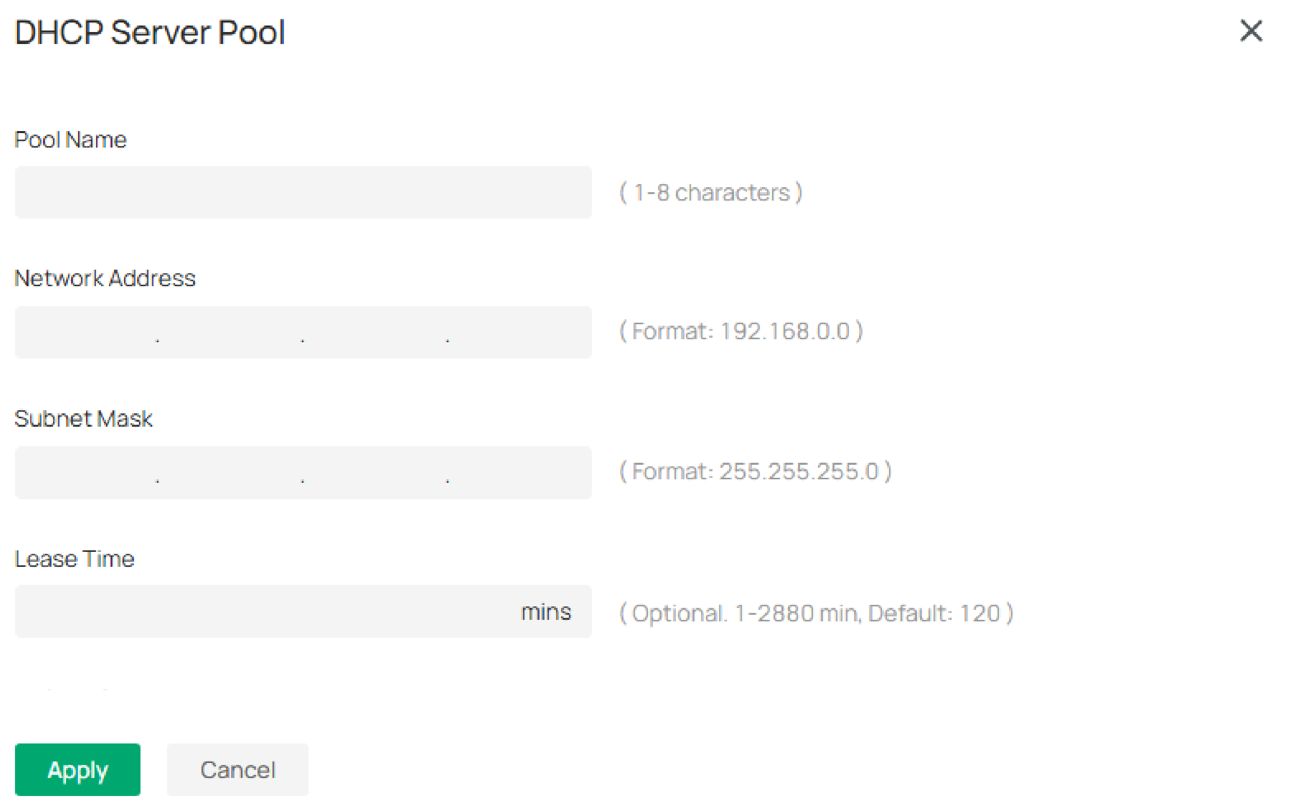
□	INDEX	STARTING IP ADDRESS	ENDING IP ADDRESS

No entry in the table.

Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address of the excluded IP address range. If the starting IP address and ending IP address are the same, the server excludes only one IP address. When configuring DHCP Server, you need to reserve certain IP addresses for each subnet, such as the default gateway address, broadcast address and DNS server address.

- **Configure DHCP Server Pool**

Go to L3 Feature > DHCP Service > DHCP Server > Pool Setting, click +Add on the upper right to configure the parameters for DHCP server pool. Click Create.


DHCP Server Pool

Pool Name

(1-8 characters)

Network Address

(Format: 192.168.0.0)

Subnet Mask

(Format: 255.255.255.0)

Lease Time

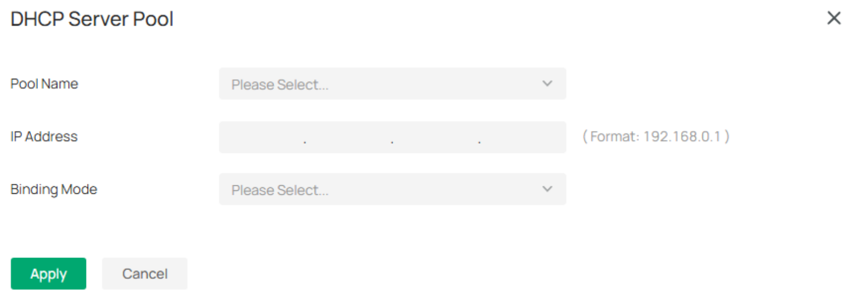
mins (Optional. 1-2880 min, Default: 120)

Pool Name	Specify a pool name for identification.
Network Address / Subnet Mask	Configure the network address and subnet mask of the DHCP server pool. The network address and subnet mask decide the range of the DHCP server pool. On the same subnet, all addresses can be assigned except the excluded addresses and addresses for special uses.
Lease Time	Specify how long the client can use the IP address assigned from this address pool. It ranges from 1 to 2880 minutes, and the default is 120 minutes.

Default Gateway	(Optional) Configure the default gateway of the DHCP server pool. You can create up to 8 default gateways for each DHCP server pool. If you leave this field blank, the DHCP server will not assign this parameter to clients. In general, you can configure the IP address of the VLAN interface as the default gateway address.
DNS Server	(Optional) Specify the DNS server of the DHCP server pool. You can specify up to 8 DNS servers for each DHCP server pool. If you leave this field blank, the DHCP server will not assign this parameter to clients. In general, you can configure the IP address of the VLAN interface as the DNS server address.
NetBIOS Server	(Optional) Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. If you leave this field blank, the DHCP server will not assign this parameter to clients. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve host names to IP addresses.
NetBIOS Node Type	(Optional) Specify the NetBIOS type for clients, which is the way of inquiring IP address resolution. If you leave this field blank, the DHCP server will not assign this parameter to clients. The following options are provided: b-node Broadcast: The client sends query messages via broadcast. p-node peer to peer: The client sends query messages via unicast. m-node Mixed: The client sends query messages via broadcast first. If it fails, the client will try again via unicast. h-node Hybrid: The client sends query messages via unicast first. If it fails, the client will try again via broadcast.
Next Server Address	(Optional) Specify the IP address of a TFTP server for clients. If needed, clients can get the configuration file from the TFTP server for auto installation. If you leave this field blank, the DHCP server will not assign this parameter to clients.
Domain Name	(Optional) Specify the domain name that clients should use when resolving host names via DNS. If you leave this field blank, the DHCP server will not assign this parameter to clients.
Bootfile	(Optional) Specify the name of the bootfile. If needed, clients can get the bootfile from the TFTP server for auto installation. If you leave this field blank, the DHCP server will not assign this parameter to clients.

Assign Static IP Address

(Optional) Go to L3 Feature > DHCP Service > Manual Binding, click +Add on the upper right to manually bind the MAC address or client ID of the device to an IP address, and the DHCP server will reserve the bound IP address to this device at all times. Click Create.

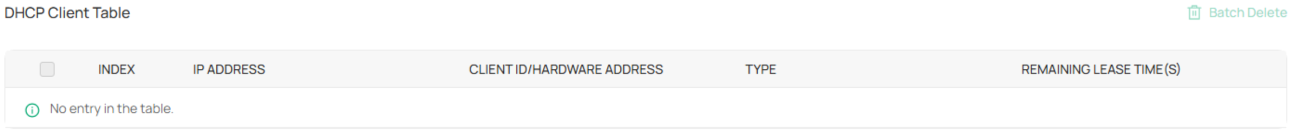

DHCP Server Pool

Pool Name	Please Select...	
IP Address	. . .	(Format: 192.168.0.1)
Binding Mode	Please Select...	

Pool Name	Select a DHCP server pool from the drop-down list.
IP Address	Enter the IP address to be bound to the client.
Binding Mode	Select the binding mode: Client ID: Bind the IP address to the client ID of the client. Client ID in ASCII: Bind the IP address to the client ID in ASCII format. Hardware Address: Bind the IP address to the MAC address of the client.
Client ID	If you select Client ID as the binding mode, enter the client ID in this field.
Hardware Address	If you select Hardware Address as the binding mode, enter the MAC address in this field.
Hardware Type	If you select Hardware Address as the binding mode, select a hardware type. The hardware type includes Ethernet and IEEE802.

View DHCP Client List

Go to L3 Feature > DHCP Service > DHCP Client List, in DHCP Client Table, you can view the DHCP client info.


DHCP Client Table

□	INDEX	IP ADDRESS	CLIENT ID/HARDWARE ADDRESS	TYPE	REMAINING LEASE TIME(S)

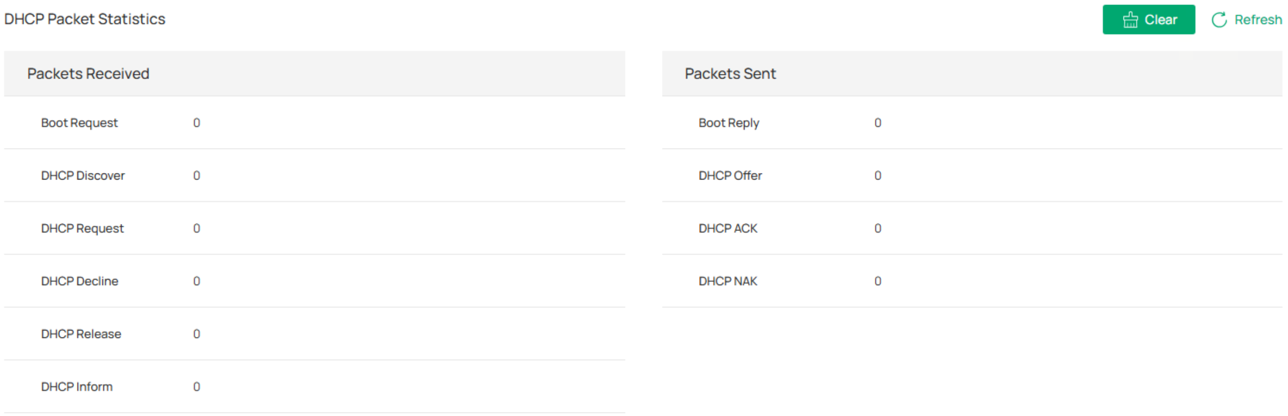
ⓘ No entry in the table.

Index	Displays the ID of the entry.
IP Address	Displays the IP address of the client.
Client ID/Hardware Address	Displays the client ID or the hardware address of the client.

Type	Displays how the client obtains its IP address. Manual: The IP address of the client is a static IP. Automatic: The IP address of the client is assigned by a DHCP server.
Left Lease Time(s)	Displays the remaining lease time of the assigned IP address.

- **View Packet Statistics**

Go to L3 Feature > DHCP Service > Packet Statistics to load the following page. Click Refresh to refresh the statistics, and click Clear to clear all statistics.



DHCP Packet Statistics

Packets Received		Packets Sent	
Boot Request	0	Boot Reply	0
DHCP Discover	0	DHCP Offer	0
DHCP Request	0	DHCP ACK	0
DHCP Decline	0	DHCP NAK	0
DHCP Release	0		
DHCP Inform	0		

5. 3. 2 DHCP Relay

Overview

DHCP Relay is used to process and forward DHCP packets between different subnets or VLANs.

DHCP clients broadcast DHCP request packets to require for IP addresses. Without this function, clients cannot obtain IP addresses from a DHCP server in the different LAN because the broadcast packets can be transmitted only in the same LAN. To equip each LAN with a DHCP server can solve this problem, but the costs of network construction will be increased and the management of central network will become inconvenient.

A device with DHCP Relay function is a better choice. It acts as a relay agent and can forward DHCP packets between DHCP clients and DHCP servers in different LANs. Therefore, DHCP clients in different LANs can share one DHCP server.

DHCP Relay includes three features: Option 82, DHCP Interface Relay and DHCP VLAN Relay.

- **Option 82**

Option 82 is called the DHCP Relay Agent Information Option. It provides additional security and a more flexible way to allocate network addresses compared with the traditional DHCP.

When enabled, the DHCP relay agent can inform the DHCP server of some specified information of clients by inserting an Option 82 payload to DHCP request packets before forwarding them to the DHCP server, so that the DHCP server can distribute the IP addresses or other parameters to clients based on the payload. In this way, Option 82 prevents DHCP client requests from untrusted sources. Besides, it allows the DHCP server to assign IP addresses of different address pools to clients in different groups.

An Option 82 has two sub-options, namely, the Agent Circuit ID and Agent Remote ID. The information that the two sub-options carry depends on the settings of the DHCP relay agent, and are different among devices from different vendors. To allocate network addresses using Option 82, you need to define the two sub-options on the DHCP relay agent, and create a DHCP class on the DHCP server to identify the Option 82 payload.

TP-Link OLT presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value.

The following tables show the packet formats of the Agent Circuit ID and Agent Remote ID, respectively.

Packet Formats of the Agent Circuit ID with Different Option 82 Settings:

Option 82 Settings		*Type (Hex)	*Length (Hex)	*Value
*Format	Circuit ID Customization			
Normal (TLV)	Disabled	00	04	Default circuit ID
	Enabled	01	Length of the customized circuit ID	Customized circuit ID
Private (Only the value)	Disabled	-	-	Default circuit ID
	Enabled	-	-	Customized circuit ID

Packet Formats of the Agent Remote ID with Different Option 82 Settings:

Option 82 Settings		*Type (Hex)	*Length (Hex)	*Value
*Format	Remote ID Customization			
Normal (TLV)	Disabled	00	06	Default remote ID
	Enabled	01	Length of the customized remote ID	Customized remote ID
Private (Only the value)	Disabled	-	-	Default remote ID
	Enabled	-	-	Customized remote ID

***Format**

Indicates the packet format of the sub-option field. Two options are available:

Normal: Indicates the field consists of three parts: Type, Length, and Value (TLV).

Private: Indicates the field consists of the value only.

***Type**

A one-byte field indicating whether the Value field is customized or not. **00** in hexadecimal means the Value field is not customized (uses the default circuit/remote ID) while **01** in hexadecimal means it is customized.

***Length**

A one-byte field indicating the length of the Value field. The length of the default circuit ID is 4 bytes and that of default remote ID is 6 bytes. For the customized circuit ID and remote ID, the length is variable, ranging from 1 to 64 bytes.

***Value**

Indicates the value of the sub-option. The OLT has preset a default circuit ID and remoter ID. You can also customize them with Circuit ID Customization and Remote ID Customization enabled.

Default circuit ID: A 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to.

For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is **00:02:00:01** in hexadecimal.

Default remote ID: A 6-byte value which indicates the MAC address of the DHCP relay agent.

Customized circuit/remote ID: You can configure a string using up to 64 characters. The OLT encodes the string using ASCII. When configuring your DHCP server to identify the string, use the correct notation that is used by your DHCP server to represent ASCII strings, or convert it into hexadecimal format if necessary.

As shown in the tables above, by default, the circuit ID records the ports of the DHCP relay agent that are connected to the clients and the VLANs that the clients belong to, and the remote ID records the MAC address of the DHCP relay agent. That is, the two sub-options together record the location of the clients. To record the accruate location of clients, configure Option 82 on the OLT which is closest to the clients.

- **DHCP Interface Relay**

DHCP Interface Relay allows clients to obtain IP addresses from a DHCP server in a different LAN. In DHCP Interface Relay, you can specify a DHCP server for the Layer 3 interface that the clients are connected to. When receiving DHCP packets from clients, the OLT fills the corresponding interface's IP address in the Relay Agent IP Address field of the DHCP packets, and forwards the packets to the DHCP server. Then the DHCP server can assign IP addresses that are in the same subnet with the Relay Agent IP Address to the clients.

The OLT supports specifying a DHCP server for multiple Layer 3 interfaces, which makes it possible to assign IP addresses to clients in different subnets from the same DHCP server.

- **DHCP VLAN Relay**

DHCP VLAN Relay allows clients in different VLANs to obtain IP addresses from the DHCP server using the IP address of a single agent interface.

In DHCP Interface Relay, to achieve this goal, you need to create a Layer 3 interface for each VLAN to ensure the reachability.

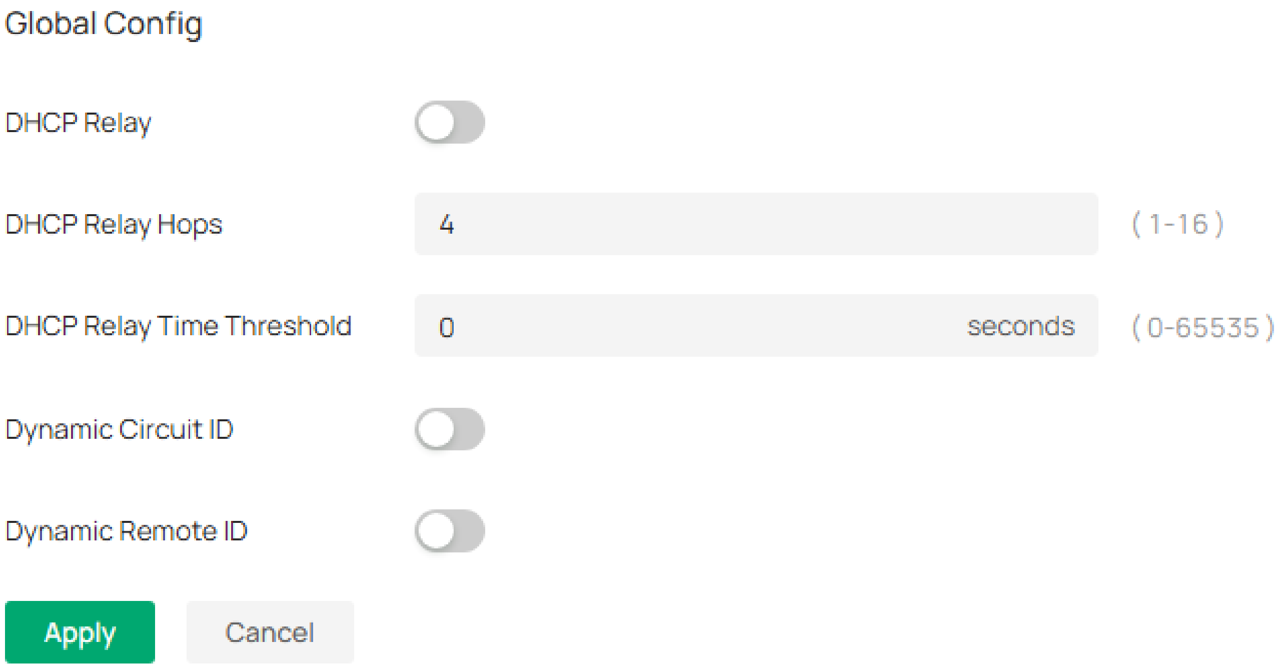
In DHCP VLAN Relay, you can simply specify a Layer 3 interface as the default agent interface for all VLANs. The OLT fills this default agent interface's IP address in the Relay Agent IP Address field of the DHCP packets from all VLANs.

Note that If the VLAN already has an IP address, the OLT will use the IP address of the VLAN as the relay agent IP address. The default relay agent IP address will not take effect.

DHCP VLAN Relay will not work on routed ports or port channel interfaces, because they are not associated with any particular VLAN.

Configuration

1. Go to L3 Feature > DHCP Service > DHCP Relay > DHCP Relay Config to load the following page. In Global Config, configure the parameters. Click Apply.



Global Config

DHCP Relay ○

DHCP Relay Hops 4 (1-16)

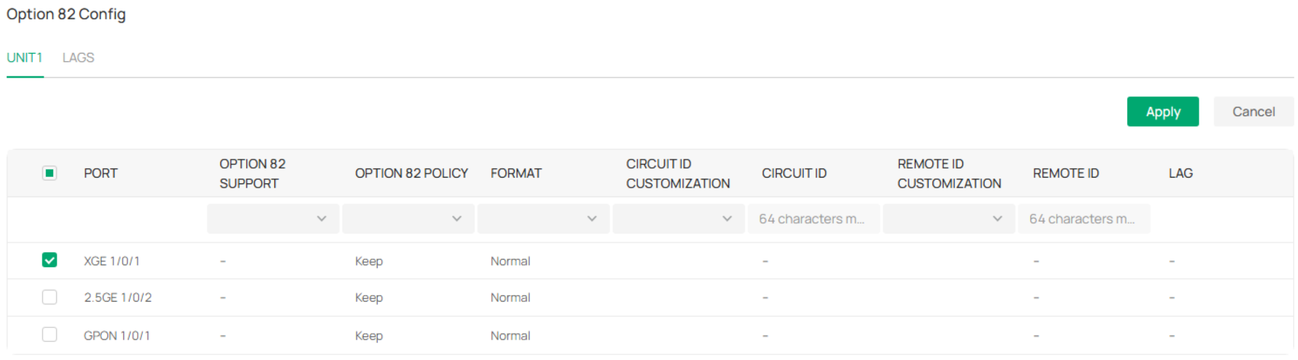
DHCP Relay Time Threshold 0 seconds (0-65535)

Dynamic Circuit ID ○

Dynamic Remote ID ○

DHCP Relay	Enable DHCP Relay globally.
DHCP Relay Hops	Specify the DHCP relay hops. DHCP Relay Hops defines the maximum number of hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped.
DHCP Relay Time Threshold	Specify the threshold of the DHCP relay time. The valid values are from 0 to 65535 seconds. DHCP relay time is the time elapsed since the client began address acquisition or renewal process. There is a field in DHCP packets which specially records this time, and the OLT will drop the packets if the value of this field is greater than the threshold. Value 0 means the OLT will not examine this field of the DHCP packets.

2. (Optional) In Option 82 Config, select one or multiple ports to configure the parameters. Click Apply.



■	PORT	OPTION 82 SUPPORT	OPTION 82 POLICY	FORMAT	CIRCUIT ID CUSTOMIZATION	CIRCUIT ID	REMOTE ID CUSTOMIZATION	REMOTE ID	LAG
						64 characters m...		64 characters m...	
☑	XGE 1/0/1	-	Keep	Normal		-		-	-
□	2.5GE 1/0/2	-	Keep	Normal		-		-	-
□	GPON 1/0/1	-	Keep	Normal		-		-	-

Option 82 Support

Select whether to enable Option 82.

Enable it if you want to prevent DHCP client requests from untrusted sources, or assign different IP addresses to clients in different groups from the same DHCP server.

Option 82 Policy

Select the operation for the OLT to take when receiving DHCP packets that include the Option 82 field.

Keep: The OLT keeps the Option 82 field of the packets.

Replace: The OLT replaces the Option 82 field of the packets with a new one. The OLT presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value.

Drop: The OLT discards the packets that include the Option 82 field.

Format

Specify the packet format for the sub-option fields of Option 82.

Normal: Indicates the fields consist of three parts: Type, Length, and Value (TLV).

Private: Indicates the fields consist of the value only.

Circuit ID Customization

Enable or disable Circuit ID Customization. Enable it if you want to manually configure the circuit ID. Otherwise, the OLT uses the default one when inserting Option 82 to DHCP packets.

The default circuit ID is a 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to. For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is 00:02:00:01 in hexadecimal.

Circuit ID

Enter the customized circuit ID with up to 64 characters. The circuit ID configurations of the OLT and the DHCP server should be compatible with each other.

Remote ID Customization

Enable or disable Remote ID Customization. Enable it if you want to manually configure the remote ID. Otherwise, the OLT uses its own MAC address as the remote ID.

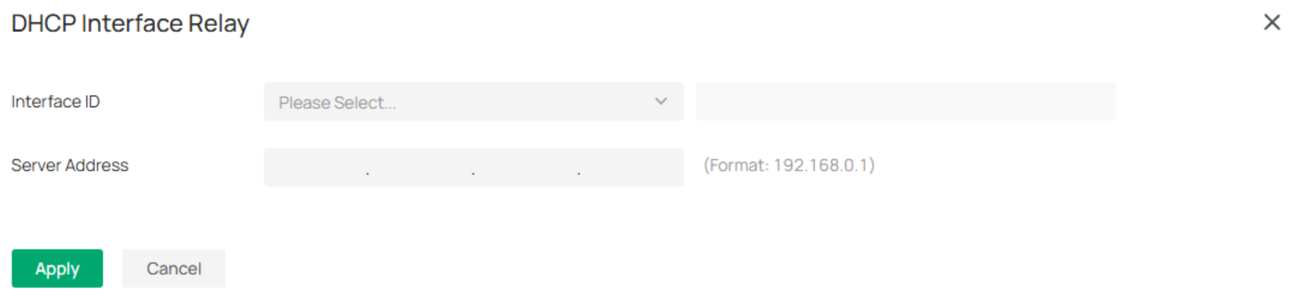
Remote ID

Enter the customized remote ID with up to 64 characters. The remote ID configurations of the OLT and the DHCP server should be compatible with each other.

3. Configure the DHCP Interface Relay or DHCP VLAN Relay based on needs.

- **DHCP Interface Relay**

Go to L3 Feature > DHCP Service > DHCP Relay > DHCP Interface Relay to load the following page. Click +Add on the upper right and configure the parameters. Click Create.



DHCP Interface Relay

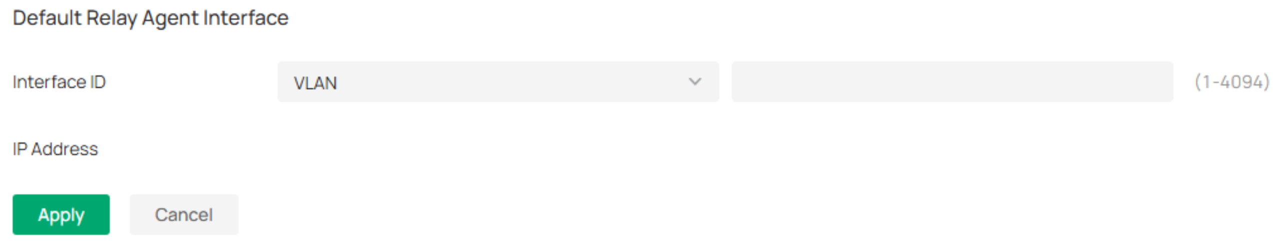
Interface ID: Please Select...

Server Address: . . . (Format: 192.168.0.1)

Interface ID	Specify the type and ID of the interface you have created. It is the Layer 3 interface which is connecting to the DHCP clients. To create a L3 interface, refer to 8. 3 Configure L3 Interface.
Server Address	Enter the IP address of the DHCP server.

- **DHCP VLAN Relay**

Go to L3 Feature > DHCP Service > DHCP Relay > DHCP VLAN Relay to load the following page to configure the parameters. Click Apply.



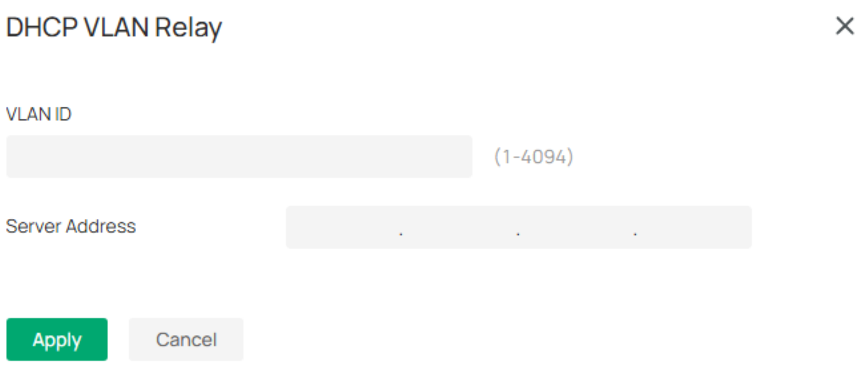
Default Relay Agent Interface

Interface ID: VLAN (1-4094)

IP Address

Interface ID	Specify the type and ID of the interface that needs to be configured as the default relay agent interface. You can configure any existing Layer 3 interface as the default relay-agent interface. The DHCP server will assign IP addresses in the same subnet with this relay agent interface to the clients who use this relay-agent interface to apply for IP addresses. To create a L3 interface, refer to 8. 3 Configure L3 Interface.
IP Address	Displays the IP address of this interface.

In DHCP VLAN Relay Config, click +Add on the upper right and configure the parameters. Click Create.


DHCP VLAN Relay

VLAN ID (1-4094)

Server Address . . .

VLAN ID	Specify the VLAN in which the clients can get IP addresses from the DHCP server.
Server Address	Enter the IP address of the DHCP server.

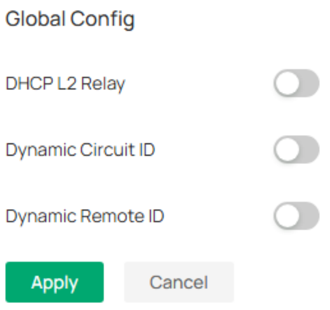
5. 3. 3 DHCP L2 Relay

Overview

DHCP L2 Relay is used in the situation that the DHCP server and clients are in the same VLAN. In DHCP L2 Relay, in addition to normally assigning IP addresses to clients from the DHCP server, the OLT can inform the DHCP server of some specified information, such as the location information, of clients by inserting an Option 82 payload to DHCP request packets before forwarding them to the DHCP server. This allows the DHCP server which supports Option 82 can set the distribution policy of IP addresses and other parameters, providing a more flexible way to distribute IP addresses.

Configuration

1. Go to L3 Feature > DHCP Service > DHCP L2 Relay > Global Config to load the following page. In Global Config, enable the feature. Click Apply.

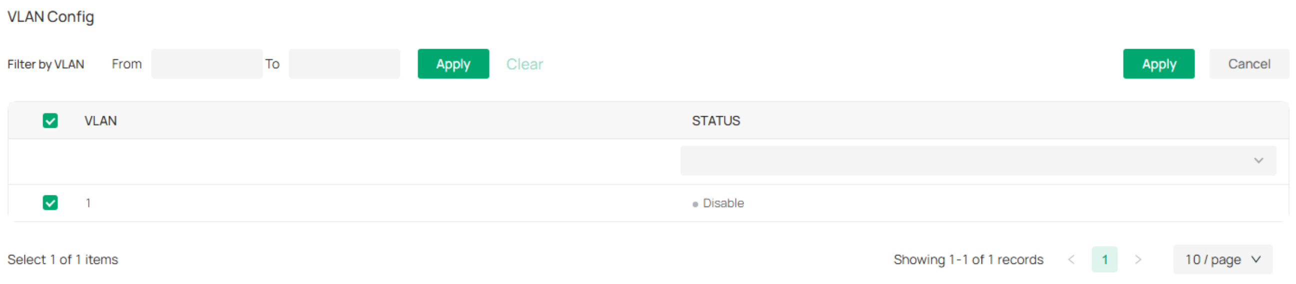

Global Config

DHCP L2 Relay ○

Dynamic Circuit ID ○

Dynamic Remote ID ○

2. In VLAN Config, select one or multiple VLANs to enable the feature. Click Apply.



VLAN Config

Filter by VLAN From [ ] To [ ] Apply Clear | Apply Cancel

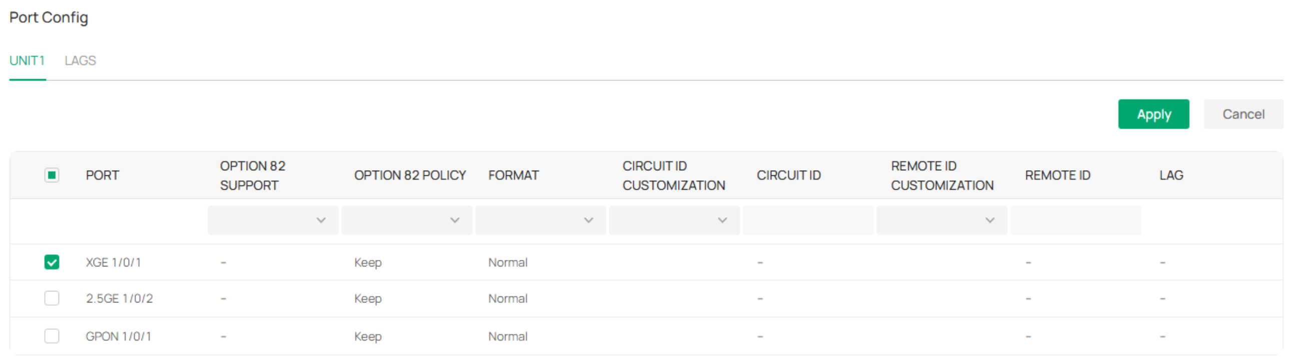
☑	VLAN	STATUS
☑	1	● Disable

Select 1 of 1 items

Showing 1-1 of 1 records < 1 > 10 / page

VLAN Config	Displays the VLAN ID.
Status	Enable DHCP L2 Relay for the specified VLAN.

Go to L3 Feature > DHCP Service > DHCP L2 Relay > Port Config to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Config

UNIT1 LAGS

Apply Cancel

■	PORT	OPTION 82 SUPPORT	OPTION 82 POLICY	FORMAT	CIRCUIT ID CUSTOMIZATION	CIRCUIT ID	REMOTE ID CUSTOMIZATION	REMOTE ID	LAG
☑	XGE 1/0/1	-	Keep	Normal		-		-	-
□	2.5GE 1/0/2	-	Keep	Normal		-		-	-
□	GPON 1/0/1	-	Keep	Normal		-		-	-

Option 82 Support	Select whether to enable Option 82 or not. Enable it if you want to prevent DHCP client requests from untrusted sources, or assign different IP addresses to clients in different groups from the same DHCP server.
Option 82 Policy	Select the operation for the OLT to take when receiving DHCP packets that include the Option 82 field. Keep: The OLT keeps the Option 82 field of the packets. Replace: The OLT replaces the Option 82 field of the packets with a new one. The OLT presets a default circuit ID and remote ID in TLV (Type, Length, and Value) format. You can also configure the format to include Value only and customize the Value. Drop: The OLT discards the packets that include the Option 82 field.
Format	Specify the packet format for the sub-option fields of Option 82. Normal: Indicates the fields consist of three parts: Type, Length, and Value (TLV). Private: Indicates the fields consist of the value only.

Circuit ID Customization	Enable or disable Circuit ID Customization. Enable it if you want to manually configure the circuit ID. Otherwise, the OLT uses the default one when inserting Option 82 to DHCP packets. The default circuit ID is a 4-byte value which consists of 2-byte VLAN ID and 2-byte Port ID. The VLAN ID indicates which VLAN the DHCP client belongs to, and the Port ID indicates which port the DHCP client is connected to. For example, if the DHCP client is connected to port 1/0/1 in VLAN 2, this field is 00:02:00:01 in hexadecimal.
Circuit ID	Enter the customized circuit ID with up to 64 characters. The circuit ID configurations of the OLT and the DHCP server should be compatible with each other.
Remote ID Customization	Enable or disable Remote ID Customization. Enable it if you want to manually configure the remote ID. Otherwise, the OLT uses its own MAC address as the remote ID.
Remote ID	Enter the customized remote ID with up to 64 characters. The remote ID configurations of the OLT and the DHCP server should be compatible with each other.

Chapter 6

Configure Multicast

This chapter guides you on how to configure multicast. The chapter includes the following sections:

6. 1 Configure IGMP Snooping

Overview

On the Layer 2 device, IGMP (Internet Group Management Protocol) Snooping transmits data on demand on data link layer by analyzing IGMP packets between the IGMP querier and the users, to build and maintain Layer 2 multicast forwarding table.

Before configurations, here are some basic concepts of IGMP Snooping:

- **IGMP Querier**

  An IGMP querier is a multicast router (a router or a Layer 3 switch) that sends query messages to maintain a list of multicast group memberships for each attached network, and a timer for each membership.

  Normally only one device acts as querier per physical network. If there are more than one multicast router in the network, a querier election process will be implemented to determine which one acts as the querier.

- **Snooping OLT**

  A snooping OLT indicates an OLT with IGMP Snooping enabled. The OLT maintains a multicast forwarding table by snooping on the IGMP transmissions between the host and the querier. With the multicast forwarding table, the OLT can forward multicast data only to the ports that are in the corresponding multicast group, so as to constrain the flooding of multicast data in the Layer 2 network.

- **Router Port**

  A router port is a port on snooping OLT that is connecting to the IGMP querier.

- **Member Port**

  A member port is a port on snooping OLT that is connecting to the host.

Configuration

To configure IGMP Snooping for IPv4, follow these steps:

1) Configure IGMP Snooping globally.

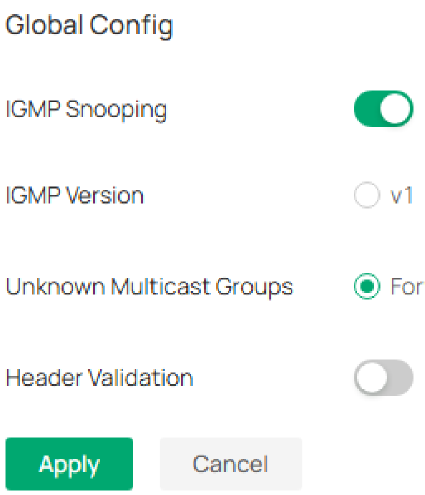
2) Configure IGMP Snooping for VLANs.

3) Configure IGMP Snooping on ports.

4) (Optional) Configure hosts to statically join a group.

6. 1. 1 Configure Globally

Go to Multicast > IGMP Snooping > Global Config to load the following page. In Global Config, enable the feature globally and configure the parameters. Click Apply.



Global Config

IGMP Snooping: on

IGMP Version: ○ v1 ○ v2 ● v3

Unknown Multicast Groups: ● Forward ○ Discard

Header Validation: off

IGMP Snooping	Enable IGMP Snooping globally.
IGMP Version	Specify the IGMP version. v1: The OLT works as an IGMPv1 Snooping OLT. It can only process IGMPv1 messages from the host. Messages of other versions are ignored. v2: The OLT works as an IGMPv2 Snooping OLT. It can process both IGMPv1 and IGMPv2 messages from the host. IGMPv3 messages are ignored. v3: The OLT works as an IGMPv3 Snooping OLT. It can process IGMPv1, IGMPv2 and IGMPv3 messages from the host.
Unknown Multicast Groups	Set how the OLT processes data that are sent to unknown multicast groups. By default, it is Forward. Forward: The OLT will forward the data. Discard: The OLT will drop the data. Unknown multicast groups are multicast groups that do not match any of the groups announced in earlier IGMP membership reports, and thus cannot be found in the multicast forwarding table of the OLT. Note that IGMP Snooping and MLD Snooping share the setting of Unknown Multicast Groups, so you have to enable MLD Snooping globally on the Multicast > MLD Snooping > Global Config page at the same time.

Header Validation

Enable or disable Header Validation. By default, it is disabled.

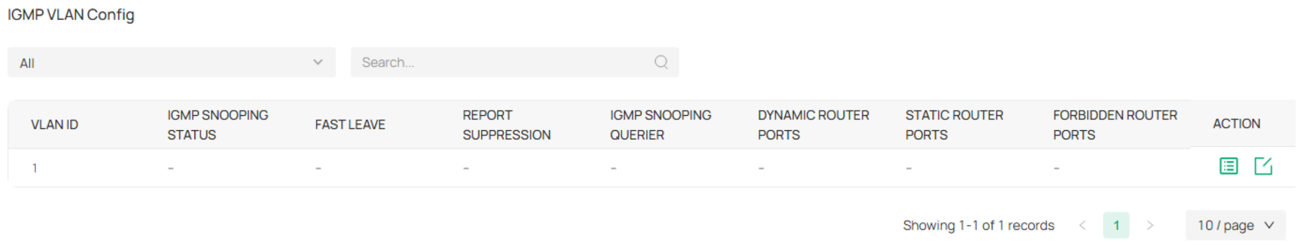
Generally, for IGMP packets, the TTL value should be 1, ToS field should be 0xC0, and Router Alert option should be 0x94040000. The fields to be validated depend on the IGMP version being used.

IGMPv1 only checks the TTL field.

IGMPv2 checks the TTL field and the Router Alert option.

IGMPv3 checks TTL field, ToS field and Router Alert option. Packets that fail the validation process will be dropped.

In IGMP VLAN Config, click ✎ of the desired VLAN entry in IGMP VLAN Config to configure the parameters. Click Save. You can also view details by clicking ☰.



IGMP VLAN Config

All

Search...

VLAN ID	IGMP SNOOPING STATUS	FAST LEAVE	REPORT SUPPRESSION	IGMP SNOOPING QUERIER	DYNAMIC ROUTER PORTS	STATIC ROUTER PORTS	FORBIDDEN ROUTER PORTS	ACTION
1	-	-	-	-	-	-	-	☰ ✎

Showing 1-1 of 1 records < 1 > 10 / page

VLAN ID

Displays the VLAN ID.

IGMP Snooping Status

Enable or disable IGMP Snooping for the VLAN.

Fast Leave

Enable or disable Fast Leave for the VLAN. IGMPv1 does not support Fast Leave.

Disabled: Without Fast Leave, after a receiver sends an IGMP leave message to leave a multicast group, the OLT will forward the leave message to the Layer 3 device (the querier).

From the point of view of the querier, the port connecting to the OLT is a member port of the corresponding multicast group. After receiving the leave message from the OLT, the querier will send out a configured number (Last Member Query Count) of group-specific queries on that port with a configured interval (Last Member Query Interval), and wait for IGMP group membership reports. If there are other receivers connecting to the OLT, they will response to the queries before the Last Member Query Interval expires. If no reports are received after the response time of the last query expires, the querier will remove the port from the forwarding list of the corresponding multicast group.

That is, if there are other receivers connecting to the OLT, the one sent leave message have to wait until the port ages out from the OLT's forwarding list of the corresponding multicast group (the maximum waiting time is decided by the Member Port Aging Time).

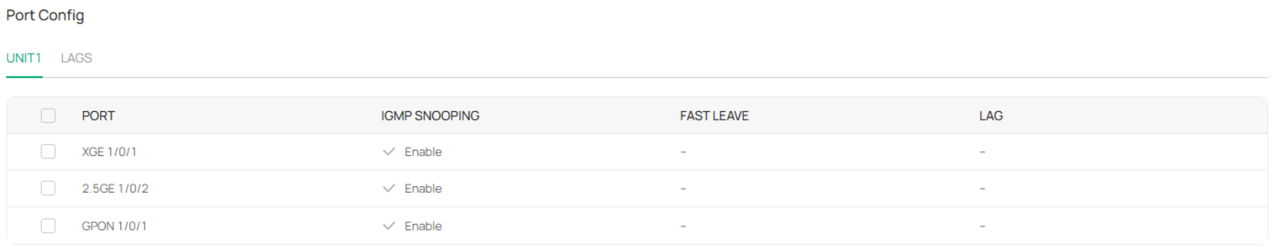
Enabled: With Fast Leave enabled on a VLAN, the OLT will remove the (Multicast Group, Port, VLAN) entry from the multicast forwarding table before forwarding the leave message to the querier. This helps reduce bandwidth waste since the OLT no longer sends the corresponding multicast streams to the VLAN of the port as soon as the port receives a leave message from the VLAN.

Report Suppression	Enable or disable Report Suppression for the VLAN. When enabled, the OLT will only forward the first IGMP report message for each multicast group to the IGMP querier and suppress subsequent IGMP report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the IGMP querier.
Member Port Aging Time	Specify the aging time of the member ports in the VLAN. Once the OLT receives an IGMP membership report message from a port, the OLT adds this port to the member port list of the corresponding multicast group. Member ports that are learned in this way are called dynamic member ports. If the OLT does not receive any IGMP membership report messages for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and will delete it from the multicast forwarding table.
Router Port Aging Time	Specify the aging time of the router ports in the VLAN. Once the OLT receives an IGMP general query message from a port, the OLT adds this port to the router port list. Router ports that are learned in this way are called dynamic router ports. If the OLT does not receive any IGMP general query message from a dynamic router port within the router port aging time, the OLT will no longer consider this port as a router port and will delete it from the router port list.
Leave Time	Specify the leave time for the VLAN. When the OLT receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the OLT receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows: 1) If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends; 2) The Leave Time mechanism will not take effect when Fast Leave takes effect. A proper leave time value can avoid other hosts connecting to the same port of the OLT being mistakenly removed from the multicast group when only some of them want to leave.
IGMP Snooping Querier	Enable or disable the IGMP Snooping Querier for the VLAN. When enabled, the OLT acts as an IGMP Snooping Querier for the hosts in this VLAN. A querier periodically sends a general query on the network to solicit membership information, and sends group-specific queries when it receives leave messages from hosts.
Query Interval	With IGMP Snooping Querier enabled, specify the interval between general query messages sent by the OLT.
Maximum Response Time	With IGMP Snooping Querier enabled, specify the host's maximum response time to general query messages.

Last Member Query Interval	With IGMP Snooping Querier enabled, when the OLT receives an IGMP leave message, it obtains the address of the multicast group that the host wants to leave from the message. Then the OLT sends out group-specific queries to this multicast group through the port receiving the leave message. This parameter determines the interval between group-specific queries.
Last Member Query Count	With IGMP Snooping Querier enabled, specify the number of group-specific queries to be sent. If specified count of group-specific queries are sent and no report message is received, the OLT will delete the multicast address from the multicast forwarding table.
General Query Source IP	With IGMP Snooping Querier enabled, specify the source IP address of the general query messages sent by the OLT. It should be a unicast address.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. Static router ports do not age. Multicast streams and IGMP packets to all groups in this VLAN will be forwarded through the static router ports. Multicast streams and IGMP packets to the groups that have dynamic router ports will be also forwarded through the corresponding dynamic router ports.
Forbidden Router Ports	Select ports to forbid them from being router ports in the VLAN.

6. 1. 2 Configure on Ports

Go to Multicast > IGMP Snooping > Port Config, select one or multiple ports to configure the parameters. Click Apply.



Port Config

UNIT1 LAGS

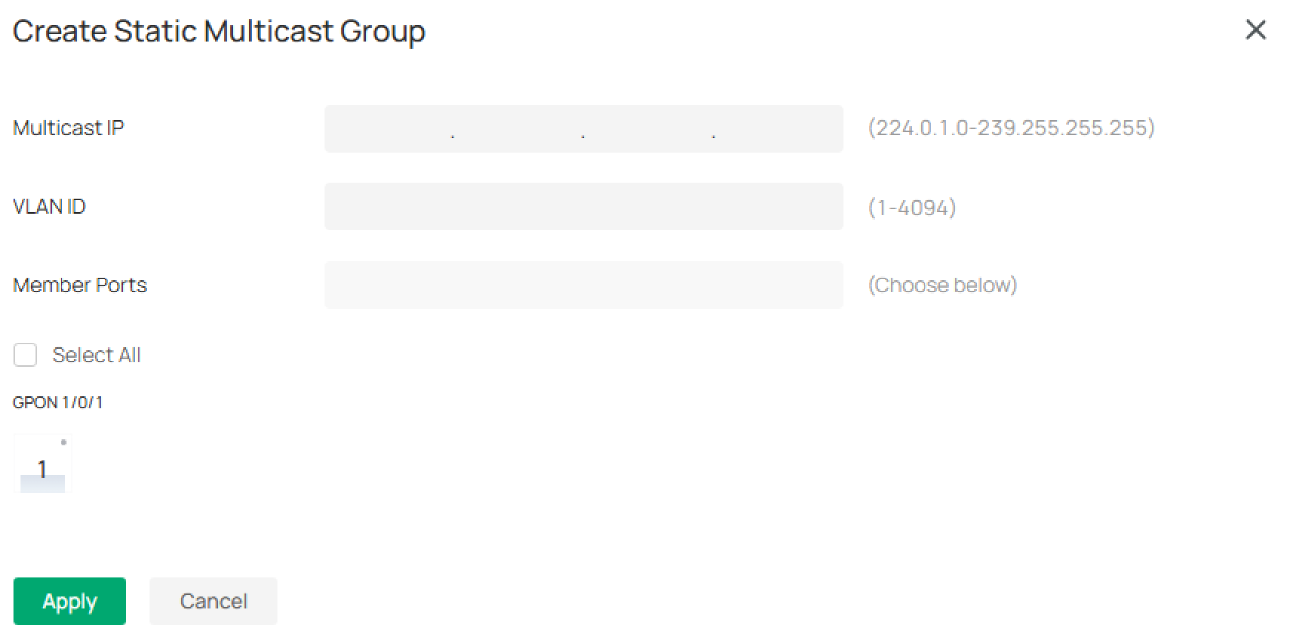
□	PORT	IGMP SNOOPING	FAST LEAVE	LAG
□	XGE 1/0/1	✓ Enable	-	-
□	2.5GE 1/0/2	✓ Enable	-	-
□	GPON 1/0/1	✓ Enable	-	-

Port (Only for Unit)	Displays the port ID.
LAG (Only for LAGS)	Displays the ID of the LAG.
IGMP Snooping	Enable or disable IGMP Snooping for the port.
Fast Leave	Enable or disable Fast Leave for the port. IGMPv1 does not support fast leave. Fast Leave can be enabled on a per-port basis or per-VLAN basis. When enabled on a per-port basis, the OLT will remove the port from the corresponding multicast group of all VLANs before forwarding the leave message to the querier. You should only use Fast Leave for a port when there is a single receiver connected to the port. For more details about Fast Leave, refer to Fast Leave.
LAG (Only for Unit)	Displays which LAG the port belongs to.

6. 1. 3 Optional Configuration

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also configure hosts to statically join a group.

Go to Multicast > IGMP Snooping > Static Group Config, click +Add on the upper right to load the following page. Configure the parameters. Click Create.



Create Static Multicast Group

Multicast IP . . . (224.0.1.0-239.255.255.255)

VLAN ID (1-4094)

Member Ports (Choose below)

□ Select All

GPON 1/0/1

Multicast IP	Specify the address of the multicast group that the hosts need to join.
VLAN ID	Specify the VLAN that the hosts are in.
Member Ports	Select the ports that the hosts are connected to. These ports will become the static member ports of the multicast group and will never age.
Unit	Select the ports to be the static member ports of the multicast group by clicking the port icons below.

6. 2 Configure MLD Snooping

Overview

On the Layer 2 device, MLD Snooping (Multicast Listener Discovery Snooping) transmits data on demand on data link layer by analyzing MLD packets between the MLD querier and the users, to build and maintain Layer 2 multicast forwarding table.

Configuration

To configure MLD Snooping for IPv6, follow these steps:

1) Configure MLD Snooping globally.

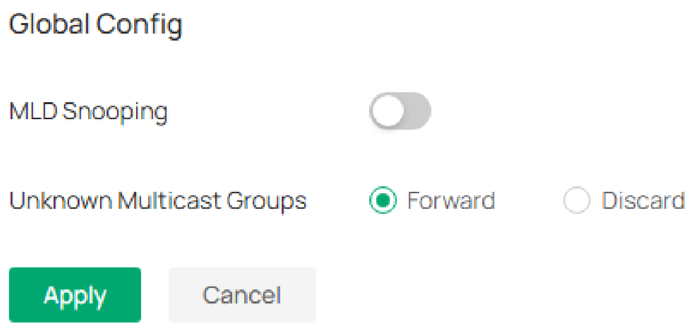
2) Configure MLD Snooping for VLANs.

3) Configure MLD Snooping on ports.

4) (Optional) Configure hosts to statically join a group.

6. 2. 1 Configure Globally

Go to Multicast > MLD Snooping > Global Config to load the following page. In Global Config, enable the feature globally and configure the parameters. Click Apply.



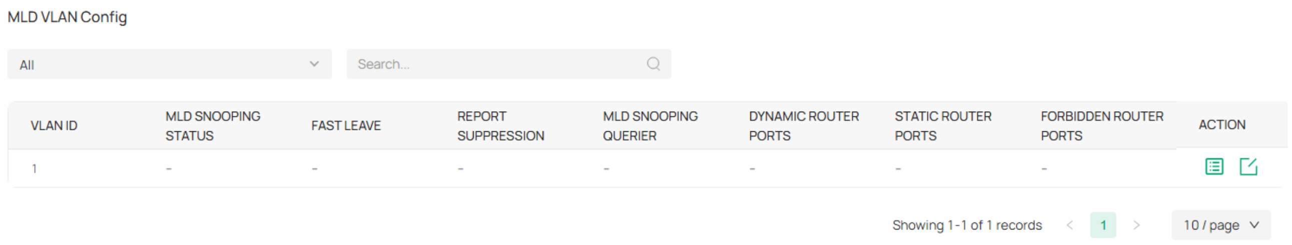
Global Config

MLD Snooping

Unknown Multicast Groups ● Forward ○ Discard

MLD Snooping	Enable MLD Snooping globally.
Unknown Multicast Groups	Set how the OLT processes data that are sent to unknown multicast groups. By default, it is Forward. Forward: The OLT will forward the data. Discard: The OLT will drop the data. Unknown multicast groups are multicast groups that do not match any of the groups announced in earlier IGMP membership reports, and thus cannot be found in the multicast forwarding table of the OLT. Note that IGMP Snooping and MLD Snooping share the setting of Unknown Multicast Groups, so you have to enable IGMP Snooping globally on the Multicast > IGMP Snooping > Global Config page at the same time.

In MLD VLAN Config, click ✎ of the desired VLAN entry in MLD VLAN Config to configure the parameters. Click Apply.



MLD VLAN Config

All

Search...

VLAN ID	MLD SNOOPING STATUS	FAST LEAVE	REPORT SUPPRESSION	MLD SNOOPING QUERIER	DYNAMIC ROUTER PORTS	STATIC ROUTER PORTS	FORBIDDEN ROUTER PORTS	ACTION
1	-	-	-	-	-	-	-	☰ ✎

Showing 1-1 of 1 records < 1 > 10 / page

VLAN ID

Displays the VLAN ID.

MLD Snooping Status

Enable or disable MLD Snooping for the VLAN.

Fast Leave

Enable or disable Fast Leave for the VLAN.

Disabled: Without Fast Leave, after a receiver sends an MLD done message (equivalent to an IGMP leave message) to leave a multicast group, the OLT will forward the done message to the Layer 3 device (the querier).

From the point of view of the querier, the port connecting to the OLT is a member port of the corresponding multicast group. After receiving the done message from the OLT, the querier will send out a configured number (Last Listener Query Count) of Multicast-Address-Specific Queries (MASQs) on that port with a configured interval (Last Listener Query Interval), and wait for MLD reports. If there are other receivers connecting to the OLT, they will response to the MASQs before the Last Listener Query Interval expires. If no reports are received after the response time of the last query expires, the querier will remove the port from the forwarding list of the corresponding multicast group.

That is, if there are other receivers connecting to the OLT, the one sent done message have to wait until the port ages out from the OLT's forwarding list of the corresponding multicast group (the maximum waiting time is decided by the Member Port Aging Time).

Enabled: With Fast Leave enabled on a VLAN, the OLT will remove the (Multicast Group, Port, VLAN) entry from the multicast forwarding table before forwarding the done message to the querier. This helps to reduce bandwidth waste since the OLT no longer sends the corresponding multicast streams to the VLAN of the port as soon as the port receives a done message from the VLAN.

Report Suppression

Enable or disable Report Suppression for the VLAN.

When enabled, the OLT will only forward the first MLD report message for each multicast group to the MLD querier and suppress subsequent MLD report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the MLD querier.

Member Port Aging Time

Specify the aging time of the member ports in the VLAN.

Once the OLT receives an MLD report message from a port, the OLT adds this port to the member port list of the corresponding multicast group. Member ports that are learned in this way are called dynamic member ports.

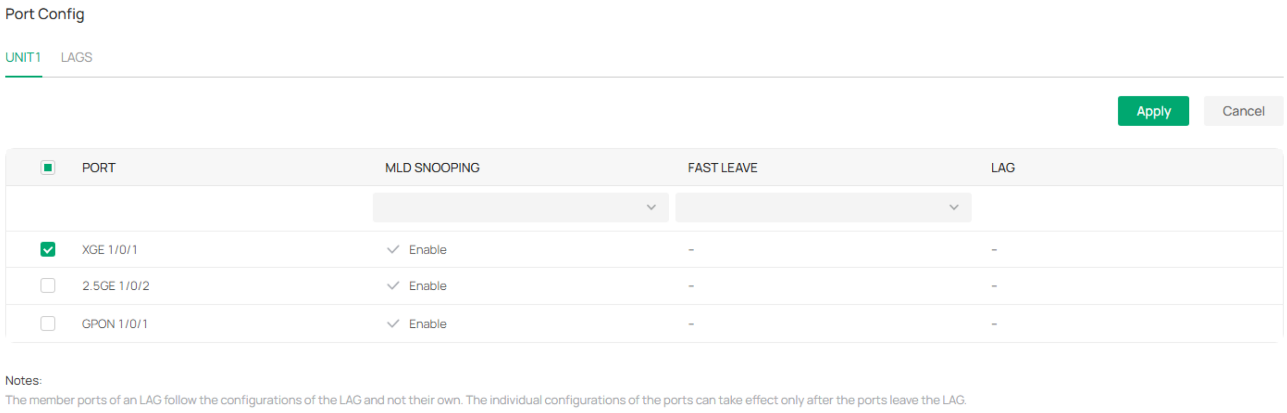
If the OLT does not receive any MLD report messages for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and delete it from the multicast forwarding table.

Router Port Aging Time	Specify the aging time of the router ports in the VLAN. Once the OLT receives an MLD general query message from a port, the OLT adds this port to the router port list. Router ports that are learned in this way are called dynamic router ports. If the OLT does not receive any MLD general query messages from a dynamic router port within the router port aging time, the OLT will no longer consider this port as a router port and delete it from the router port list.
Leave Time	Specify the leave time for the VLAN. When the OLT receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the OLT receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows: 1) If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends; 2) The Leave Time mechanism will not take effect when Fast Leave takes effect. A proper leave time value can avoid other hosts connecting to the same port of the OLT being mistakenly removed from the multicast group when only some of them want to leave.
MLD Snooping Querier	Enable or disable the MLD Snooping Querier for the VLAN. When enabled, the OLT acts as an MLD Snooping Querier for the hosts in this VLAN. A querier periodically sends a general query on the network to solicit membership information, and sends MASQs when it receives done messages from hosts.
Query Interval	With MLD Snooping Querier enabled, specify the interval between general query messages sent by the OLT.
Maximum Response Time	With MLD Snooping Querier enabled, specify the host's maximum response time to general query messages.
Last Listener Query Interval	With MLD Snooping Querier enabled, when the OLT receives a done message, it obtains the address of the multicast group that the host wants to leave from the message. Then the OLT sends out MASQs to this multicast group through the port receiving the done message. This parameter determines the interval between MASQs.
Last Listener Query Count	With MLD Snooping Querier enabled, specify the number of MASQs to be sent. If specified count of MASQs are sent and no report message is received, the OLT will delete the multicast address from the multicast forwarding table.
General Query Source IP	With MLD Snooping Querier enabled, specify the source IPv6 address of the general query messages sent by the OLT. It should be a unicast address.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. Static router ports do not age. Multicast streams and MLD packets to all groups in this VLAN will be forwarded through the static router ports. Multicast streams and MLD packets to the groups that have dynamic router ports will be also forwarded through the corresponding dynamic router ports.

Forbidden Router Ports	Select the ports to forbid them from being router ports in the VLAN.

6. 2. 2 Configure on Ports

Go to Multicast > MLD Snooping > Port Config, select one or multiple ports to configure the parameters. Click Apply.



■	PORT	MLD SNOOPING	FAST LEAVE	LAG
☑	XGE 1/0/1	✓ Enable	-	-
□	2.5GE 1/0/2	✓ Enable	-	-
□	GPON 1/0/1	✓ Enable	-	-

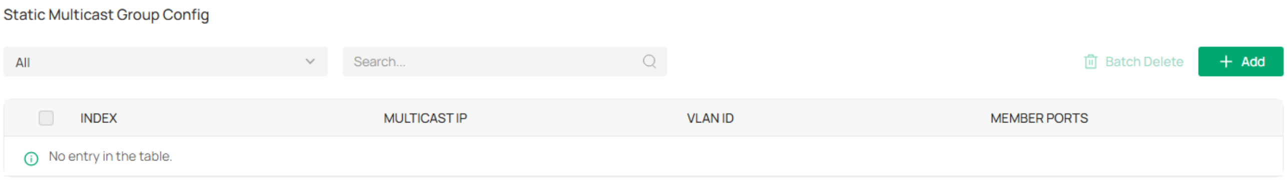
Notes:
The member ports of an LAG follow the configurations of the LAG and not their own. The individual configurations of the ports can take effect only after the ports leave the LAG.

Port (Only for Unit)	Displays the port ID.
LAG (Only for LAGS)	Displays the ID of the LAG.
MLD Snooping	Enable or disable MLD Snooping for the port.
Fast Leave	Enable or disable Fast Leave for the port. Fast Leave can be enabled on a per-port basis or per-VLAN basis. When enabled on a per-port basis, the OLT will remove the port from the corresponding multicast group of all VLANs before forwarding the leave message to the querier. You should only use Fast Leave for a port when there is a single receiver connected to the port. For more details about Fast Leave, refer to Fast Leave.
LAG (Only for Unit)	Displays which LAG the port belongs to.

6. 2. 3 Optional Configuration

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also configure hosts to statically join a group.

Go to Multicast > MLD Snooping > Static Group Config, click +Add on the upper right to load the following page. Configure the parameters. Click Create.



Static Multicast Group Config

□	INDEX	MULTICAST IP	VLAN ID	MEMBER PORTS

ⓘ No entry in the table.

Multicast IP	Specify the address of the multicast group that the hosts need to join.
VLAN ID	Specify the VLAN that the hosts are in.
Member Ports	Select the ports that the hosts are connected to. These ports will become the static member ports of the multicast group and will never age.

6. 3 Configure MVR

Overview

Multicast VLAN Registration (MVR) allows a single multicast VLAN to be shared for multicast member ports in different VLANs in IPv4 network. In IGMP Snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the Layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

There are two types of MVR modes:

- **Compatible Mode**

  In compatible mode, the MVR OLT does not forward report or leave messages from the hosts to the IGMP querier. So the IGMP querier cannot learn the multicast groups membership information from the MVR OLT. You have to statically configure the IGMP querier to transmit all the required multicast streams to the MVR OLT via the multicast VLAN.

- **Dynamic Mode**

  In dynamic mode, after receiving report or leave messages from the hosts, the MVR OLT will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So the IGMP querier can learn the multicast groups membership information through the report and leave messages, and transmit the multicast streams to the MVR OLT via the multicast VLAN according to the multicast forwarding table.

Configuration

To configure MVR Snooping for IPv6, follow these steps:

1) Configure 802.1Q VLANs and MVR globally.
2) Add multicast groups to MVR.
3) Configure MVR on ports.
4) (Optional) Statically add ports to MVR groups.

Configuration Guidelines:

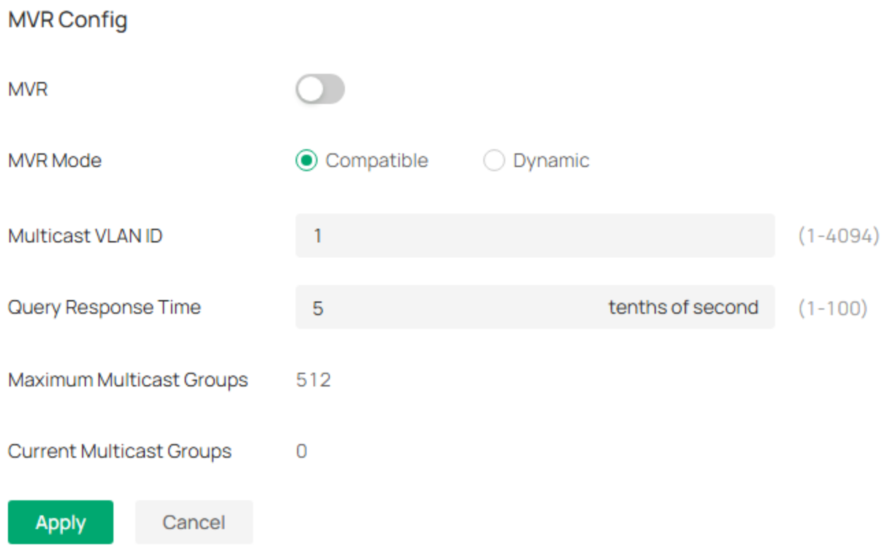
- MVR does not support IGMPv3 messages.
- Do not configure MVR on private VLAN ports, otherwise MVR cannot take effect.
- MVR operates on the underlying mechanism of IGMP Snooping, but the two features operate independently of each other. Both protocols can be enabled on a port at the same time. When both are enabled, MVR listens to the report and leave messages only for the multicast groups configured in MVR. All other multicast groups are managed by IGMP Snooping.

6. 3. 1 Configure Globally

1. Before configuring MVR, create an 802.1Q VLAN as the multicast VLAN.

   Add all source ports (uplink ports that receive multicast data from the router) to the multicast VLAN as tagged ports. Configure 802.1Q VLANs for the receiver ports (ports that are connecting to the hosts) according to network requirements. Note that receiver ports can only belong to one VLAN and cannot be added to the multicast VLAN. For details, refer to Chapter 4. 4. 1. 802.1Q VLAN.

2. Go to Multicast > MVR > MVR Config to load the following page and configure the parameters. Click Apply.



MVR Config

MVR: off

MVR Mode: ● Compatible ○ Dynamic

Multicast VLAN ID: 1 (1-4094)

Query Response Time: 5 tenths of second (1-100)

Maximum Multicast Groups: 512

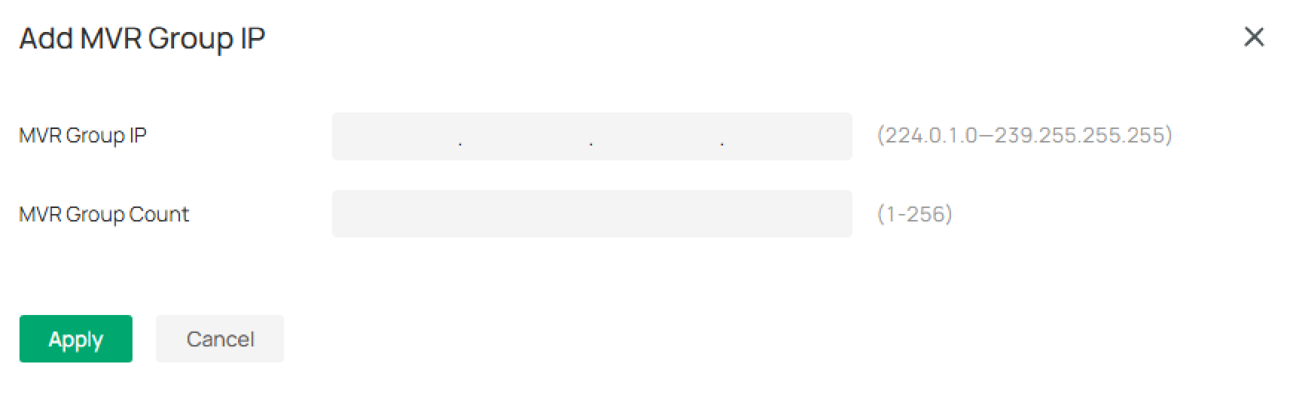
Current Multicast Groups: 0

MVR	Enable or disable MVR globally.
MVR Mode	Specify the MVR mode as compatible or dynamic. Compatible: In this mode, the OLT does not forward report or leave messages from the hosts to the IGMP querier. This means IGMP querier cannot learn the multicast groups' membership information from the OLT. The IGMP querier must be statically configured to transmit all the required multicast streams to the OLT via the multicast VLAN. Dynamic: In this mode, after receiving report or leave messages from the hosts, the OLT will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). The IGMP querier can learn the multicast groups' membership information through the report and leave messages, and transmit the multicast streams to the OLT via the multicast VLAN according to the multicast forwarding table.
Multicast VLAN ID	Specify an existing 802.1Q VLAN as the multicast VLAN.
Query Response Time	Specify the maximum time to wait for IGMP report on a receiver port before removing the port from multicast group membership.
Maximum Multicast Groups	Displays the maximum number of multicast groups that can be configured on the OLT.

Current Multicast Groups	Displays the current number of multicast groups that have been configured on the OLT.

6. 3. 2 Add Multicast Groups

1. Go to Multicast > MVR > MVR Group Config, click +Add on the upper right to load the following page. Configure the parameters. Click Create.



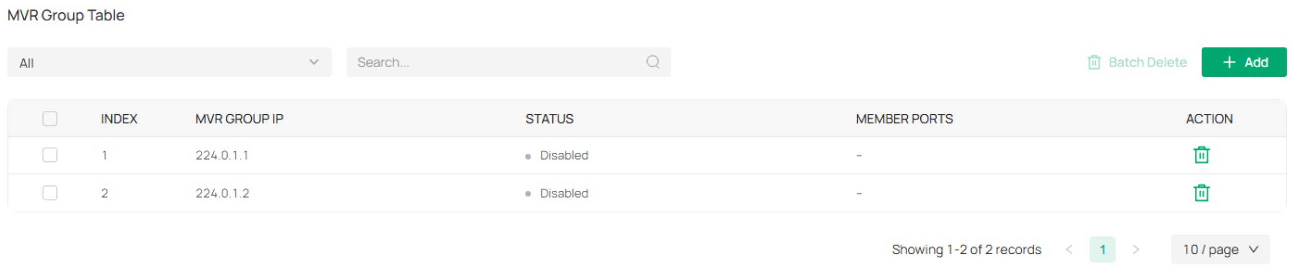
Add MVR Group IP ✕

MVR Group IP . . . (224.0.1.0—239.255.255.255)

MVR Group Count (1-256)

MVR Group IP / MVR Group Count	Specify the start IP address and the number of contiguous series of multicast groups. Multicast data sent to the address specified here will be sent to all source ports on the OLT and all receiver ports that have requested to receive data from that multicast address.

2. The added multicast groups will appear in the MVR group table.



MVR Group Table

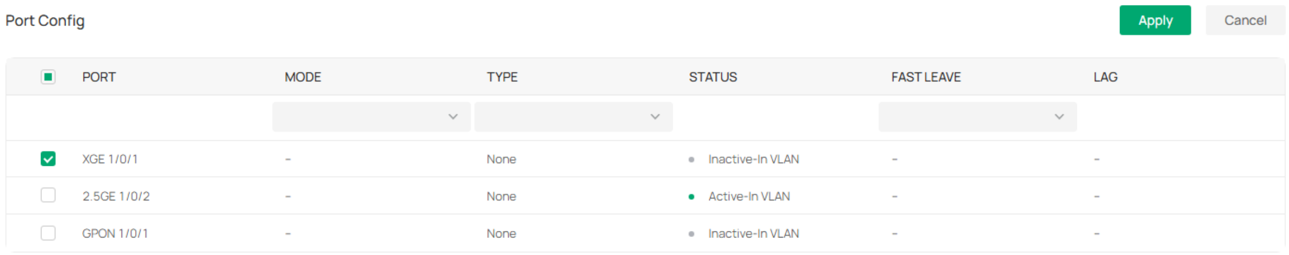
□	INDEX	MVR GROUP IP	STATUS	MEMBER PORTS	ACTION
□	1	224.0.1.1	Disabled	-	🗑
□	2	224.0.1.2	Disabled	-	🗑

Showing 1-2 of 2 records < 1 > 10 / page

MVR Group IP	Displays the IP address of multicast group.
Status	Displays the status of the MVR group. In compatible mode, all the MVR groups are added manually, so the status is always active. In dynamic mode, there are two status: Disabled: The MVR group is added successfully, but the source port has not received any query messages from this multicast group. Enabled: The MVR group is added successfully and the source port has received query messages from this multicast group.
Member	Displays the member ports in this MVR group.

6. 3. 3 Configure on Ports

Go to Multicast > MVR > Port Config, select one or multiple ports to configure the parameters. Click Apply.



Port Config

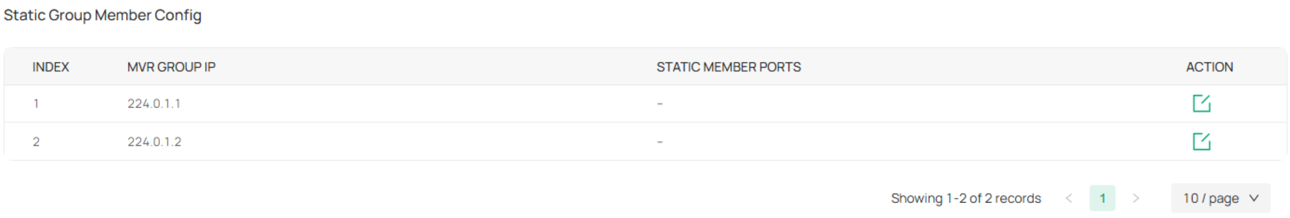
■	PORT	MODE	TYPE	STATUS	FAST LEAVE	LAG
☑	XGE 1/0/1	-	None	● Inactive-In VLAN	-	-
□	2.5GE 1/0/2	-	None	● Active-In VLAN	-	-
□	GPON 1/0/1	-	None	● Inactive-In VLAN	-	-

Port	Displays the port ID.
Mode	Enable or disable MVR for the selected ports.
Type	Configure the port type. None: The port is a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation will be unsuccessful. Source: Configure the uplink ports that receive and send multicast data on the multicast VLAN as source ports. Source ports should belong to the multicast VLAN. In compatible mode, source ports will be automatically added to all multicast groups, while in dynamic mode, you need to manually add them to the corresponding multicast groups. Receiver: Configure the ports that are connecting to the hosts as receiver ports. A receiver port can only belong to one VLAN, and cannot belong to the multicast VLAN. In both modes, the OLT will add or remove the receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts.
Status	Displays the port status. Active/InVLAN: The port is physically up and in one or more VLANs. Active/NotInVLAN: The port is physically up and not in any VLAN. Inactive/InVLAN: The port is physically down and in one or more VLANs. Inactive/NotInVLAN: The port is physically down and not in any VLAN.
Fast Leave	Enable or disable Fast Leave for the selected ports. Only receiver ports support Fast Leave. Before enabling Fast Leave for a port, make sure there is only a single receiver device connecting to the port.
LAG	Displays which LAG the port belongs to.

6. 3. 4 Optional Configuration

The OLT adds or removes receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts. You can also statically add a receiver port to an MVR group.

Go to Multicast > MVR > Static Group Members, click ☑ of the desired MVR group to configure the parameters. Click Save.



Static Group Member Config

INDEX	MVR GROUP IP	STATIC MEMBER PORTS	ACTION
1	224.0.1.1	-	☑
2	224.0.1.2	-	☑

Showing 1-2 of 2 records < 1 > 10 / page

MVR Group IP	Displays the IP of the MVR group.
Static Member Ports	Select the ports to be the static member ports by clicking the port icons below.

6. 4 Configure Multicast Filtering

Overview

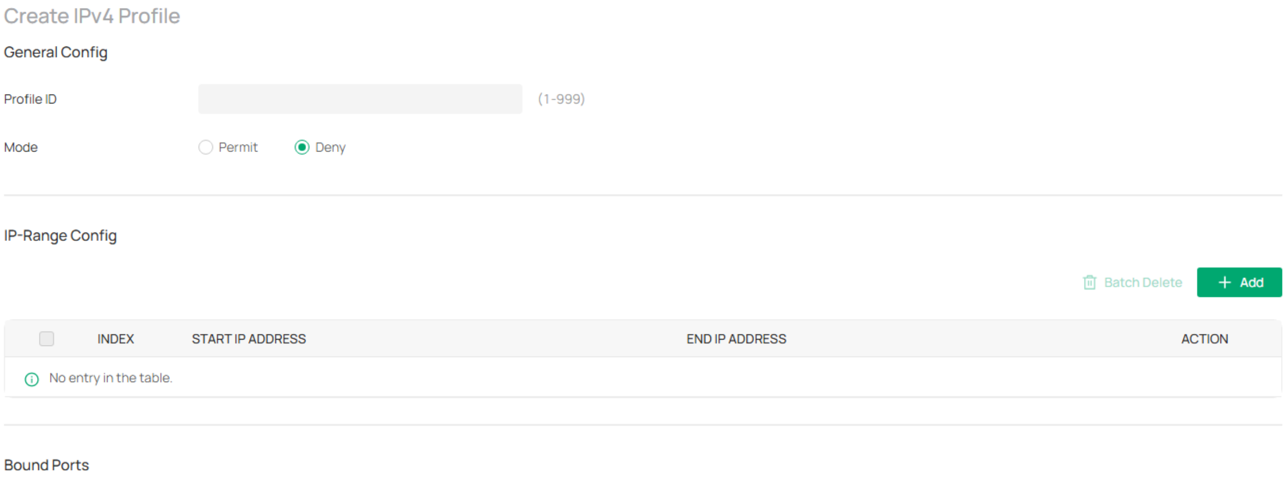
Multicast Filtering allows you to control the set of multicast groups to which a host can belong. You can filter multicast joins on a per-port basis by configuring IP multicast profiles (IGMP profiles or MLD profiles) and associating them with individual ports.

You can create multicast profiles for both IPv4 and IPv6 network. With multicast profile, the OLT can define a allow list or deny list of multicast groups so as to filter multicast sources. The process for creating multicast profiles for IPv4 and IPv6 are similar. The following configuration take creating an IPv4 profile as an example.

Configuration

6. 4. 1 Configure IPv4 Multicast Filtering

1. Go to Multicast > Multicast Filtering > IPv4, and click +Add on the upper right to load the following page. In General Config, configure the parameters.



Create IPv4 Profile

General Config

Profile ID (1-999)

Mode ○ Permit ● Deny

IP-Range Config

□	INDEX	START IP ADDRESS	END IP ADDRESS	ACTION
No entry in the table.				

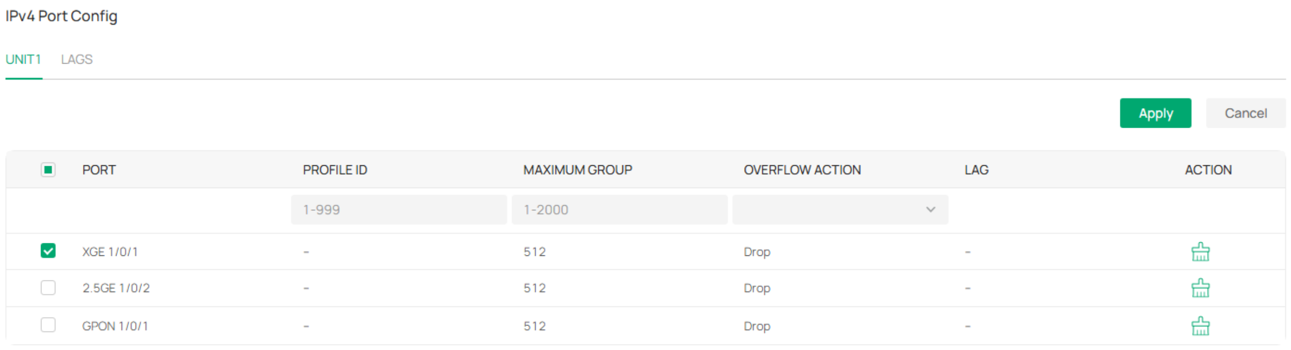
Bound Ports

Profile ID	Enter a profile ID between 1 and 999.
Mode	Select the filtering mode. Permit: Acts as a allow list and only allows specific member ports to join specified multicast groups. Deny: Acts as a deny list and prevents specific member ports from joining specific multicast groups.

2. In IP-Range List, click +Add on the upper right to load the page. Configure the start and end IP address of the multicast groups for filtering. Click Create.

3. In Bound Ports, select your desired ports to bind to the profile by clicking the port icons below. Click Save.

4. Go to Multicast > Multicast Filtering > IPv4. In IPv4 Port Config, select one or multiple ports and configure the parameters. Click Apply.



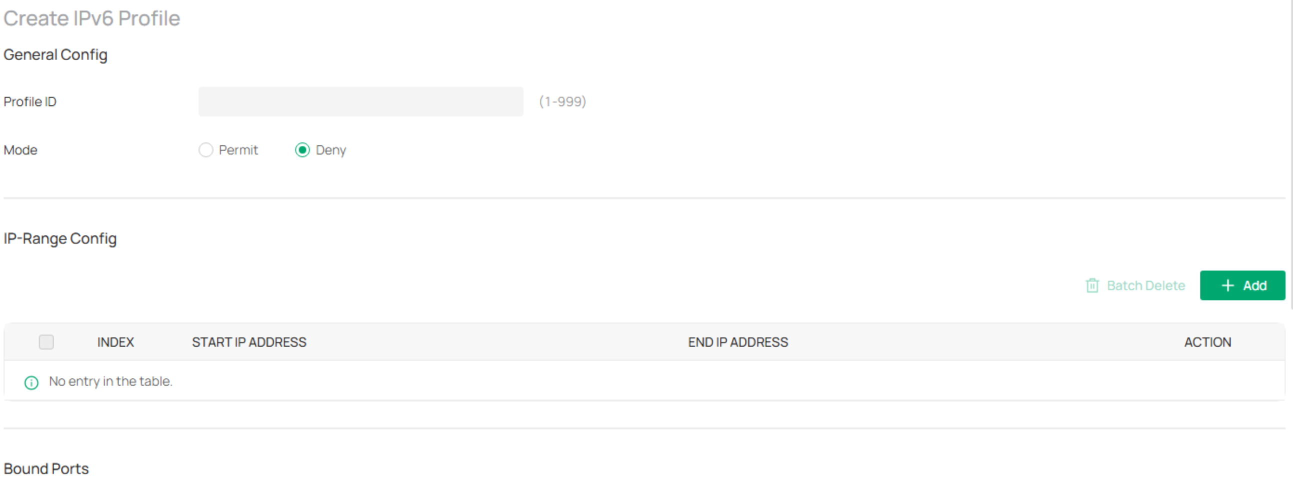
IPv4 Port Config

■	PORT	PROFILE ID	MAXIMUM GROUP	OVERFLOW ACTION	LAG	ACTION
		1-999	1-2000			
☑	XGE 1/0/1	-	512	Drop	-	🧹
□	2.5GE 1/0/2	-	512	Drop	-	🧹
□	GPON 1/0/1	-	512	Drop	-	🧹

Port (Only for Unit)	Displays the port ID.
LAG (Only for LAGS)	Displays the ID of the LAG.
Profile ID	Specify the ID of an existing profile to bind the profile to the selected ports. One port can only be bound to one profile.
Maximum Groups	Enter the number of multicast groups the port can join. Valid values are from 0 to 2000.
Overflow Action	Select the action the OLT will take with the new multicast member groups when the number of multicast groups the port has joined exceeds the maximum. Drop: Drop all subsequent membership report messages to prevent the port joining a new multicast groups. Replace: Replace the existing multicast group that has the lowest multicast MAC address with the new multicast group.
LAG (Only for Unit)	Displays which LAG the port belongs to.
Operation	Click 🧹 to clear the binding between the profile and the port.

6. 4. 2 Configure IPv6 Multicast Filtering

1. Go to Multicast > Multicast Filtering > IPv6, and click +Add on the upper right to load the following page. In General Config, configure the parameters.



Create IPv6 Profile

General Config

Profile ID (1-999)

Mode ○ Permit ● Deny

IP-Range Config

Batch Delete + Add

□	INDEX	START IP ADDRESS	END IP ADDRESS	ACTION
No entry in the table.				

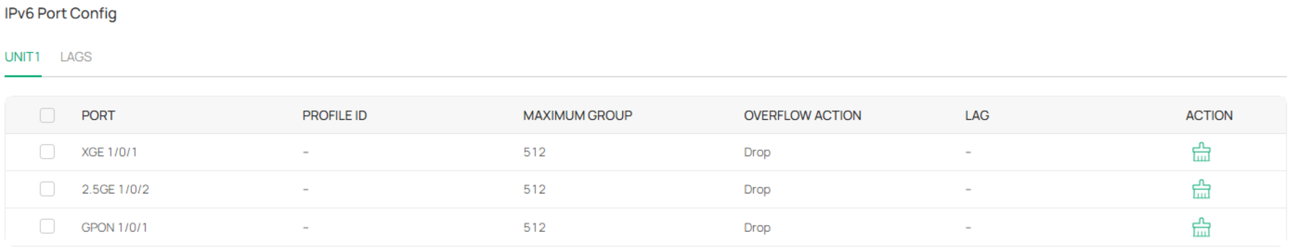
Bound Ports

Profile ID	Enter a profile ID between 1 and 999.
Mode	Select the filtering mode. Permit: Acts as a allow list and only allows specific member ports to join specified multicast groups. Deny: Acts as a deny list and prevents specific member ports from joining specific multicast groups.

2. In IP-Range List, click +Add on the upper right to load the page. Configure the start and end IP address of the multicast groups for filtering. Click Create.

3. In Bound Ports, select your desired ports to bind to the profile by clicking the port icons below. Click Save.

4. Go to Multicast > Multicast Filtering > IPv6. In IPv6 Port Config, select one or multiple ports and configure the parameters. Click Apply.



IPv6 Port Config

UNIT1 LAGS

□	PORT	PROFILE ID	MAXIMUM GROUP	OVERFLOW ACTION	LAG	ACTION
□	XGE 1/0/1	-	512	Drop	-	
□	2.5GE 1/0/2	-	512	Drop	-	
□	GPON 1/0/1	-	512	Drop	-	

Port (Only for Unit)	Displays the port ID.
LAG (Only for LAGS)	Displays the ID of the LAG.
Profile ID	Specify the ID of an existing profile to bind the profile to the selected ports. One port can only be bound to one profile.
Maximum Groups	Enter the number of multicast groups the port can join. Valid values are from 0 to 2000.

Overflow Action	Select the action the OLT will take with the new multicast member groups when the number of multicast groups the port has joined exceeds the maximum. Drop: Drop all subsequent membership report messages to prevent the port joining a new multicast groups. Replace: Replace the existing multicast group that has the lowest multicast MAC address with the new multicast group.
LAG (Only for Unit)	Displays which LAG the port belongs to.
Operation	Click 🧹 to clear the binding between the profile and the port.

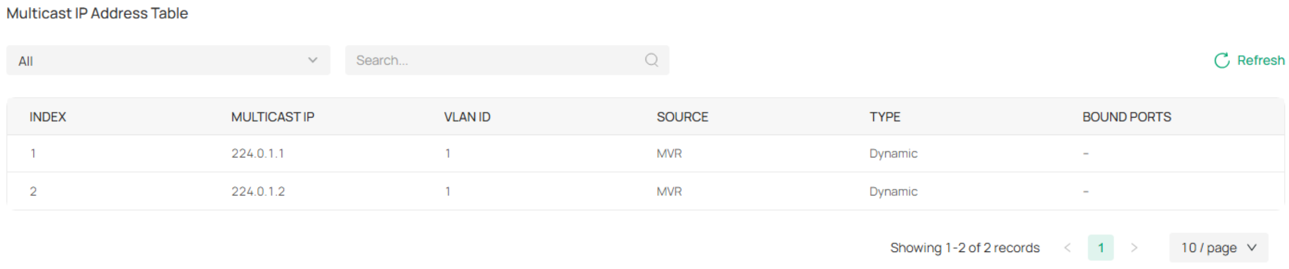
6. 5 View Multicast Snooping Information

Overview

In Multicast Info, you can view information and statistics of the IPv4 and IPv6 multicast. Also, you can view statistics on each port and set auto refresh for the statistics table.

6. 5. 1 View IPv4 Multicast Table

Go to Multicast > Multicast Info > IPv4 Multicast Table to load the following page and it displays all the valid Multicast IP-VLAN-Port entries.



Multicast IP Address Table

INDEX	MULTICAST IP	VLAN ID	SOURCE	TYPE	BOUND PORTS
1	224.0.1.1	1	MVR	Dynamic	-
2	224.0.1.2	1	MVR	Dynamic	-

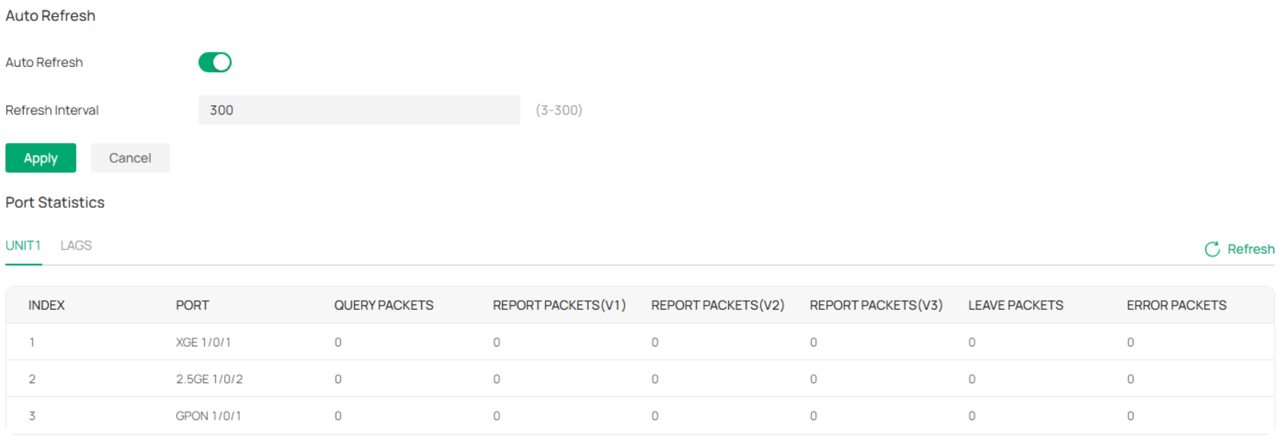
Showing 1-2 of 2 records

Multicast IP	Displays the multicast source IP address.
VLAN ID	Displays the ID of the VLAN the multicast group belongs to.
Source	Displays the source of the multicast entry. IGMP Snooping: The multicast entry is learned by IGMP Snooping. MVR: The multicast entry is learned by MVR.
Type	Displays how the multicast entry is generated. Dynamic: The entry is dynamically learned. All the member ports are dynamically added to the multicast group. Static: The entry is manually added. All the member ports are manually added to the multicast group. Mix: The entry is dynamically learned or manually learned, and some of the member ports are manually added, while some are dynamically added to the multicast group.
Bound Ports	All ports in the multicast group, including router ports and member ports.

6. 5. 2 View IPv4 Multicast Statistics on Each Port

1. Go to Multicast > Multicast Info > IPv4 Multicast Statistics to load the following page and

configure the parameters. Click Apply.



Auto Refresh

Auto Refresh: on

Refresh Interval: 300 (3-300)

Port Statistics

INDEX	PORT	QUERY PACKETS	REPORT PACKETS(V1)	REPORT PACKETS(V2)	REPORT PACKETS(V3)	LEAVE PACKETS	ERROR PACKETS
1	XGE 1/0/1	0	0	0	0	0	0
2	2.5GE 1/0/2	0	0	0	0	0	0
3	GPON 1/0/1	0	0	0	0	0	0

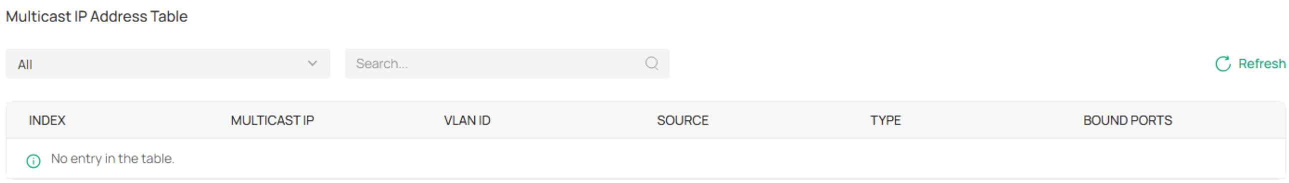
Auto Refresh	Enable or disable Auto Refresh. When enabled, the OLT will automatically refresh the multicast statistics.
Refresh Interval	After Auto Refresh is enabled, specify the time interval for the OLT to refresh the multicast statistics.

2. In Port Statistics, view IPv4 multicast statistics on each port.

Query Packets	Displays the number of query packets received by the port.
Report Packets (v1)	Displays the number of IGMPv1 report packets received by the port.
Report Packets (v2)	Displays the number of IGMPv2 report packets received by the port.
Report Packets (v3)	Displays the number of IGMPv3 report packets received by the port.
Leave Packets	Displays the number of leave packets received by the port.
Error Packets	Displays the number of error packets received by the port.

6. 5. 3 View IPv6 Multicast Table

Go to Multicast > Multicast Info > IPv6 Multicast Table to load the following page and it displays all the valid Multicast IP-VLAN-Port entries.



Multicast IP Address Table

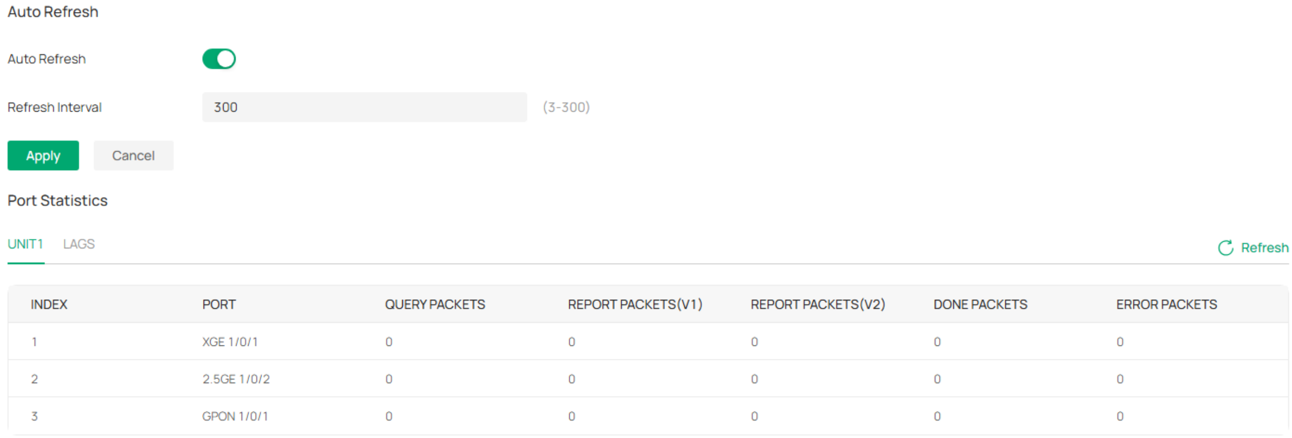
INDEX	MULTICAST IP	VLAN ID	SOURCE	TYPE	BOUND PORTS
No entry in the table.					

Multicast IP	Displays the multicast source IP address.
VLAN ID	Displays the ID of the VLAN the multicast group belongs to.

Source	Displays the source of the multicast entry. MLD Snooping: The multicast entry is learned by MLD Snooping.
Type	Displays how the multicast entry is generated. Dynamic: The entry is dynamically learned. All the member ports are dynamically added to the multicast group. Static: The entry is manually added. All the member ports are manually added to the multicast group. Mix: The entry is dynamically learned or manually learned, and some of the member ports are manually added, while some are dynamically added to the multicast group.
Bound Ports	All ports in the multicast group, including router ports and member ports.

6. 5. 4 View IPv6 Multicast Statistics on Each Port

1. Go to Multicast > Multicast Info > IPv6 Multicast Statistics to load the following page and configure the parameters. Click Apply.



Auto Refresh

Auto Refresh: ●

Refresh Interval: 300 (3-300)

Port Statistics

INDEX	PORT	QUERY PACKETS	REPORT PACKETS(V1)	REPORT PACKETS(V2)	DONE PACKETS	ERROR PACKETS
1	XGE 1/0/1	0	0	0	0	0
2	2.5GE 1/0/2	0	0	0	0	0
3	GPON 1/0/1	0	0	0	0	0

Auto Refresh	Enable or disable Auto Refresh. When enabled, the OLT will automatically refresh the multicast statistics.
Refresh Interval	After Auto Refresh is enabled, specify the time interval for the OLT to refresh the multicast statistics.

2. In Port Statistics, view IPv6 multicast statistics on each port.

Query Packets	Displays the number of query packets received by the port.
Report Packets (v1)	Displays the number of MLDv1 packets received by the port.
Report Packets (v2)	Displays the number of MLDv2 packets received by the port.
Done Packets	Displays the number of done packets received by the port.
Error Packets	Displays the number of error packets received by the port.

Chapter 7

Configure QoS

This chapter guides you on how to configure QoS features. The chapter includes the following sections:

7. 1 Configure Class of Service

Overview

With network scale expanding and applications developing, internet traffic is dramatically increased, thus resulting in network congestion, packet drops and long transmission delay. Typically, networks treat all traffic equally on FIFO (First In First Out) delivery basis, but nowadays many special applications like VoD, video conferences, VoIP, etc, require more bandwidth or shorter transmission delay to guarantee the performance.

With QoS (Quality of Service) technology, you can classify and prioritize network traffic to provide differentiated services to certain types of traffic. The OLT classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduler settings to implement QoS function. In Priority Mode, three modes are supported: Port Priority, 802.1p Priority and DSCP Priority. In Scheduler Mode, Two scheduler types are supported: Strict and Weighted.

Note: The member ports of an LAG follow the configurations of the LAG and not their own. The individual configurations of the ports can take effect only after the ports leave the LAG

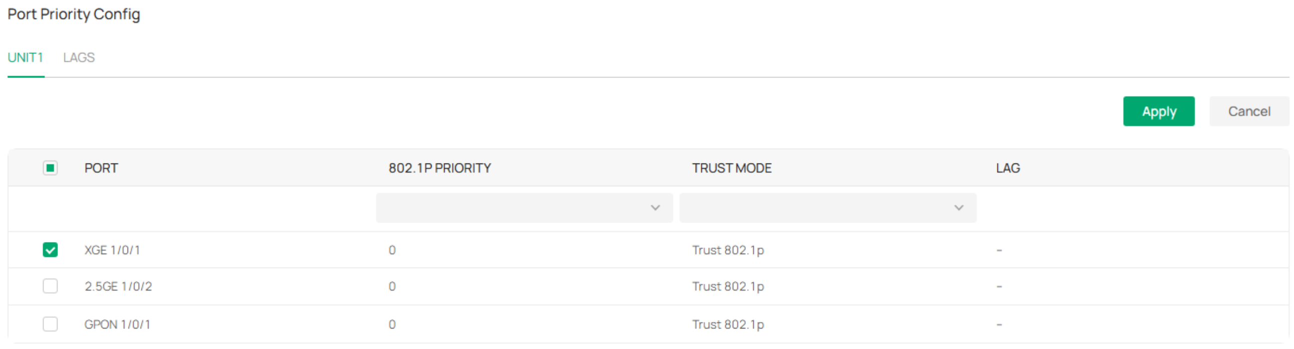
7. 1. 1 Configure Port Priority

Overview

In Port Priority mode, the OLT prioritizes packets according to their ingress ports, regardless of the packet field or type.

Configuration

1. Go to QoS > Class of Service > Port Priority to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Priority Config

■	PORT	802.1P PRIORITY	TRUST MODE	LAG
☑	XGE 1/0/1	0	Trust 802.1p	-
□	2.5GE 1/0/2	0	Trust 802.1p	-
□	GPON 1/0/1	0	Trust 802.1p	-

802.1p Priority	Specify the priority level for the traffic through the chosen port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p priority mapping.

Trust Mode	Select the Trust mode as Trust 802.1p. In this mode, the tagged packets will be processed according to the 802.1p priority configuration and the untagged packets will be processed according to the port priority configuration.

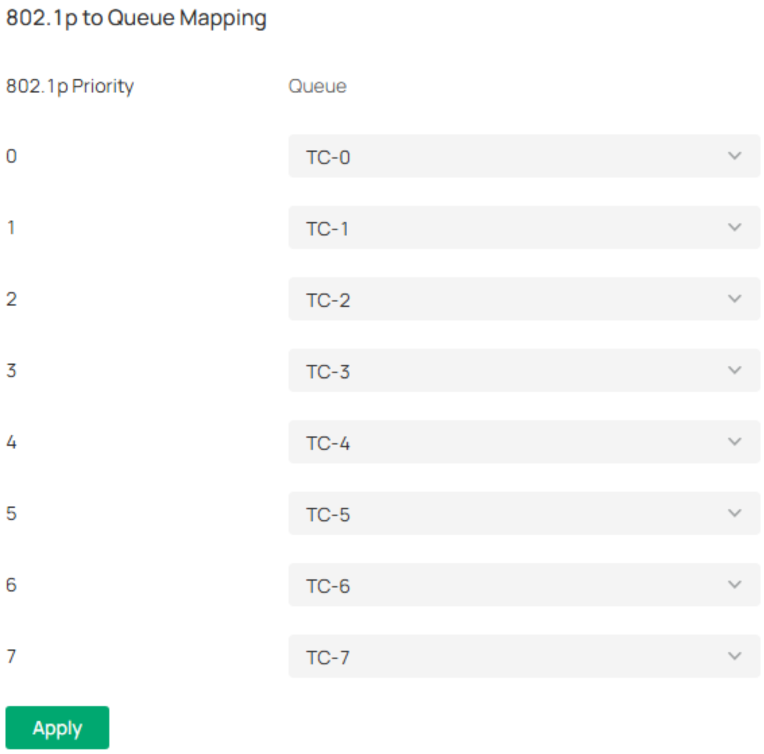
7. 1. 2 Configure 802.1p Priority

Overview

802.1p defines the first three bits in 802.1q Tag as PRI field. The PRI values are from 0 to 7. 802.1p priority determines the priority of packets based on the PRI value. In this mode, the OLT only prioritizes packets with VLAN tag, regardless of the IP header of the packets.

Configuration

1. Go to QoS > Class of Service > 802.1p Priority to load the following page. Configure the queue. Click Apply.

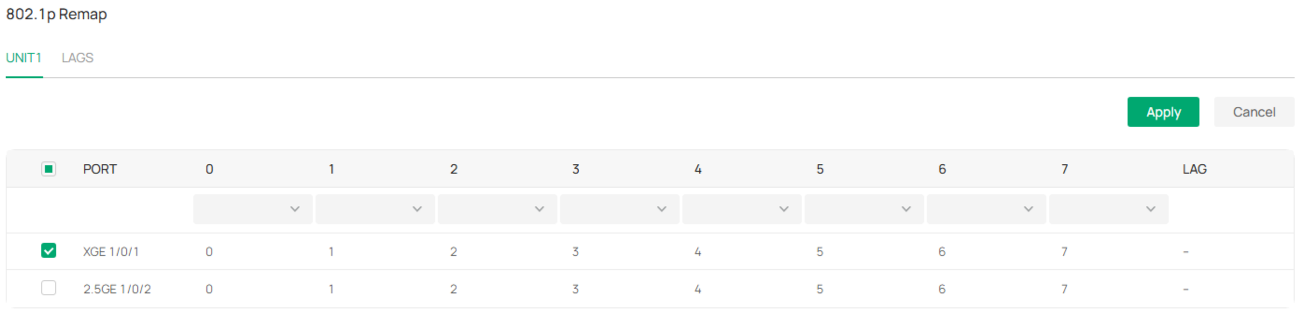


802.1p to Queue Mapping

802.1p Priority	Queue
0	TC-0
1	TC-1
2	TC-2
3	TC-3
4	TC-4
5	TC-5
6	TC-6
7	TC-7

0/1/2/3/4/5/6/7	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

2. (Optional) In 802.1p Remap, Select one or multiple ports to configure the parameters. Click Apply.



802.1p Remap

■	PORT	0	1	2	3	4	5	6	7	LAG
☑	XGE 1/0/1	0	1	2	3	4	5	6	7	-
□	2.5GE 1/0/2	0	1	2	3	4	5	6	7	-

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

Select the number of 802.1p priority to which the desired 802.1p priority will be remapped. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the OLT detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map.

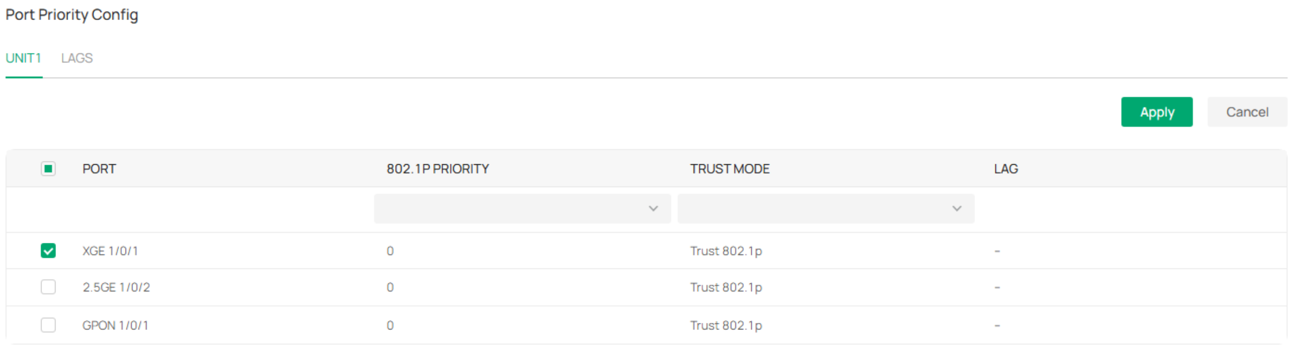
7. 1. 3 Configure DSCP Priority

Overview

DSCP priority determines the priority of packets based on the ToS (Type of Service) field in their IP header. RFC2474 re-defines the ToS field in the IP packet header as DS field. The first six bits (bit 0-bit 5) of the DS field is used to represent DSCP priority. The DSCP values are from 0 to 63. In this mode, the OLT only prioritizes IP packets.

Configuration

1. Go to QoS > Class of Service > Port Priority to load the following page. Select one or multiple ports to configure the parameters. Click Apply.

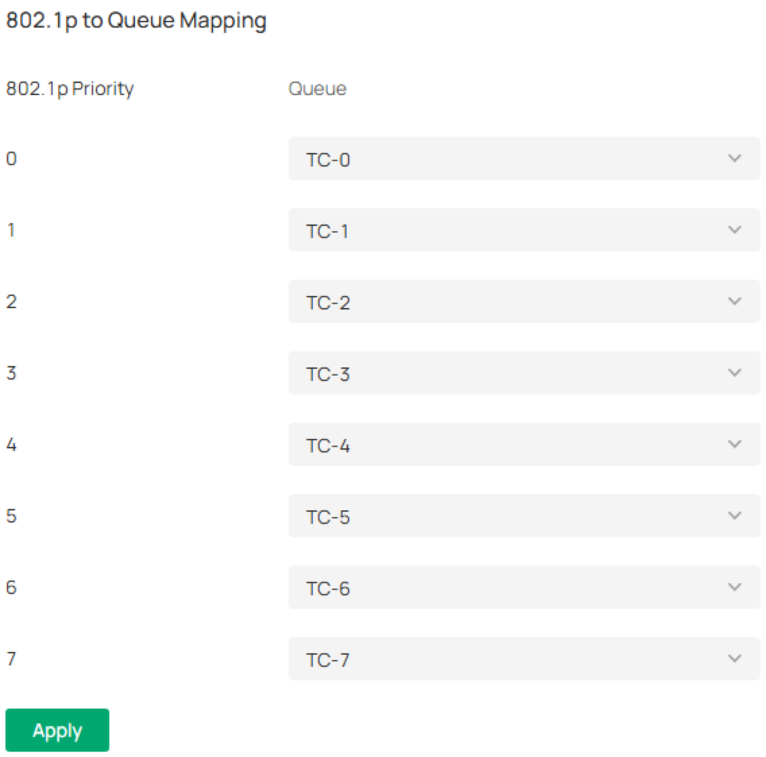


Port Priority Config

■	PORT	802.1P PRIORITY	TRUST MODE	LAG
☑	XGE 1/0/1	0	Trust 802.1p	-
□	2.5GE 1/0/2	0	Trust 802.1p	-
□	GPON 1/0/1	0	Trust 802.1p	-

802.1p Priority	Specify the priority level for the traffic through the chosen port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p priority mapping.
Trust Mode	Select the Trust mode as Trust DSCP. In this mode, the IP packets will be processed according to the DSCP priority configuration and the non-IP packets will be processed according to the port priority configuration.

2. Go to QoS > Class of Service > 802.1p Priority to load the following page. Configure the queue. Click Apply.

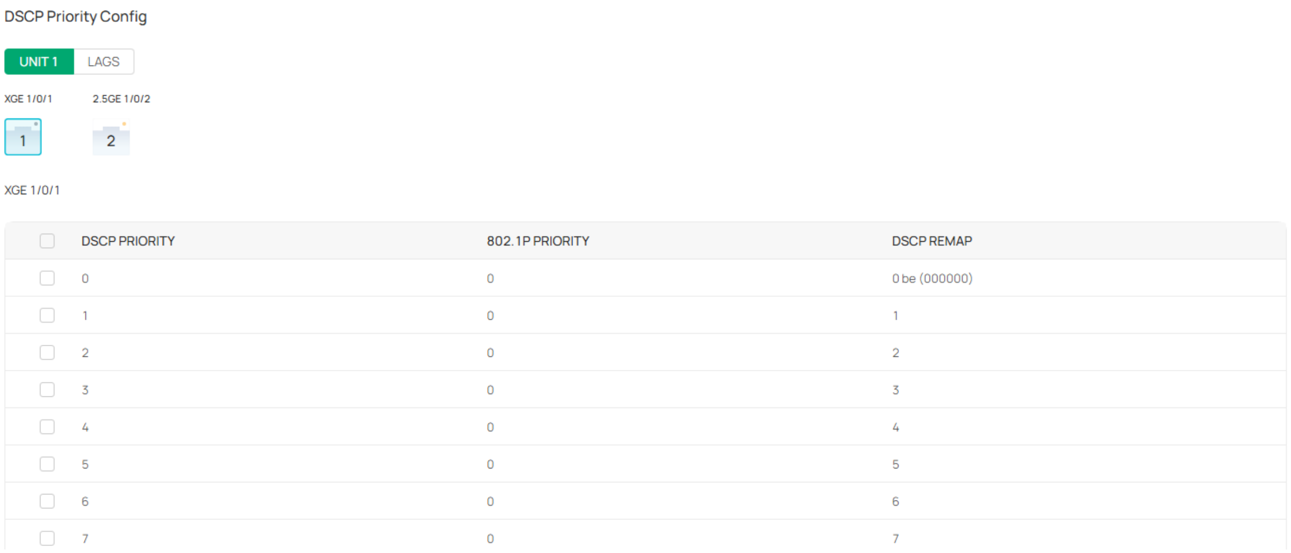


802.1p to Queue Mapping

802.1p Priority	Queue
0	TC-0
1	TC-1
2	TC-2
3	TC-3
4	TC-4
5	TC-5
6	TC-6
7	TC-7

1/2/3/4/5/6/7	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service. IEEE 802.1p standard defines three bits in 802.1Q tag as PRI filed. The PRI values are called 802.1p priority and used to represent the priority of the layer 2 packets. This function requires packets with VLAN tags.
Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

3. Go to QoS > Class of Service > DSCP Priority to load the following page. Select one port to configure the parameters. Click Apply.



DSCP Priority Config

XGE 1/0/1

□	DSCP PRIORITY	802.1P PRIORITY	DSCP REMAP
□	0	0	0 be (000000)
□	1	0	1
□	2	0	2
□	3	0	3
□	4	0	4
□	5	0	5
□	6	0	6
□	7	0	7

DSCP Priority	Displays the number of DSCP priority. DSCP Priority is used to classify the packets based on the value of DSCP, and map them to different queues. ToS (Type of Service) is a part of IP header, and DSCP uses the first six bits of ToS to represent the priority of IP packets. The DSCP values range from 0 to 63.
802.1p Priority	Specify the DSCP to 802.1p mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p to queue mappings.
DSCP Remap	(Optional) Select the DSCP priority to which the desired DSCP priority will be remapped for the port. When the OLT detects the packets with desired DSCP value, it will modify the packets' DSCP value according to the map.

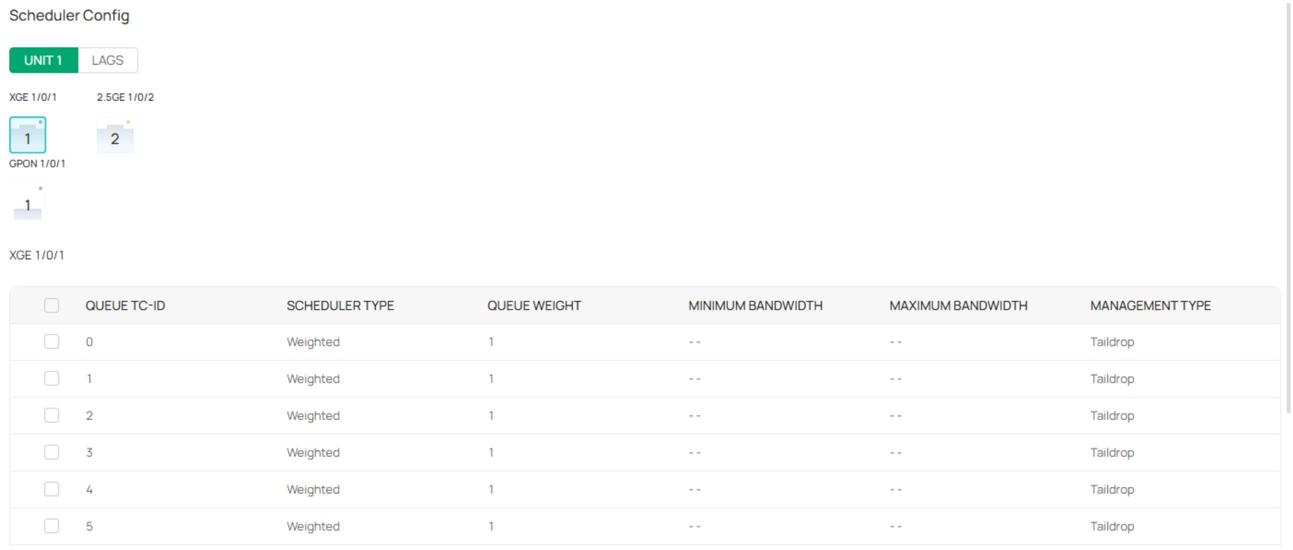
7. 1. 4 Configure the Scheduler Settings

Overview

When congestion occurs, the scheduler settings helps control the forwarding sequence of different TC queues.

Configuration

Go to QoS > Class of Service > Scheduler Settings to load the following page. Select one port and the desired queue to configure the parameters. Click Apply.



Scheduler Config

XGE 1/0/1

□	QUEUE TC-ID	SCHEDULER TYPE	QUEUE WEIGHT	MINIMUM BANDWIDTH	MAXIMUM BANDWIDTH	MANAGEMENT TYPE
□	0	Weighted	1	--	--	Taildrop
□	1	Weighted	1	--	--	Taildrop
□	2	Weighted	1	--	--	Taildrop
□	3	Weighted	1	--	--	Taildrop
□	4	Weighted	1	--	--	Taildrop
□	5	Weighted	1	--	--	Taildrop

Queue TC-id	Displays the ID number of priority Queue.
Scheduler Type	Select the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. Strict: In this mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. Weighted: In this mode, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.
Queue Weight	Specify the queue weight for the desired queue. This value can be set only in the Weighted mode. The valid values are from 1 to 127.
Minimum/Maximum Bandwidth	Specify the minimum/maximum guaranteed bandwidth for the desired queue. The valid values are from 0 to 100 and 0 means Minimum/Maximum Bandwidth is disabled. If the queue bandwidth calculated according to the weight is smaller than the minimum/maximum bandwidth, the OLT will be forced to allocated the minimum/maximum bandwidth to the queue, and the other queue will share the rest bandwidth based on the weight.
Management Type	Displays the Management Type for the queues. The OLT supports Taildrop mode. When the traffic exceeds the limit, the additional traffic will be dropped.

7. 2 Configure Bandwidth Control

Overview

Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. It includes two features: Rate Limit and Storm Control.

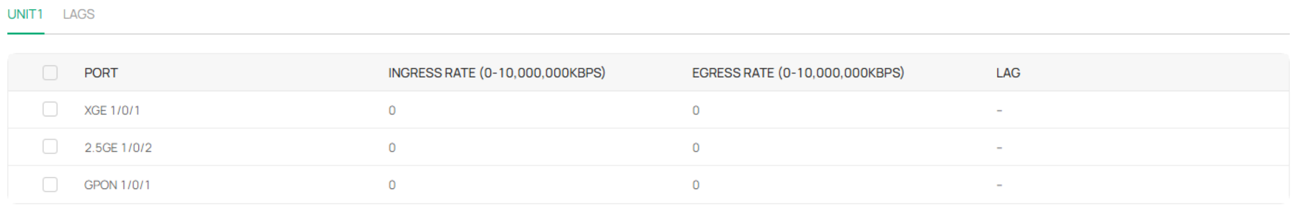
7. 2. 1 Configure Rate Limit

Overview

Rate limit functions to limit the ingress/egress traffic rate on each port. In this way, the network bandwidth can be reasonably distributed and utilized.

Configuration

Go to QoS > Bandwidth Control > Rate Limit to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



□	PORT	INGRESS RATE (0-10,000,000KBPS)	EGRESS RATE (0-10,000,000KBPS)	LAG
□	XGE 1/0/1	0	0	-
□	2.5GE 1/0/2	0	0	-
□	GPON 1/0/1	0	0	-

Ingress Rate (0-10,000,000Kbps)	Specify the upper rate limit for receiving packets on the port. The rate ranges from 1 to 10,000,000 kbps, and is rounded off to the nearest multiple of 64. 0 means the ingress rate limit is disabled.
Egress Rate (0-10,000,000Kbps)	Specify the upper rate limit for sending packets on the port. The rate ranges from 1 to 10,000,000 kbps, and is rounded off to the nearest multiple of 64. 0 means the egress rate limit is disabled.

Note:

1. The member ports of an LAG follow the configurations of the LAG and not their own. The individual configurations of the ports can take effect only after the ports leave the LAG.

2. You cannot enable Storm Control and Ingress Rate control at the same time for a port.

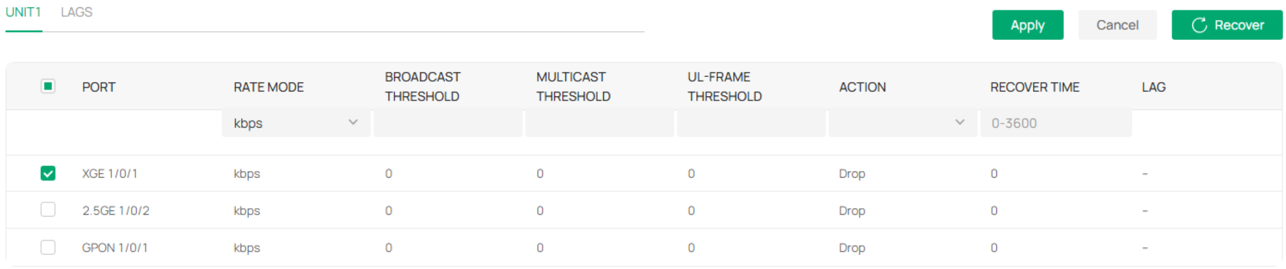
7. 2. 2 Configure Storm Control

Overview

Storm Control function allows the OLT to monitor broadcast packets, multicast packets and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the packets exceeds the set rate, the packets will be automatically discarded to avoid network broadcast storm.

Configuration

Go to QoS > Bandwidth Control > Storm Control to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



▣	PORT	RATE MODE	BROADCAST THRESHOLD	MULTICAST THRESHOLD	UL-FRAME THRESHOLD	ACTION	RECOVER TIME	LAG
		kbps					0-3600	
☑	XGE 1/0/1	kbps	0	0	0	Drop	0	-
☐	2.5GE 1/0/2	kbps	0	0	0	Drop	0	-
☐	GPON 1/0/1	kbps	0	0	0	Drop	0	-

Rate Mode

Specify the Rate Mode for the broadcast threshold, multicast threshold and UL-Frame threshold on the desired port.

kbps: The OLT will limit the maximum speed of the specific kinds of traffic in kilo-bits per second.

ratio: The OLT will limit the percentage of bandwidth utilization for specific kinds of traffic.

pps: The OLT will limit the maximum number of packets per second for specific kinds of traffic.

Broadcast Threshold

Specify the upper rate limit for receiving broadcast packets.

The valid values differ among different rate modes. For kbps, the rate ranges from 0 to 10,000,000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate is 0 or ranges from 2 to 14,880,000 packets per second. The value 0 means the broadcast threshold is disabled.

The broadcast traffic exceeding the limit will be processed according to the Action configurations.

Multicast Threshold

Specify the upper rate limit for receiving multicast packets.

The valid values differ among different rate modes. For kbps, the rate ranges from 0 to 10,000,000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate is 0 or ranges from 2 to 14,880,000 packets per second. The value 0 means the multicast threshold is disabled.

The multicast traffic exceeding the limit will be processed according to the Action configurations.

UL-Frame Threshold

Specify the upper rate limit for receiving unknown unicast frames.

The valid values differ among different rate modes. For kbps, the rate ranges from 0 to 10,000,000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate is 0 or ranges from 2 to 14,880,000 packets per second. The value 0 means the unknown unicast threshold is disabled.

The traffic exceeding the limit will be processed according to the Action configurations.

Action	Select the action that the OLT will take when the traffic exceeds its corresponding limit. Drop: The port will drop the subsequent packets when the traffic exceeds the limit. Shutdown: The port will be shutdown when the traffic exceeds the limit.
Recover Time	Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 seconds. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, it means the port will not recover to its normal state automatically and you can recover the port manually by clicking ↻ Recover .
LAG (Only for Unit)	Displays which LAG the port belongs to.

7. 3 Configure Voice VLAN

Overview

The voice VLAN is used to prioritize the transmission of voice traffic. Voice traffic is typically more time-sensitive than data traffic, and the voice quality can deteriorate a lot because of packet loss and delay. To ensure the high voice quality, you can configure Voice VLAN.

The feature can be enabled on the ports that transmit voice traffic only or transmit both voice traffic and data traffic. Voice VLAN can change the voice packets' 802.1p priority and transmit the packets in desired VLAN.

Configuration

To configure Voice VLAN, follow these steps:

1) Create a 802.1Q VLAN.

2) Configure OUI addresses.

3) Configure Voice VLAN globally.

4) Add ports to the Voice VLAN.

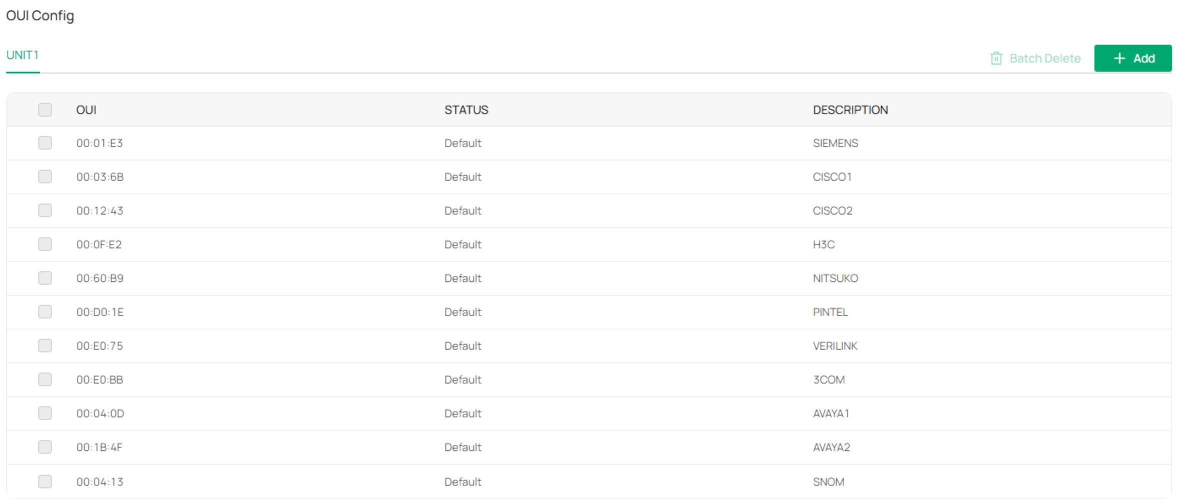
- **Create 802.1Q VLAN**

  Go to L2 Features > VLAN > 802.1Q VLAN to create a 802.1Q VLAN, which will be used for voice traffic. Note that VLAN 1 is a default VLAN and it cannot be configured as the voice VLAN. For details, refer to 4. 4. 1 802.1Q VLAN.

- **Configure OUI Address**

  Go to QoS > Voice VLAN > OUI Config to load the following page.

  The OUI address is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. It is used by the OLT to determine whether a packet is a voice packet. If the OUI address of your voice device is not in the OUI table, click +Add on the upper right to add the OUI address to the table. Click Create.



OUI Config

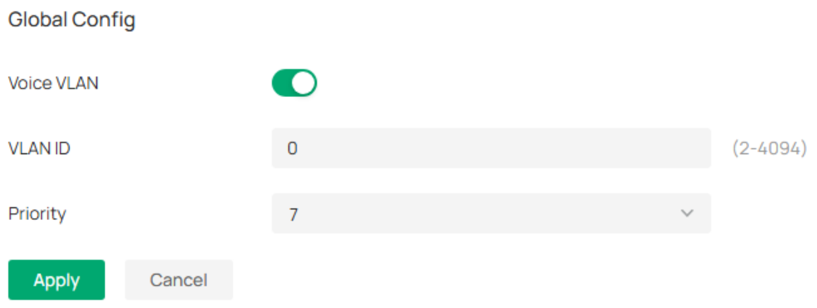
UNIT1

☐	OUI	STATUS	DESCRIPTION
☐	00:01:E3	Default	SIEMENS
☐	00:03:6B	Default	CISCO1
☐	00:12:43	Default	CISCO2
☐	00:0F:E2	Default	H3C
☐	00:60:B9	Default	NITSUKO
☐	00:D0:1E	Default	PINTEL
☐	00:E0:75	Default	VERILINK
☐	00:E0:BB	Default	3COM
☐	00:04:0D	Default	AVAYA1
☐	00:1B:4F	Default	AVAYA2
☐	00:04:13	Default	SNOM

OUI	Enter the OUI address of your voice devices. The OUI address is used by the OLT to determine whether a packet is a voice packet. An OUI address is the first 24 bits of a MAC address, and is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. If the source MAC address of a packet matches the OUI addresses in the OUI list, the OLT identifies the packet as a voice packet and prioritizes it in transmission.
Description	Give an OUI address description for identification.

- **Configure Globally**

Go to QoS > Voice VLAN > Global Config to load the following page and configure the parameters. Click Apply.



Global Config

Voice VLAN: On

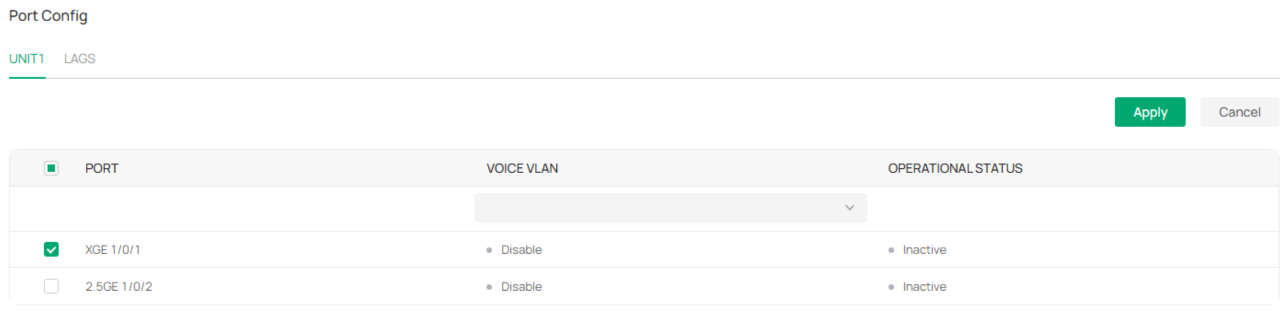
VLAN ID: 0 (2-4094)

Priority: 7

Voice VLAN	Enable Voice VLAN globally.
VLAN ID	Specify the 802.1Q VLAN ID to set the 802.1Q VLAN as the voice VLAN.
Priority	Select the priority that will be assigned to voice packets. A bigger value means a higher priority. This is an IEEE 802.1p priority, and you can further configure its scheduler mode in Class of Service if needed.

- **Add Ports**

Go to QoS > Voice VLAN > Port Config to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Config

■	PORT	VOICE VLAN	OPERATIONAL STATUS
☑	XGE 1/0/1	● Disable	● Inactive
□	2.5GE 1/0/2	● Disable	● Inactive

Voice VLAN	Select Enable to enable the voice VLAN feature on ports to add the desired ports to Voice VLAN.

Optional Status	Displays the state of the Voice VLAN on the corresponding port. Active: Indicates that Voice VLAN function is enabled on the port. Inactive: Indicates that Voice VLAN function is disabled on the port.

7. 4 Configure Auto VoIP

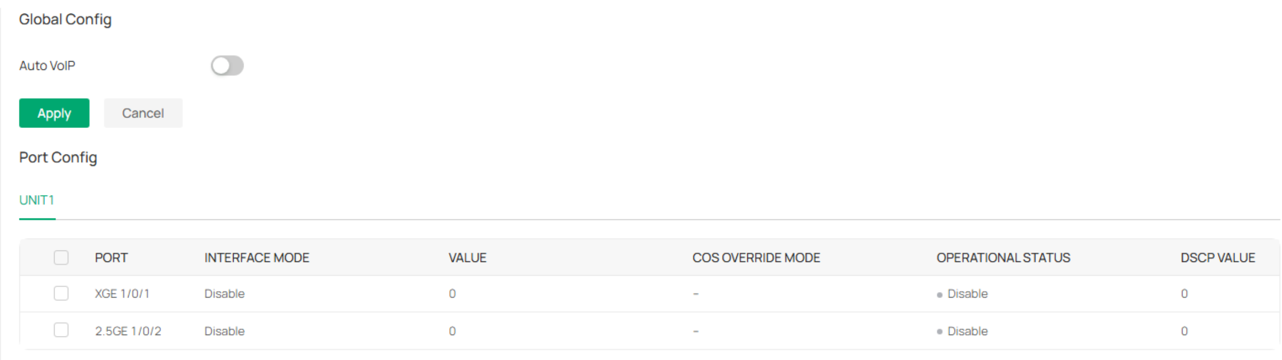
Overview

The Auto VoIP feature is used to prioritize the transmission of voice traffic. Voice traffic is typically more time-sensitive than data traffic, and the voice quality can deteriorate a lot because of packet loss and delay. To ensure the high voice quality, you can configure Auto VoIP.

The feature can be enabled on the ports that transmit voice traffic only or transmit both voice traffic and data traffic. Auto VoIP can inform the voice devices of send the packets with specific configuration by working with the LLDP-MED feature. Auto VoIP provide flexible solutions for optimizing the voice traffic. It can work with other features such as VLAN and Class of Service to process the voice packets with specific fields.

Configuration

1. Go to L2 Feature > LLDP > LLDP-MED to enable LLDP-MED on ports and configure the relevant parameters. For details, refer to 4. 6. 2 LLDP-MED Configuration.
2. Go to QoS > Auto VoIP to load the following page. In Global Config, enable the feature globally.



Global Config

Auto VoIP

Port Config

UNIT1

□	PORT	INTERFACE MODE	VALUE	COS OVERRIDE MODE	OPERATIONAL STATUS	DSCP VALUE
□	XGE 1/0/1	Disable	0	-	● Disable	0
□	2.5GE 1/0/2	Disable	0	-	● Disable	0

3. In Port Config, select one or multiple ports to configure the parameters. Click Apply.

Interface Mode	Select the interface mode for the port. Disable: Disable the Auto VoIP function on the corresponding port. None: Allow the voice devices to use its own configuration to send voice traffic. VLAN ID: The voice devices will send voice packets with desired VLAN tag. If this mode is selected, it is necessary to specify the VLAN ID in the Value field. In addition, you need to configure the 802.1Q VLAN to ensure the corresponding ports can forward the packets normally. Dot1p: The voice devices will send voice packets with desired 802.1p priority. If this mode is selected, it is necessary to specify 802.1p priority in the Value field. In addition, you can configure the Class of Service to make the OLT process the packets according to the 802.1p priority. Untagged: The voice devices will send untagged voice packets.

Value	Enter the value of VLAN ID or 802.1p priority for the port when you select VLAN ID or Dot1p in the Interface Mode configurations.
CoS Override Mode	Enable or disable the Class of Service override mode. Enabled: Enable Class of Service override. The OLT will ignore Class of Service settings and put the packets in TC-5 directly. Disabled: Disable Class of Service override. The OLT will then put the voice packets in the corresponding TC queue according to Class of Service settings.
Operational Status	Displays the operating status of the Auto VoIP feature on the interface. The Operational Status is enabled on the condition that Auto VoIP is enabled globally, the port is linkup, and Interface Mode is not Disable.
DSCP Value	Enter the value of DSCP priority. The voice device will send the packets with the corresponding DSCP value. In addition, you can configure the Class of Service to make the OLT process the packets according to the DSCP priority.

Chapter 8

Configure Security

This chapter guides you on how to configure QoS features. The chapter includes the following sections:

8. 1 Configure Access Security

Overview

Users can access and manage the device via different access interfaces. With Access Security, you can configure parameters for the access interfaces and set limits to them. The following are some common access interfaces:

- **HTTP / HTTPS**

  HTTP or HTTPS allows users to access and manage the device via a web browser. HTTPS is more secure than HTTP.

- **Telenet / SSH**

  Telenet or SSH allows users to access and manage the device via the CLI (Command Line Interface). SSH is more secure than Telenet.

- **Serial Port**

  When the user connects a terminal to the Console port of the device, the user can access and manage the device via the CLI (Command Line Interface).

Configuration

With Access Security, you can configure the following features:

- **Configure Access Control.**

  With Access Control, you can make certain access interfaces available only for a group of users. The filtering critera can be based on IP addresses, MAC addresses, or ports.

- **Configure parameters for different access interfaces**

  You can configure parameters for different access interfaces. including HTTP, HTTPS, SSH, Telenet, and Serail Port.

8. 1. 1 Configure Access Control

Overview

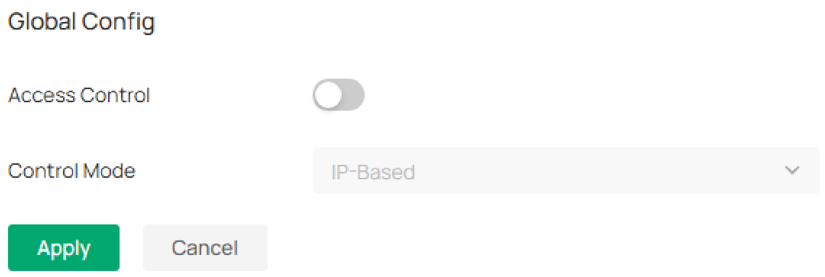
With Access Control, you can make certain access interfaces available only for a group of users. The filtering critera can be based on IP addresses, MAC addresses, or ports.

Note: Access Control is not available for the MGMT port.

Configuration

1. Go to Security > Access Security > Access Control to load the following page. In Global Config,

enable Access Control, and select a control mode according to your needs. Click Apply.

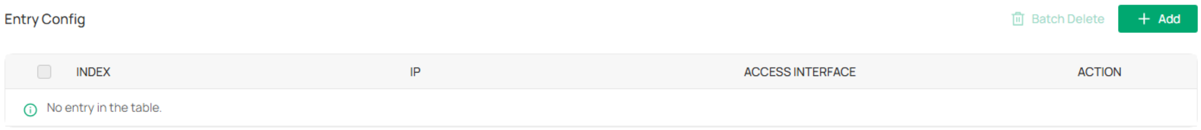

Global Config

Access Control ○

Control Mode IP-Based

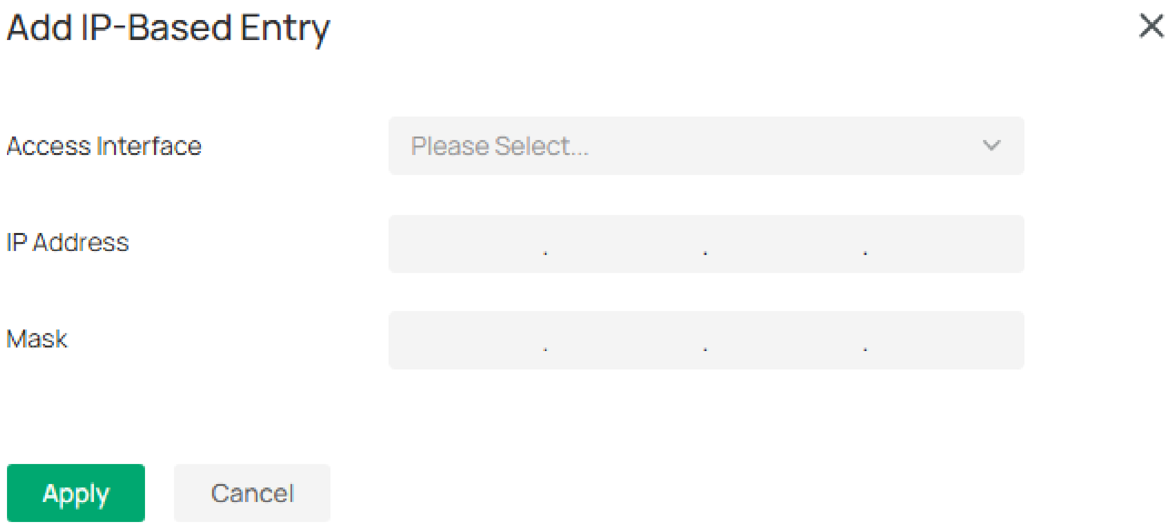
Control Mode	Choose how to control the users' access. IP-based: Only the users within a certain IP-range can access the OLT via the specified interfaces MAC-based: Only the users with a certain MAC address can access the OLTh via the specified interfaces. Port-based: Only the users who are connected to certain ports can access the OLT via the specified interfaces.

2. In Entry Config, click + Add to add an Access Control entry. Configure the following parameters and click Create.


Entry Config

□ INDEX	IP	ACCESS INTERFACE	ACTION

No entry in the table.


Add IP-Based Entry

Access Interface Please Select...

IP Address . . .

Mask . . .

Access Interface	Select the access interfaces where to apply the Access Control rule. If an access interface is selected, only the specified users can access it. If an access interface is unselected, all users can access it. SNMP: SNMP allows users to access and manage the device via NMS. Telnet: Telenet allows users to access and manage the device via the CLI (Command Line Interface). SSH: SSH allows users to access and manage the device via the CLI (Command Line Interface). SSH is more secure than Telenet. HTTP: HTTP allows users to access and manage the device via a web browser. HTTPS: HTTPS allows users to access and manage the device via a web browser. HTTPS is more secure than HTTP. Ping: Ping allows users to test the connection to the device.
IP Address/Mask	Enter the IP address and mask to specify an IP range. Only the users within this IP range can access the specified interfaces.

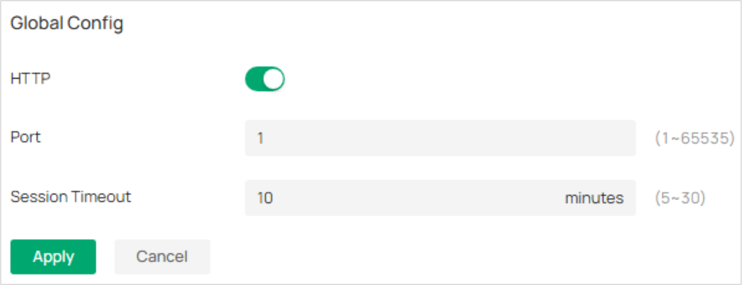
8. 1. 2 Configuring the HTTP Function

Overview

HTTP allows users to access and manage the device via a web browser. You can configure parameters for the HTTP access interface.

Configuration

1. Go to Security > Access Security > HTTP Config to load the following page. In Global Config, enable HTTP and configure other parameters. Click Apply.



Global Config

HTTP: ON

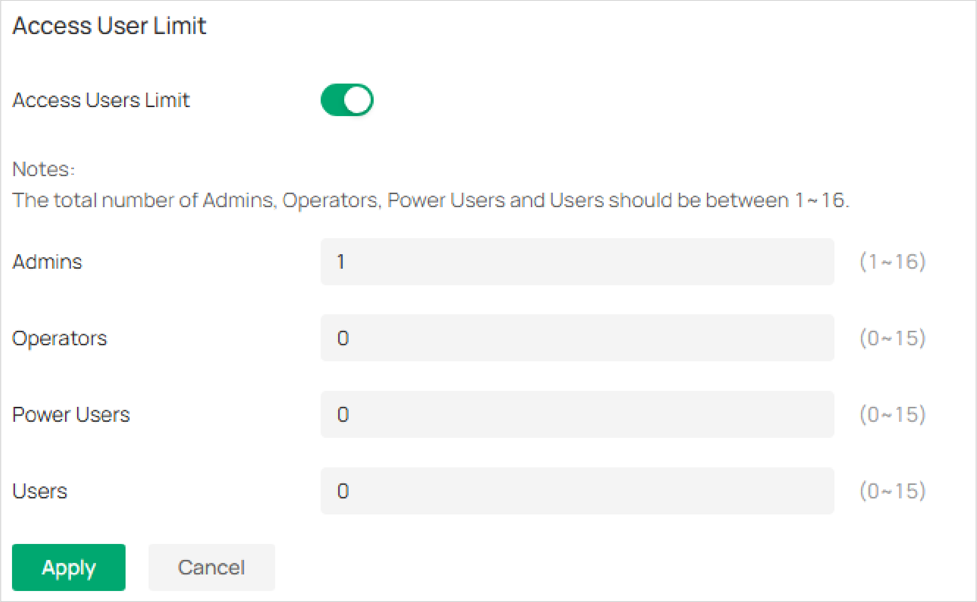
Port: 1 (1~65535)

Session Timeout: 10 minutes (5~30)

HTTP	Check the box to enable HTTP. HTTP allows users to access and manage the device via a web browser.
Port	Specify the port number for HTTP service.
Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

2. In Access Users Limit, you can enable Access Users Limit and configure other parameters. Click

Apply.



Access User Limit

Access Users Limit ●

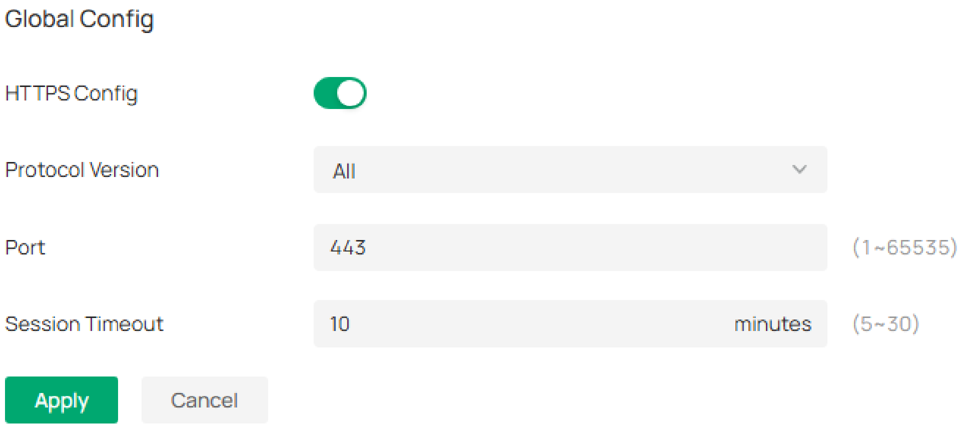
Notes:
The total number of Admins, Operators, Power Users and Users should be between 1~16.

Admins	1	(1~16)
Operators	0	(0~15)
Power Users	0	(0~15)
Users	0	(0~15)

Access Users Limit	With this option enabled, you can configure the maximum number of users who simultaneously log in to the web page of the device via HTTP . The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operators.
Number of Power Users	Specify the maximum number of users whose access level is Power Users.
Number of Users	Specify the maximum number of users whose access level is Users.

8. 1. 3 Configuring the HTTPS Function

1. Go to Security > Access Security > HTTPS Config to load the following page. In Global Config, enable HTTPS and configure other parameters. Click Apply.



Global Config

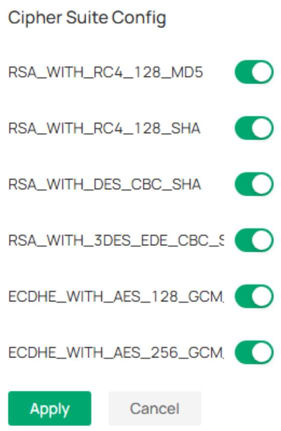
HTTPS Config ●

Protocol Version	All	
Port	443	(1~65535)
Session Timeout	10 minutes	(5~30)

HTTPS	Check the box to enable HTTPS. HTTPS allows users to access and manage the device via a web browser. HTTPS is more secure than HTTP.

Protocol Version	Select the protocol version for HTTPS. Make sure the protocol in use is compatible with that on your HTTPS client. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection. TLS is a transport protocol upgraded from SSL. It can support a more secure connection than SSL. TLS and SSL are not compatible with each other. SSL Version 3.0: Select SSL Version 3.0 as the protocol for HTTPS. TLS Version 1.0: Select TLS Version 1.0 as the protocol for HTTPS. TLS Version 1.1: Select TLS Version 1.1 as the protocol for HTTPS. TLS Version 1.2: Select TLS Version 1.2 as the protocol for HTTPS. All: Enable all the above protocols for HTTPS. The HTTPS server and client will negotiate the protocol each time.
Port	Specify the port number for HTTPS service.
Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

2. In Cipher Suite Config, select the algorithm for HTTPS service and click Apply.



Cipher Suite Config

RSA_WITH_RC4_128_MD5 ●

RSA_WITH_RC4_128_SHA ●

RSA_WITH_DES_CBC_SHA ●

RSA_WITH_3DES_EDE_CBC_S ●

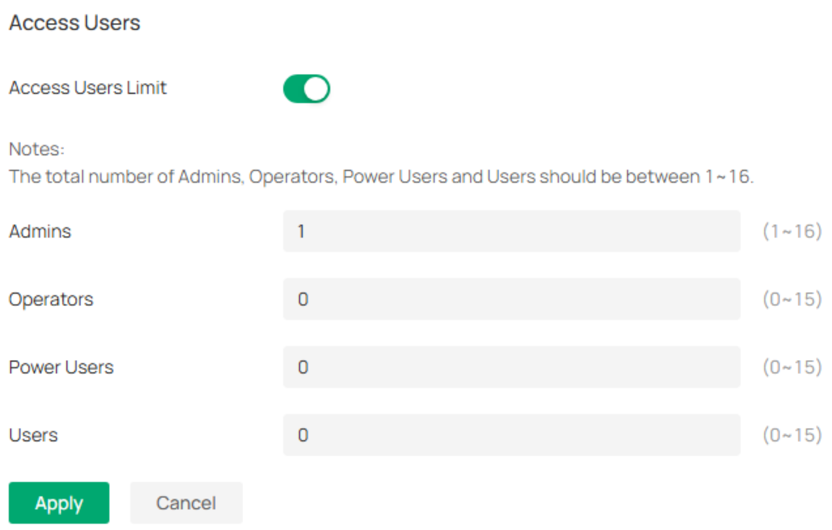
ECDHE_WITH_AES_128_GCM ●

ECDHE_WITH_AES_256_GCM ●

RSA_WITH_RC4_128_MD5	128-bit RC4 encryption with MD5 message authentication and RSA key exchange.
RSA_WITH_RC4_128_SHA	128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange.
RSA_WITH_DES_CBC_SHA	56-bit DES encryption with SHA-1 message authentication and RSA key exchange.
RSA_WITH_3DES_EDE_CBC_SHA	168-bit Triple DES encryption with SHA-1 message authentication and RSA key exchange.
ECDHE_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with SHA-256 message authentication and elliptic curve Diffie-Hellman key exchange signed with an RSA certificate or ECDSA certificate.

ECDHE_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with SHA-384 message authentication and elliptic curve Diffie-Hellman key exchange signed with an RSA certificate or ECDSA certificate.

3. In Access Users, you can enable Access Users Limit and configure other parameters. Click Apply.



Access Users

Access Users Limit ●

Notes:
The total number of Admins, Operators, Power Users and Users should be between 1~16.

Admins: 1 (1~16)

Operators: 0 (0~15)

Power Users: 0 (0~15)

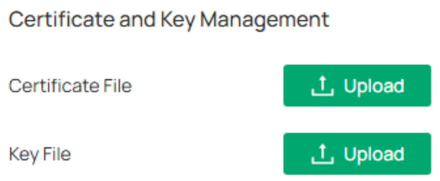
Users: 0 (0~15)

Access Users Limit	With this option enabled, you can configure the maximum number of users who simultaneously log in to the web page of the device via HTTP . The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operators.
Number of Power Users	Specify the maximum number of users whose access level is Power Users.
Number of Users	Specify the maximum number of users whose access level is Users.

4. If you want to use a certificate and key for HTTPS service, follow these steps:

1) Generate a certificate file and key file using a third-party software, such as XCA. The certificate must be BASE64 encoded. The SSL certificate and key must match each other, otherwise the HTTPS connection will not work.

2) In Certificate and Key Management, Upload the certificate file and key file.



Certificate and Key Management

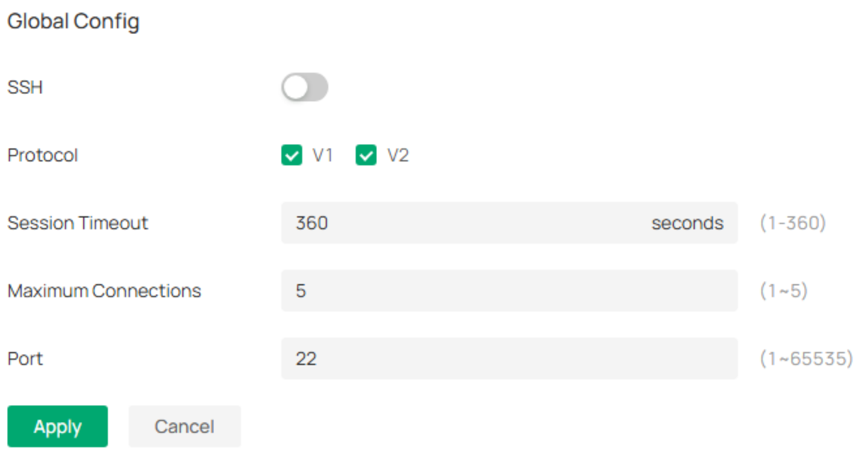
Certificate File

Key File

Certificate File	Click Browse and select the certificate file on your PC. Then click Upload.
Key File	Click Browse and select the key file on your PC. Then click Upload.

8. 1. 4 Configuring the SSH Function

1. Go to Security > Access Security > SSH Config to load the following page. In Global Config, enable SSH and configure other parameters. Click Apply.



Global Config

SSH ○

Protocol ☑ V1 ☑ V2

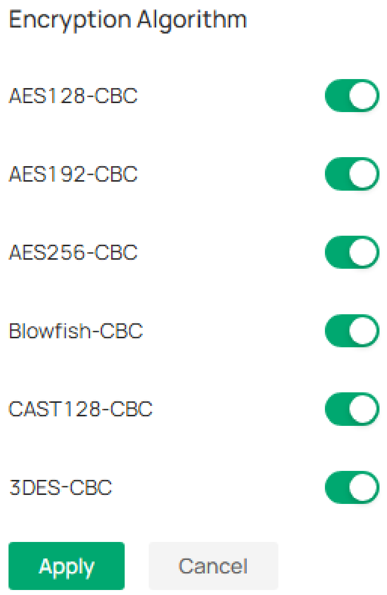
Session Timeout 360 seconds (1-360)

Maximum Connections 5 (1~5)

Port 22 (1~65535)

SSH	Check the box to enable SSH. SSH allows users to access and manage the device via the CLI (Command Line Interface). SSH is more secure than Telnet.
Protocol	Select the versions of SSH protocol to enable.
Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.
Maximum Connections	Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set.
Port	Specify the port number for SSH.

2. In Encryption Algorithm, enable the encryption algorithm you want the device to support and click Apply.



Encryption Algorithm

AES128-CBC ●

AES192-CBC ●

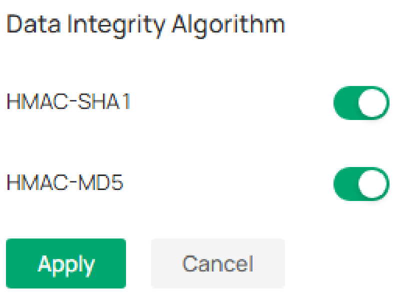
AES256-CBC ●

Blowfish-CBC ●

CAST128-CBC ●

3DES-CBC ●

3. In Data Integrity Algorithm, enable the integrity algorithm you want the device to support and click Apply.

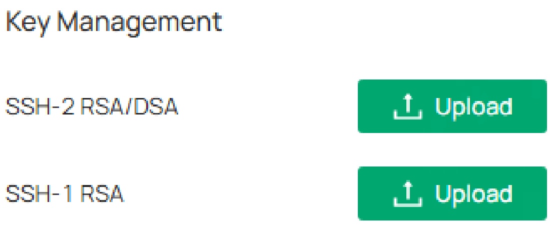


Data Integrity Algorithm

HMAC-SHA1 ●

HMAC-MD5 ●

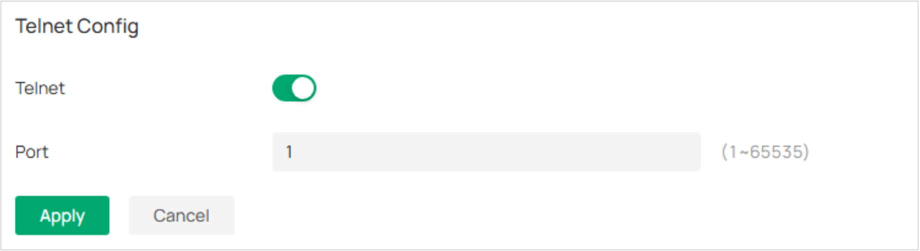
4. In Key Management, upload the SSH key file.



Key Management

8. 1. 5 Configuring the Telnet Function

Go to Security > Access Security > Telnet Config to load the following page. Enable Telent and configure the following parameters. Click Apply.



Telnet Config

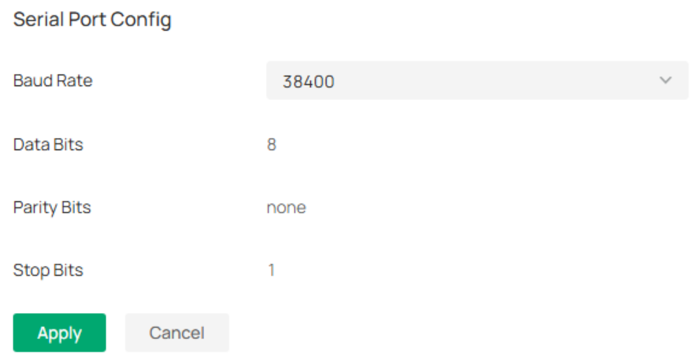
Telnet ●

Port: 1 (1~65535)

Telent	Check the box to enable Telnet. Telnet allows users to access and manage the device via the CLI (Command Line Interface).
Port	Specify the port number for Telnet service.

8. 1. 6 Configuring the Serial Port

Go to Security > Access Security > Serial Port Config to load the following page. Configure the following parameters. Click Apply.



Serial Port Config

Baud Rate 38400

Data Bits 8

Parity Bits none

Stop Bits 1

Baud Rate	Configure the baud rate of the console connection. The default value is 38400 bps.
Data Bits	Displays the data bits.
Parity Bits	Displays the parity bits.
Stop Bits	Displays the stop bits.

8. 2 Configure Port Security

Overview

You can use the Port Security feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets. In addtion, the device can send a notification if the number of learned MAC addresses on the port exceeds the limit.

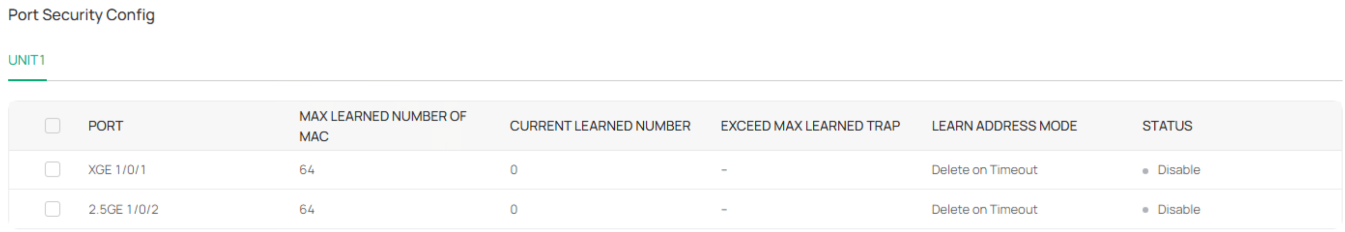
Configuration

Go to Security > Port Security to load the following page. select one or more ports and configure the following parameters. Click Apply.

Note:

1. Port Security cannot be enabled on the member port of a LAG, and the port with Port Security enabled cannot be added to a LAG.

2. Port Security and 802.1x cannot be enabled at the same time for a port.



Port Security Config

UNIT1

☐	PORT	MAX LEARNED NUMBER OF MAC	CURRENT LEARNED NUMBER	EXCEED MAX LEARNED TRAP	LEARN ADDRESS MODE	STATUS
☐	XGE 1/0/1	64	0	-	Delete on Timeout	● Disable
☐	2.5GE 1/0/2	64	0	-	Delete on Timeout	● Disable

Port	Displays the port number.
Max Learned Number of MAC	Specify the maximum number of MAC addresses that can be learned on the port. When the learned MAC address number reaches the limit, the port will stop learning. It ranges from 0 to 64. The default value is 64.
Current Learned Number	Displays the current number of MAC addresses that have been learned on the port.
Exceed Max Learned Trap	Enable Exceed Max Learned, and when the maximum number of learned MAC addresses on the specified port is exceeded, a notification will be generated and sent to the management host.
Learn Address Mode	Select the learn mode of the MAC addresses on the port. Three modes are provided: Delete on Timeout: The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting. Delete on Reboot: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. Permanent: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.

Status	Select the status of Port Security. Three kinds of status can be selected: Drop: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned. Forward: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned. Disable: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.

8. 3 Configure ACL

Overview

ACL (Access Control List) filters traffic as it passes through the device, permitting or denying packets which cross specified interfaces or VLANs. It accurately identifies and processes the packets based on the ACL rules. In this way, ACL helps to limit network traffic, manage network access behaviors, forward packets to specified ports and more.

Configuration

To configure ACL, follow these steps:

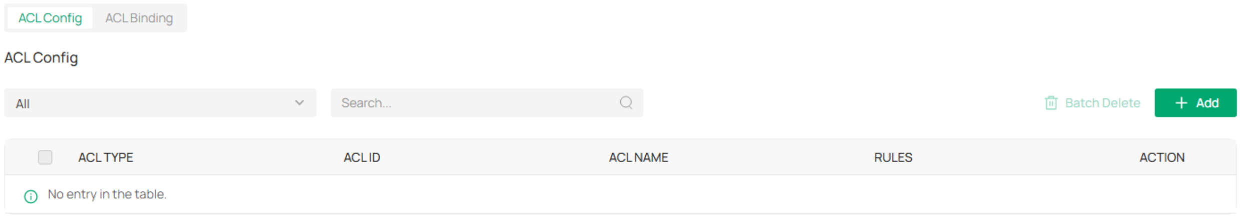
1) Create an ACL entry and select the ACL type.

2) Configure ACL rules for the ACL entry to filter different packets.

3) Bind the ACL entry to a port or VLAN to make it effective.

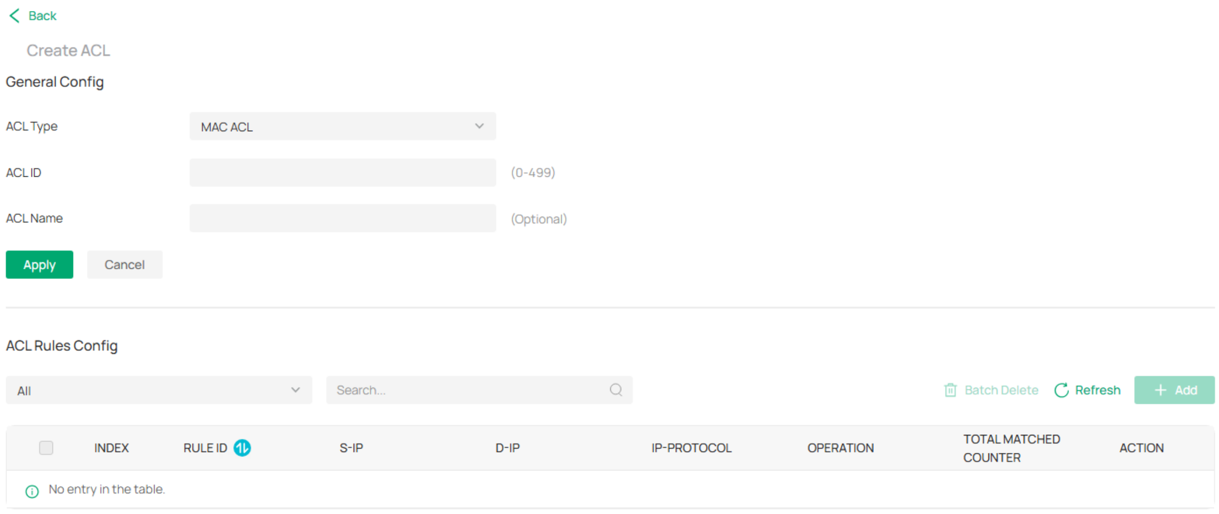
■ Create an ACL Entry

1. Go to Security > ACL > ACL Config to load the following page.



□	ACL TYPE	ACL ID	ACL NAME	RULES	ACTION
No entry in the table.					

2. Click + Add. In General Config, select an ACL type according to your needs and specify the other parameters. Click Apply.



ACL Type: MAC ACL

ACL ID: (0-499)

ACL Name: (Optional)

□	INDEX	RULE ID	S-IP	D-IP	IP-PROTOCOL	OPERATION	TOTAL MATCHED COUNTER	ACTION
No entry in the table.								

ACL Type	MAC ACL: ACL rules use source and destination MAC address to match and filter packets. IP ACL: ACL rules use source and destination IP address to match and filter packets. Combined ACL: ACL rules use source and destination MAC address and IP address to match and filter packets. IPv6 ACL: ACL rules use source and destination IPv6 address to match and filter packets.
ACL ID	Specify the ACL ID for this entry. The ACL ID is used to identify the ACL entry.
ACL Name	(Optional) Specify the ACL Name for this entry.

Configure ACL Rules

In ACL Rules Config, click +Add to add an ACL Rule of the corresponding ACL type. You can configure multiple ACL rules for an ACL entry. A packet "matches" an ACL rule when it meets the rule's matching criteria. The resulting action will be either to "permit" or "deny" the packet that matches the rule.

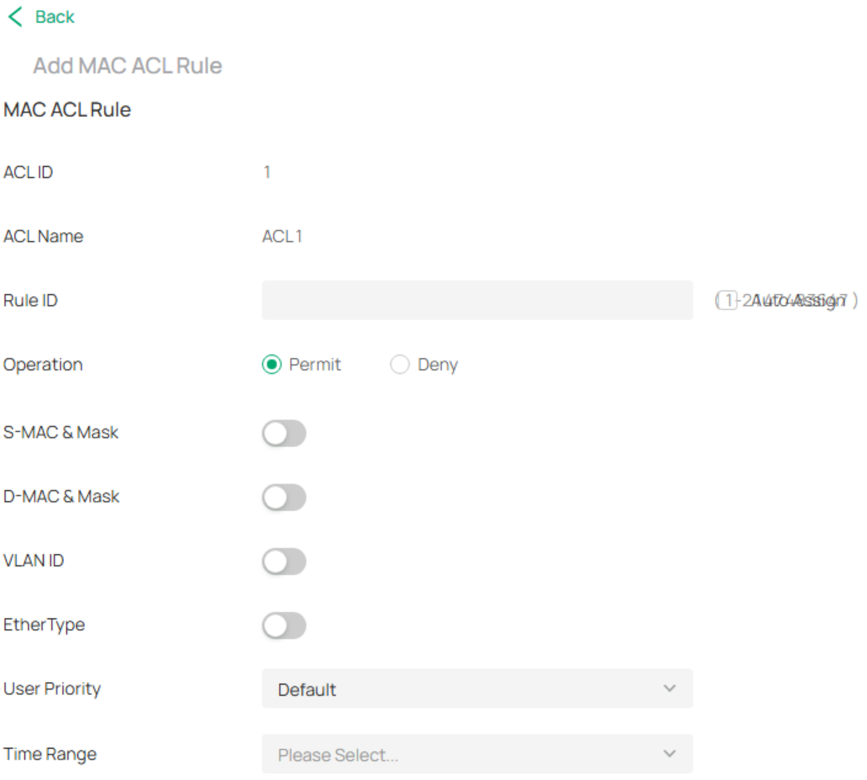
Note:

1. If no ACL rule is configured, all the packets will be forwarded without being processed by the ACL.

2. If there are configured ACL rules and no matching rule is found, the packets will be dropped.

1. Configure the operation, filtering criteria, and other parameters of the ACLrule.

For MAC ACL



< Back

Add MAC ACL Rule

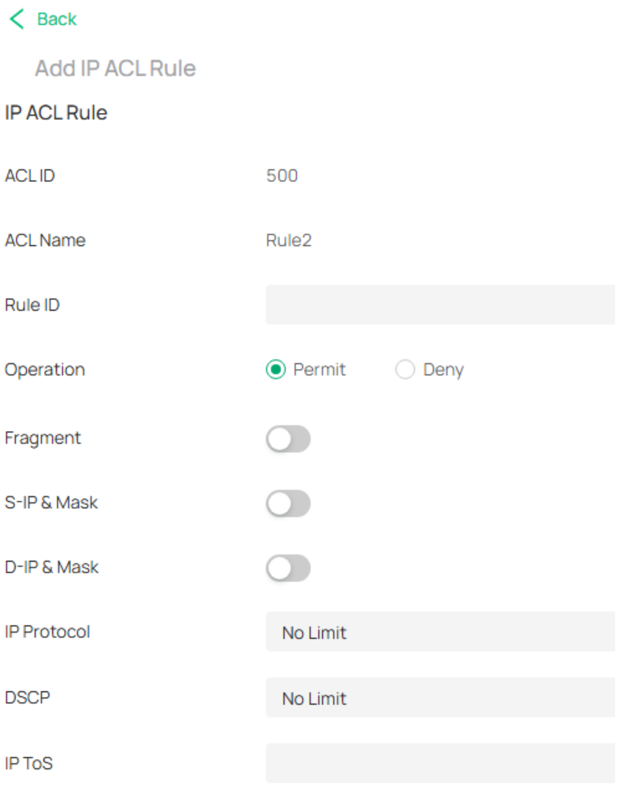
MAC ACL Rule

ACL ID	1
ACL Name	ACL1
Rule ID	(1-2Auto-Assign7)
Operation	● Permit ○ Deny
S-MAC & Mask	○
D-MAC & Mask	○
VLAN ID	○
EtherType	○
User Priority	Default
Time Range	Please Select...

ACL ID	Displays the ID of the ACL entry which the ACL rule belongs to.

ACL Name	Displays the name of the ACL entry which the ACL rule belongs to.
Rule ID	Specify the ID of the ACL rule. The rule ID is used to identify the ACL rule. If you enable Auto Assign, the system automatically assigns a rule ID to the ACLrule.
Operation	Permit: The matched packets are forwarded. Deny: The matched packets are discarded..
S-MAC & Mask	Enter the source MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-MAC & Mask	Enter the destination MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
VLAN ID	Enter the ID of the VLAN to which the ACL will apply.
Ether Type	Specify the EtherType to be matched using 4 hexadecimal numbers.
User Priority	Specify the User Priority to be matched.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the SYSTEM > Time Range page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

■ For IP ACL



Add IP ACL Rule

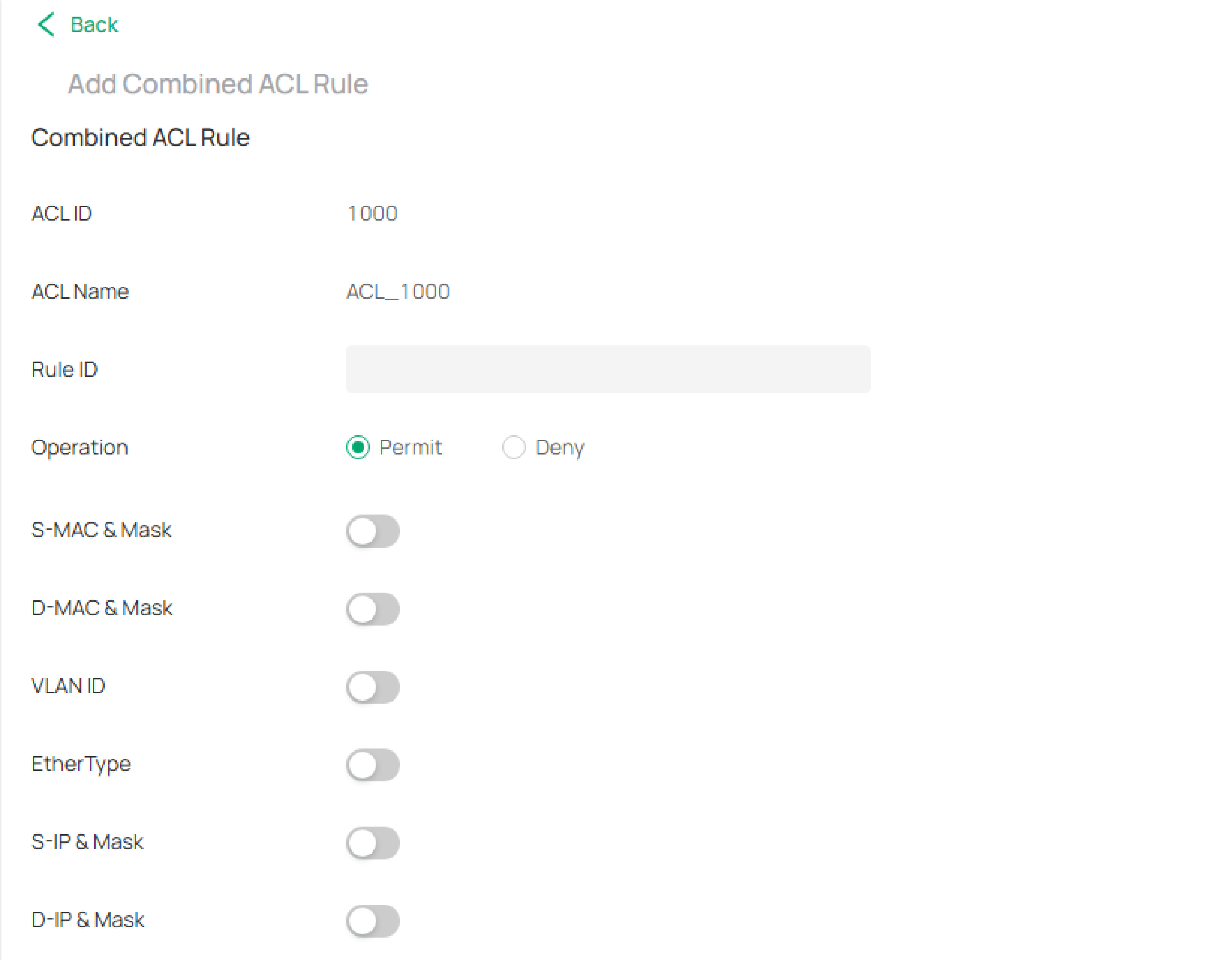
IP ACL Rule

ACL ID	500
ACL Name	Rule2
Rule ID	
Operation	● Permit ○ Deny
Fragment	
S-IP & Mask	
D-IP & Mask	
IP Protocol	No Limit
DSCP	No Limit
IP ToS	

ACL ID	Displays the ID of the ACL entry which the ACL rule belongs to.
ACL Name	Displays the name of the ACL entry which the ACL rule belongs to.
Rule ID	Specify the ID of the ACL rule. The rule ID is used to identify the ACL rule. If you enable Auto Assign, the system automatically assigns a rule ID to the ACLrule.
Operation	Permit: The matched packets are forwarded. Deny: The matched packets are discarded..
S-IP & Mask	Enter the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP & Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IP Protocol	Select a protocol type from the drop-down list. The default is No Limit, which indicates that packets of all protocols will be matched. You can also select User-defined to customize the IP protocol.
S-Port / D-Port	If TCP/UDP is selected as the IP protocol, specify the source and destination port number with a mask. Value: Specify the port number. Mask: Specify the port mask with 4 hexadacimal numbers.

DSCP	Specify a DSCP value to be matched between 0 and 63. The default is No Limit.
IP ToS	Specify an IP ToS value to be matched between 0 and 15. The default is No Limit.
IP Pre	Specify an IP Precedence value to be matched to be matched between 0 and 7. The default is No Limit.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the SYSTEM > Time Range page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

- **For Combined ACL**



Add Combined ACL Rule

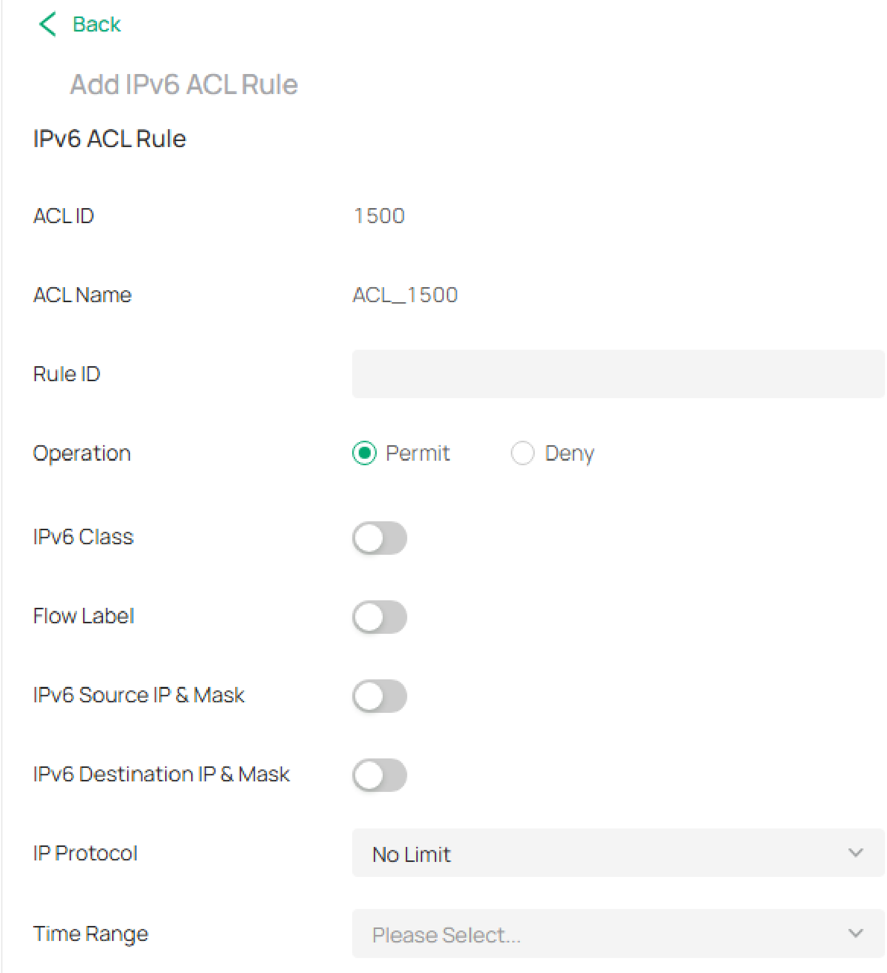
Combined ACL Rule

ACL ID	1000
ACL Name	ACL_1000
Rule ID	
Operation	● Permit ○ Deny
S-MAC & Mask	○
D-MAC & Mask	○
VLAN ID	○
EtherType	○
S-IP & Mask	○
D-IP & Mask	○

ACL ID	Displays the ID of the ACL entry which the ACL rule belongs to.
ACL Name	Displays the name of the ACL entry which the ACL rule belongs to.

Rule ID	Specify the ID of the ACL rule. The rule ID is used to identify the ACL rule. If you enable Auto Assign, the system automatically assigns a rule ID to the ACLrule.
Operation	Permit: The matched packets are forwarded. Deny: The matched packets are discarded..
S-MAC & Mask	Enter the source MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-MAC & Mask	Enter the destination MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
VLAN ID	Enter the ID of the VLAN to which the ACL will apply.
Ether Type	Specify the EtherType to be matched using 4 hexadecimal numbers.
S-IP & Mask	Enter the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP & Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IP Protocol	Select a protocol type from the drop-down list. The default is No Limit, which indicates that packets of all protocols will be matched. You can also select User-defined to customize the IP protocol.
S-Port / D-Port	If TCP/UDP is selected as the IP protocol, specify the source and destination port number with a mask. Value: Specify the port number. Mask: Specify the port mask with 4 hexadacimal numbers.
DSCP	Specify a DSCP value to be matched between 0 and 63. The default is No Limit.
IP ToS	Specify an IP ToS value to be matched between 0 and 15. The default is No Limit.
IP Pre	Specify an IP Precedence value to be matched to be matched between 0 and 7. The default is No Limit.
User Priority	Specify the User Priority to be matched.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the SYSTEM > Time Range page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

For IPv6 ACL



Add IPv6 ACL Rule

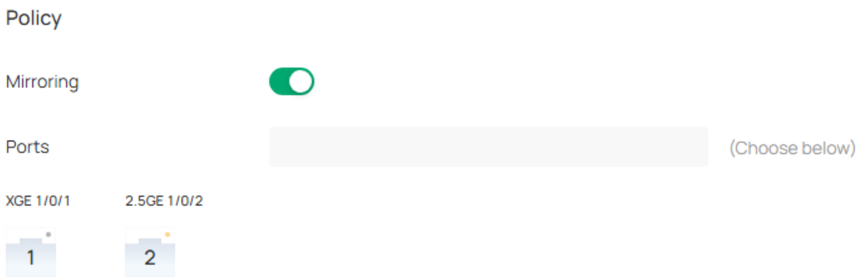
IPv6 ACL Rule

ACL ID	1500
ACL Name	ACL_1500
Rule ID	
Operation	● Permit ○ Deny
IPv6 Class	
Flow Label	
IPv6 Source IP & Mask	
IPv6 Destination IP & Mask	
IP Protocol	No Limit
Time Range	Please Select...

ACL ID	Displays the ID of the ACL entry which the ACL rule belongs to.
ACL Name	Displays the name of the ACL entry which the ACL rule belongs to.
Rule ID	Specify the ID of the ACL rule. The rule ID is used to identify the ACL rule. If you enable Auto Assign, the system automatically assigns a rule ID to the ACLrule.
Operation	Permit: The matched packets are forwarded. Deny: The matched packets are discarded..
IPv6 Class	Specify an IPv6 class value to be matched. The device will check the class field of the IPv6 header.
Flow Label	Specify a Flow Label value to be matched.
IPv6 Source IP	Enter the source IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.

Mask	The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, FFFF:FFFF:0000:FFFF). The IPv6 address mask specifies which bits in the source IPv6 address to match the rule. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IPv6 Destination IP	Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.
Mask	The mask is required if the destination IPv6 address is entered. Enter the complete mask (for example, FFFF:FFFF:0000:FFFF). The IPv6 address mask specifies which bits in the destination IPv6 address to match the rule. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IP Protocol	Select a protocol type from the drop-down list. The default is No Limit, which indicates that packets of all protocols will be matched. You can also select User-defined to customize the IP protocol.
Time Range	Select a time range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect. The Time Range referenced here can be created on the SYSTEM > Time Range page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

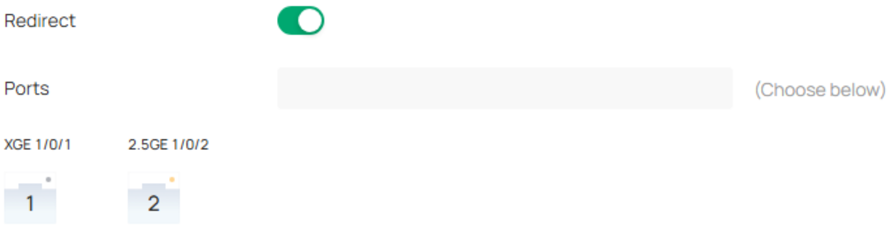
2. In Policy, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored. (For DS-P8000-X2 and DS-P7001-16, the Mirroring feature is only applicable to the uplink port.)


Policy

Mirroring

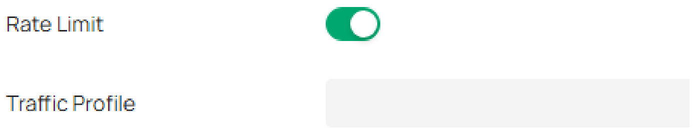
Ports (Choose below)

3. In Policy, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected. (For DS-P8000-X2 and DS-P7001-16, the Redirect feature is only applicable to the uplink port.)


Redirect

Ports (Choose below)

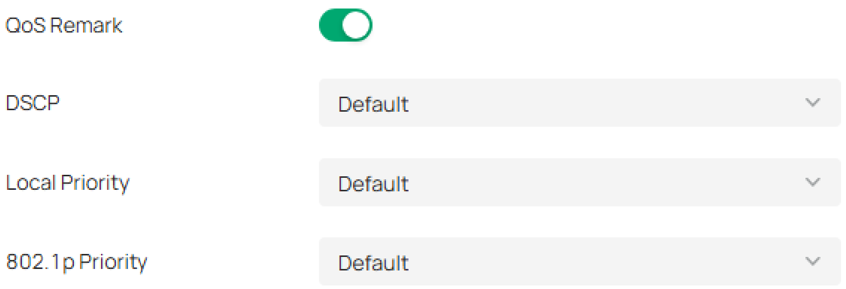
4. In Policy, enable or disable the Rate Limit feature for the matched packets. With this option enabled, choose a traffic profile which is applied to Rate Limit.



Rate Limit: ●

Traffic Profile:

5. In Policy, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the device.



QoS Remark: ●

DSCP: Default

Local Priority: Default

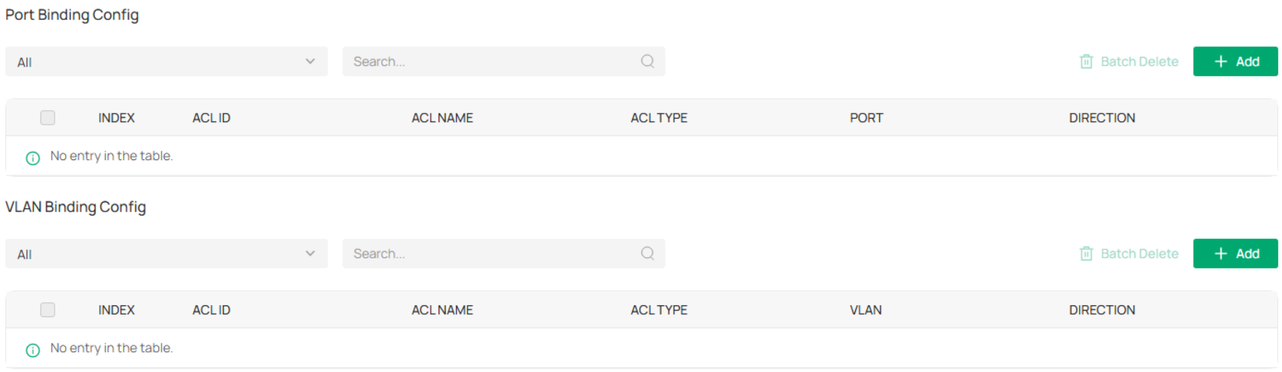
802.1p Priority: Default

DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6. Click Apply.

- **Bind the ACL Entry**

1. Go to Security > ACL > ACL Binding to load the following page.



Port Binding Config

□	INDEX	ACL ID	ACL NAME	ACL TYPE	PORT	DIRECTION

No entry in the table.

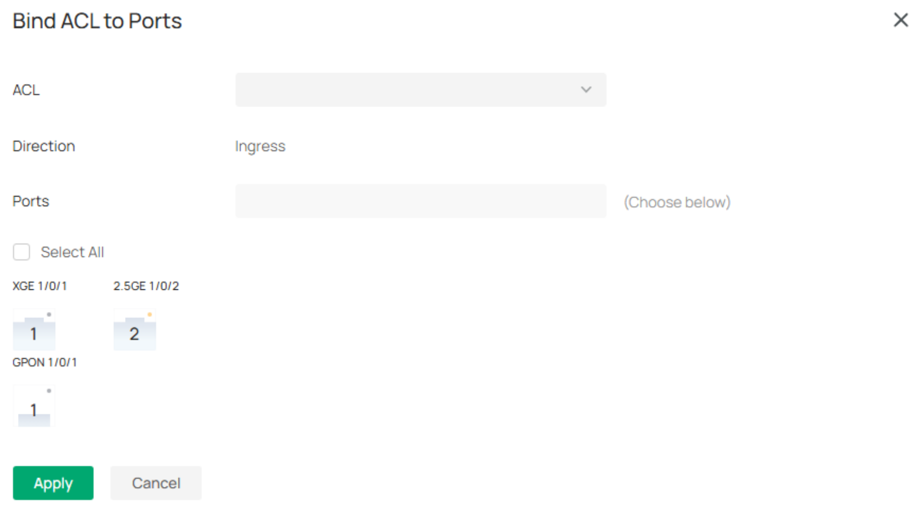
VLAN Binding Config

□	INDEX	ACL ID	ACL NAME	ACL TYPE	VLAN	DIRECTION

No entry in the table.

2. Determine whether to bind the ACL entry to ports or VLANs, and click the correponding +Add button. Then configure the related parameters and click Apply.

To Bind ACL to Ports



Bind ACL to Ports

ACL

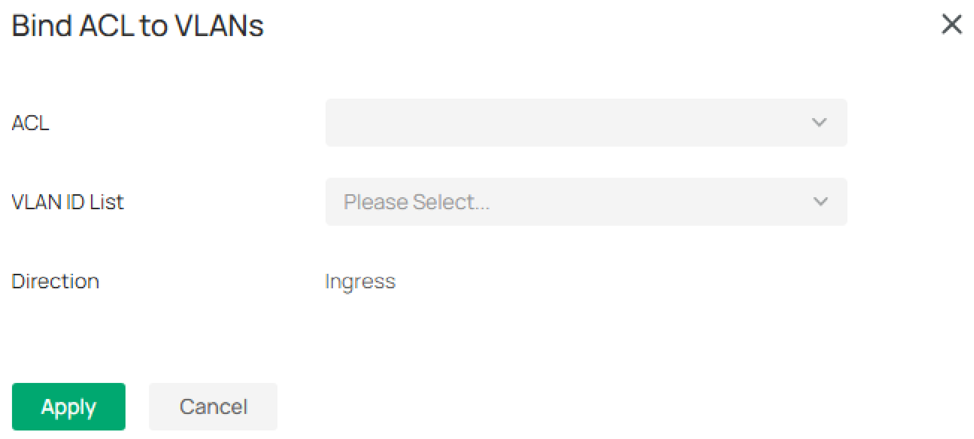
Direction Ingress

Ports (Choose below)

□ Select All

ACL	Select the ACL to be bound to the ports
Direction	Display whether the ACL entry takes effect in the Ingress or egress direction in terms of the traffic that passes through the ports.
Ports	Select the ports which the ACL is bound to.

To Bind ACL to VLANs



Bind ACL to VLANs

ACL

VLAN ID List Please Select...

Direction Ingress

ACL	Select the ACL to be bound to the VLANs
VLAN ID List	Select the VLANs which the ACL is bound to.
Direction	Display whether the ACL entry takes effect in the Ingress or egress direction in terms of the traffic that passes through the VLANs.

8. 4 Configure DHCP Filter

Overview

With DHCP Filter configured, the switch can check whether the received DHCP packets are legal and discard the illegal ones. In this way, DHCP Filter ensures that users get IP addresses only from the legal DHCP server and enhances the network security.

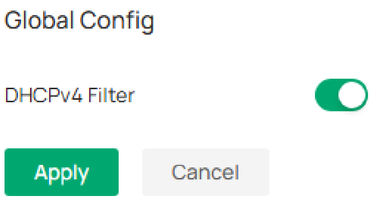
Configuration

The device supports the following features:

- **DHCPv4 Filter**
- **DHCPv6 Filter**

8. 4. 1 Configure DHCPv4 Filter

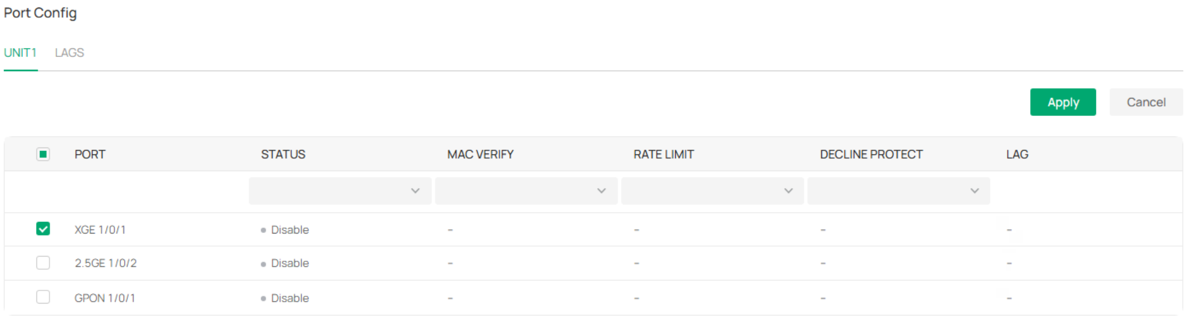
1. Go to Security > DHCP Filter > DHCPv4 Filter to load the following page. In Global Config, enable DHCPv4 Filter and click Apply.



Global Config

DHCPv4 Filter: ●

2. In Port Config, select the ports and configure related parameters. Click Apply.



Port Config

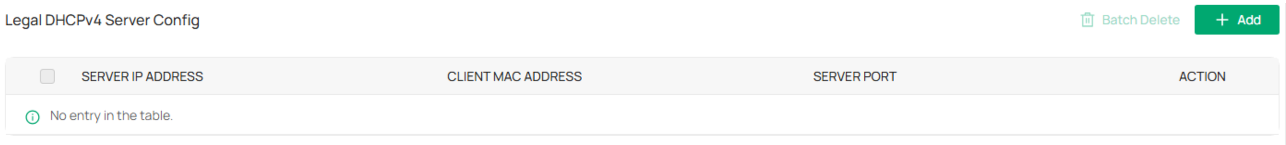
UNIT1 LAGS

■	PORT	STATUS	MAC VERIFY	RATE LIMIT	DECLINE PROTECT	LAG
☑	XGE 1/0/1	● Disable	-	-	-	-
□	2.5GE 1/0/2	● Disable	-	-	-	-
□	GPON 1/0/1	● Disable	-	-	-	-

Port	Displays the port number.
Status	Enable or disable DHCPv4 Filter feature on the port.
MAC Verify	Enable or disable the MAC Verify feature. There are two fields in the DHCPv4 packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCPv4 packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCPv4 server from being exhausted by forged MAC addresses.

Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCPv4 packets that can be forwarded on the port per second. The excessive DHCPv4 packets will be discarded.
Decline Protect	Select to enable the decline protect feature and specify the maximum number of Decline packets that can be forwarded on the port per second. The excessive Decline packets will be discarded.
LAG	Displays the LAG that the port is in.

3. Go to Security > DHCP Filter > Legal DHCPv4 Servers to load the following page. Click +Add and configure the parameters. Click Create.



Legal DHCPv4 Server Config

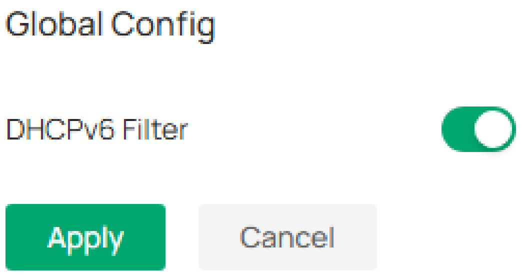
□	SERVER IP ADDRESS	CLIENT MAC ADDRESS	SERVER PORT	ACTION

No entry in the table.

Server IP Address	Specify the IP address of the legal DHCPv4 server.
Client MAC Address	(Optional) Specify the MAC address of the DHCP Client. You can also keep this field empty, which represents for all DHCP clients.
Server Port	Select the port that the legal DHCPv4 server is connected.

8. 4. 2 Configure DHCPv6 Filter

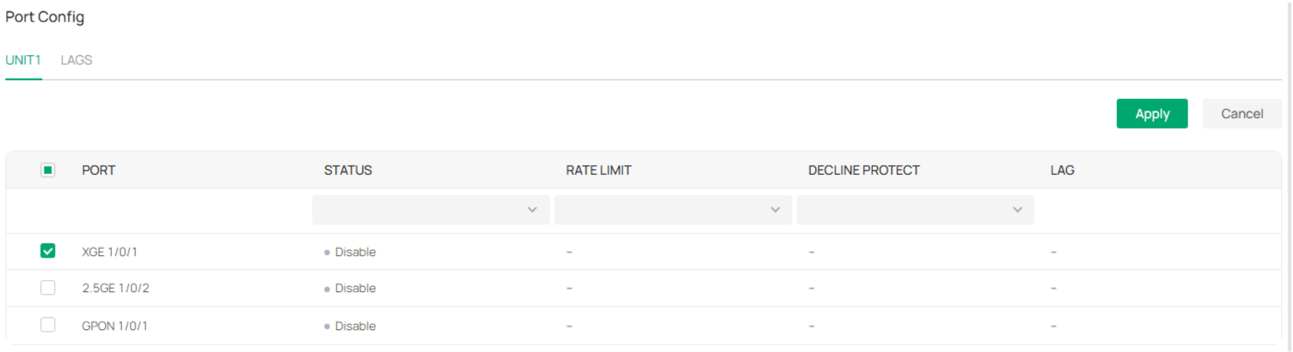
1. Go to Security > DHCP Filter > DHCPv6 Filter to load the following page. In Global Config, enable DHCPv6 Filter and click Apply.



Global Config

DHCPv6 Filter: enabled

2. In Port Config, select the ports and configure related parameters. Click Apply.

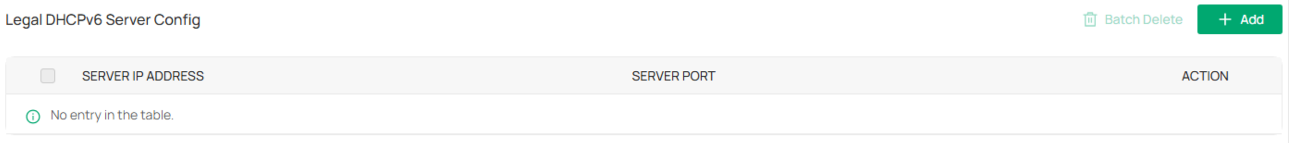


Port Config

■	PORT	STATUS	RATE LIMIT	DECLINE PROTECT	LAG
☑	XGE 1/0/1	Disable	-	-	-
□	2.5GE 1/0/2	Disable	-	-	-
□	GPON 1/0/1	Disable	-	-	-

Port	Displays the port number.
Status	Enable or disable DHCPv6 Filter feature on the port.
Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCPv6 packets that can be forwarded on the port per second. The excessive DHCPv6 packets will be discarded.
Decline Protect	Select to enable the decline protect feature and specify the maximum number of Decline packets that can be forwarded on the port per second. The excessive Decline packets will be discarded.
LAG	Displays the LAG that the port is in.

3. Go to Security > DHCP Filter > Legal DHCPv6 Servers to load the following page. Click +Add and configure the parameters. Click Create.



□	SERVER IP ADDRESS	SERVER PORT	ACTION
ⓘ No entry in the table.			

Server IPv6 Address	Specify the IP address of the legal DHCPv6 server.
Server Port	Select the port that the legal DHCPv6 server is connected.

Chapter 9

Configure Device Maintenance

This chapter guides you on how to configure device maintenance features. The chapter includes the following sections:

9. 1 System Monitor

With System Monitor function, you can:

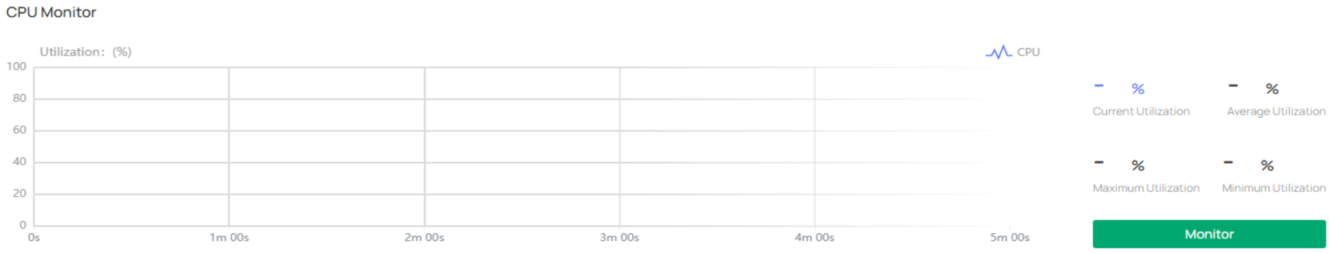
- **Monitor the CPU utilization of the device.**
- **Monitor the memory utilization of the device.**

  You can configure parameters for different access interfaces. including HTTP, HTTPS, SSH, Telenet, and Serail Port.

Note: The CPU utilization should be always under 80%, and excessive use may result in device malfunctions. You can monitor the system to verify a CPU utilization problem.

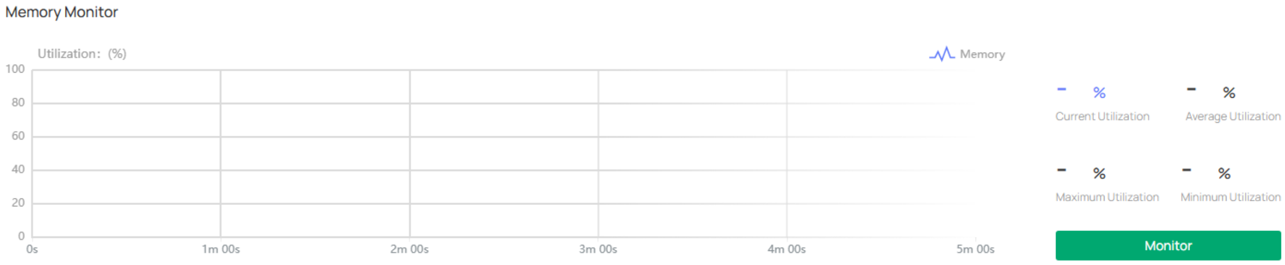
9. 1. 1 Monitor the CPU

Go to Maintenance > System Monitor > CPU Monitor to load the following page. Click Monitor to enable the device to monitor and display its CPU utilization rate every five seconds.



9. 1. 2 Monitor the Memory

Go to Maintenance > System Monitor > Memory Monitor to load the following page. Click Monitor to enable the device to monitor and display its Memory utilization rate every five seconds.



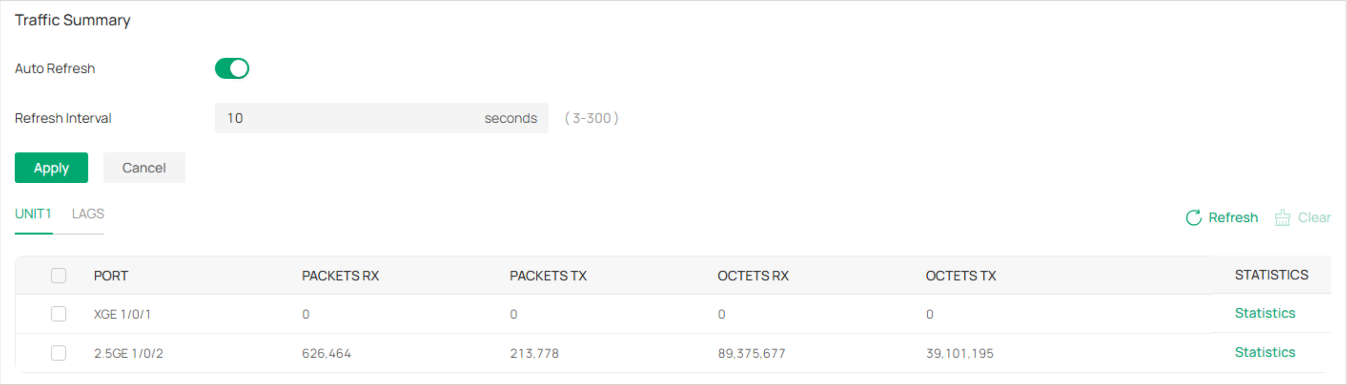
9. 2 Traffic Monitor

Overview

With Traffic Monitor function, you can monitor each port's traffic information, including the traffic summary and traffic statistics in detail.

Configuration

Go to Maintenance > Traffic Monitor to load the following page.



Traffic Summary

Auto Refresh: ●

Refresh Interval: 10 seconds (3-300)

Apply Cancel

UNIT1 LAGS

Refresh Clear

□	PORT	PACKETS RX	PACKETS TX	OCTETS RX	OCTETS TX	STATISTICS
□	XGE 1/0/1	0	0	0	0	Statistics
□	2.5GE 1/0/2	626,464	213,778	89,375,677	39,101,195	Statistics

Follow these steps to monitor port traffic:

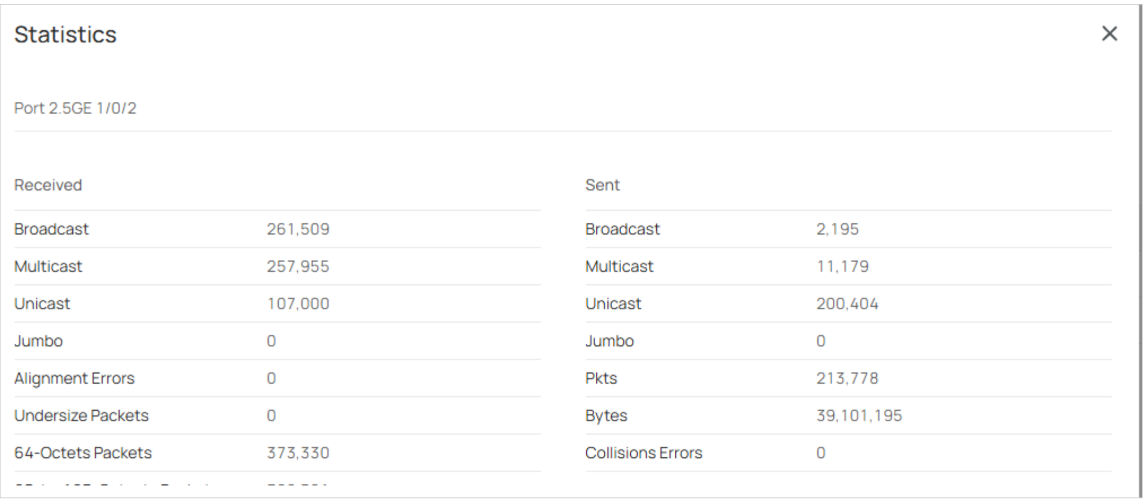
1. To get the real-time traffic summary, enable Auto Refresh, or click Refresh.

Auto Refresh	With this option enabled, the device will automatically refresh the traffic summary.
Refresh Interval	Specify the time interval for the device to refresh the traffic summary.

2. Click UNIT1 to show the information of the physical ports, and click LAGS to show the information of the LAGs.

Packets Rx	Displays the number of packets received on the port. Error packets are not counted.
Packets Tx	Displays the number of packets transmitted on the port. Error packets are not counted.
Octets Rx:	Displays the number of octets received on the port. Error octets are counted.
Octets Tx:	Displays the number of octets transmitted on the port. Error octets are counted .

To view a port's traffic statistics in detail, click Statistics on the right side of the entry.



Statistics

Port 2.5GE 1/0/2

Received		Sent	
Broadcast	261,509	Broadcast	2,195
Multicast	257,955	Multicast	11,179
Unicast	107,000	Unicast	200,404
Jumbo	0	Jumbo	0
Alignment Errors	0	Pkts	213,778
Undersize Packets	0	Bytes	39,101,195
64-Octets Packets	373,330	Collisions Errors	0

Received	Displays the detailed information of received packets. Broadcast: Displays the number of valid broadcast packets received on the port. Error frames are not counted. Multicast: Displays the number of valid multicast packets received on the port. Error frames are not counted. Unicast: Displays the number of valid unicast packets received on the port. Error frames are not counted. Jumbo: Displays the number of valid jumbo packets received on the port. Error frames are not counted. Alignment Errors: Displays the number of the received packets that have a Frame Check Sequence (FCS) with a non-integral octet (Alignment Error). The size of the packet is between 64 bytes and 1518 bytes. Undersize Packets: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long. 64-Octets Packets: Displays the number of the received packets (including error packets) that are 64 bytes long. 65-to-127-Octects Packets: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long. 128-to-255-Octects Packets: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long. 256-to-511-Octects Packets: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long. 512-to-1023-Octects Packets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. 1024-to-1518-Octects Packets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. Pkts: Displays the number of packets received on the port. Error packets are not counted. Bytes: Displays the number of bytes received on the port. Error packets are not counted.

Sent	Displays the detailed information of sent packets. Broadcast: Displays the number of valid broadcast packets transmitted on the port. Error frames are not counted. Multicast: Displays the number of valid multicast packets transmitted on the port. Error frames are not counted. Unicast: Displays the number of valid unicast packets transmitted on the port. Error frames are not counted. Pkts: Displays the number of packets transmitted on the port. Error packets are not counted. Bytes: Displays the number of bytes transmitted on the port. Error packets are not counted. Collisions Errors: Displays the number of collisions experienced by a half-duplex port during packet transmissions.

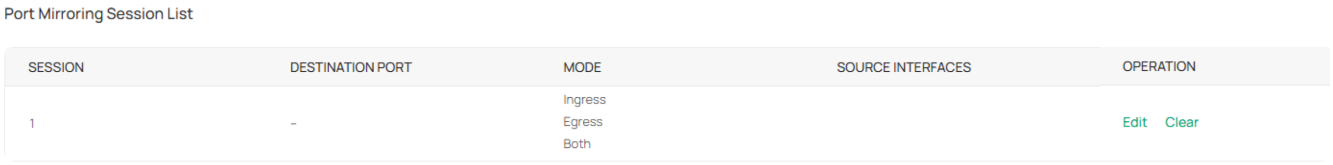
9. 3 Mirroring

Overview

You can analyze network traffic and troubleshoot network problems using Mirroring. Mirroring allows the device to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic from the source.

Configuration

Go to Maintenance > Mirroring and select the port mirroring session from the list and click Edit.

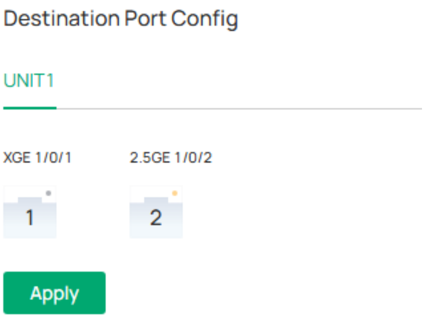


Port Mirroring Session List

SESSION	DESTINATION PORT	MODE	SOURCE INTERFACES	OPERATION
1	-	Ingress Egress Both		Edit Clear

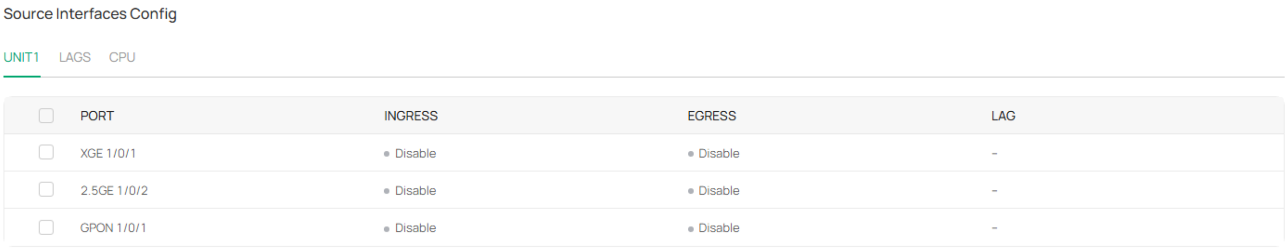
Follow these steps to configure the mirroring session:

1. Click Edit. In the Destination Port Config section, specify a destination port for the mirroring session, and click Apply.



Destination Port Config

2. In the Source Interfaces Config section, specify the source interfaces and click Apply. Traffic passing through the source interfaces will be mirrored to the destination port. There are three source interface types: port, LAG, and CPU. Choose one or more types according to your need.



Source Interfaces Config

□	PORT	INGRESS	EGRESS	LAG
□	XGE 1/0/1	● Disable	● Disable	-
□	2.5GE 1/0/2	● Disable	● Disable	-
□	GPON 1/0/1	● Disable	● Disable	-

UNIT1	Select the desired ports as the source interfaces. The device will send a copy of traffic passing through the port to the destination port.
LAGS	Select the desired LAGs as the source interfaces. The device will send a copy of traffic passing through the LAG members to the destination port.

CPU	When selected, the device will send a copy of traffic passing through the CPU to the destination port.
Ingress	With this option enabled, the packets received by the corresponding interface (port, LAG or CPU) will be copied to the destination port. By default, it is disabled.
Egress	With this option enabled, the packets sent by the corresponding interface (port, LAG or CPU) will be copied to the destination port. By default, it is disabled.

Note:

1. The member ports of an LAG cannot be set as a destination port or source port.

2. A port cannot be set as the destination port and source port at the same time.

9. 4 Ethernet OAM

Overview

Ethernet OAM (Operation, Administration, and Maintenance) is a Layer 2 protocol for monitoring and troubleshooting Ethernet networks. It can monitor link performance, monitor faults and generate alarms so that a network administrator can manage the network effectively. The device supports Ethernet OAM which is defined in IEEE 802.3ah.

Configuration

To complete OAM configurations, follow these steps:

1) Enable OAM and configure OAM mode on the port.

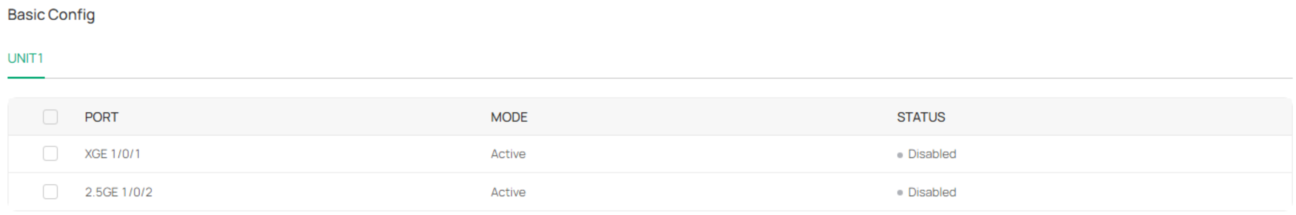
2) Configure the following OAM features according to your needs:

   - Link Monitoring
   - Remote Failure Indication (RFI)
   - Remote Loopback

3) View the OAM status on the port.

9. 4. 1 Enabling OAM and Configuring OAM Mode

1. Go to Maintenance > Ethernet OAM > Basic Config to load the following page. In the Basic Config section, select one or more ports, configure the OAM mode and enable OAM. Click Apply.



Basic Config

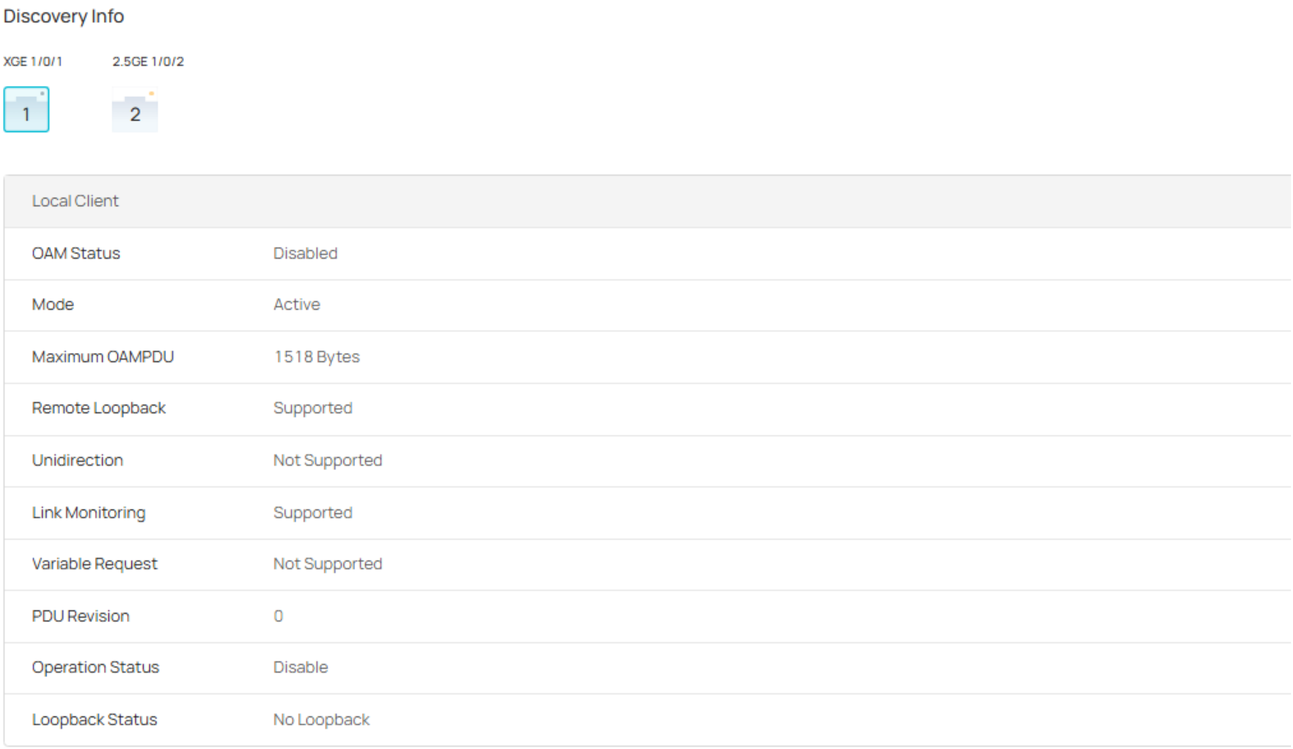
UNIT1

□	PORT	MODE	STATUS
□	XGE 1/0/1	Active	● Disabled
□	2.5GE 1/0/2	Active	● Disabled

Mode	Select OAM mode for the port. Active: The port in this mode can initiate OAM connection. It is the default setting. Passive: The port in this mode cannot initiate OAM connection or send loopback control OAMPDUs. **Note**: OAM connection cannot be established between two ports in passive mode. Make sure that at least one side is in active mode.
Status	Enable or disable OAM on the port. By default, it is disabled.

2. In the Discovery Info section, Select a port to view whether the OAM connection is established

with the peer. Additionally, you can view the OAM information of the local and the remote entities.



Local Client	
OAM Status	Disabled
Mode	Active
Maximum OAMPDU	1518 Bytes
Remote Loopback	Supported
Unidirection	Not Supported
Link Monitoring	Supported
Variable Request	Not Supported
PDU Revision	0
Operation Status	Disable
Loopback Status	No Loopback

The OAM information of the local entity is as follows:

OAM Status	Displays whether OAM is enabled.
Mode	Displays the OAM mode of the local entity.
Maximum OAMPDU	Displays the maximum size of OAMPDU.
Remote Loopback	Displays whether the local entity supports Remote Loopback.
Unidirection	Displays whether the local entity supports Unidirection.
Link Monitoring	Displays whether the local entity supports Link Monitoring.
Variable Request	Displays whether the local entity supports Variable Request.
PDU Revision	Displays the PDU Revision of the local entity.

Operation Status	Displays the status of OAM connection: Disable: OAM is disabled on the port. LinkFault: The link between the local entity and the remote entity is down. PassiveWait: The port is in passive mode and is waiting to see if the peer device is OAM capable. ActiveSendLocal: The port is in active mode and is sending local information. SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. SendLocalAndRemoteOK: The local device agrees the OAM peer entity. PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity. PeeringRemotelyRejected: The remote OAM entity rejects the local device. NonOperHalfDuplex: Ethernet OAM is enabled but the port is in half-duplex operation. You should configure the port as a full-duplex port. Operational: OAM connection is established with the peer and OAM works normally.
Loopback Status	Displays the loopback status. No Loopback: Neither the local entity nor the remote entity is in the loopback mode. Local Loopback: The local entity is in the loopback mode. Remote Loopback: The remote entity is in the loopback mode.

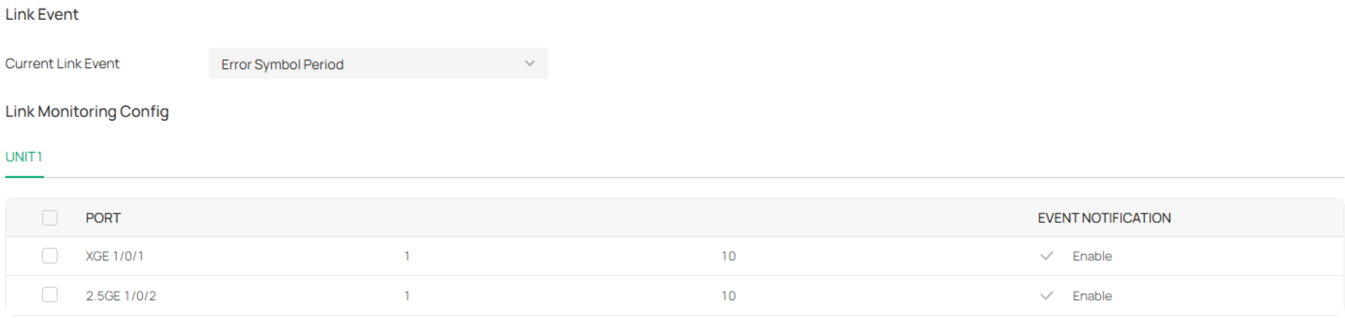
The OAM information of the remote entity is as follows:

Mode	Displays the OAM mode of the remote entity.
MAC Address	Displays the MAC address of the remote entity.
Vendor (OUI)	Displays the Vendor's OUI of the remote entity.
Maximum OAMPDU	Displays the maximum size of OAMPDU.
Remote Loopback	Displays whether the remote entity supports Remote Loopback.
Unidirection	Displays whether the remote entity supports Unidirection.
Link Monitoring	Displays whether the remote entity supports Link Monitoring.
Variable Request	Displays whether the remote entity supports Variable Request.
PDU Revision	Displays the PDU Revision of the remote entity.

Vendor Information	Displays the vendor information of the remote entity.

9. 4. 2 Configure Link Monitoring

Go to Maintenance > Ethernet OAM > Link Monitoring to load the following page.



Link Event

Current Link Event: Error Symbol Period

Link Monitoring Config

UNIT1

☐	PORT			EVENT NOTIFICATION
☐	XGE 1/0/1	1	10	✓ Enable
☐	2.5GE 1/0/2	1	10	✓ Enable

Follow these steps to configure the mirroring session:

1. In the Link Event section, select a Link Event type to configure.

Current Link Event	Error Symbol Period: An Error Symbol Period event occurs if the number of error symbols exceeds the defined threshold within a specific period of time. Error Frame: An Error Frame event occurs if the number of error frames exceeds the defined threshold within a specific period of time. Error Frame Period: An Error Frame Period event occurs if the number of error frames in a specific number of received frames exceeds the defined threshold. Error Frame Seconds: An Error Frame Seconds event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is defined as an error frame second if error frames occur within that second.

2. In the Link Monitoring Config section, select one or more ports, and configure the following parameters for the selected link event.

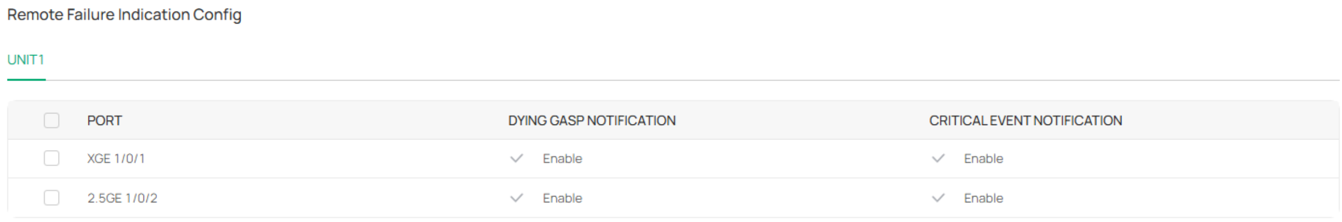
Threshold	Threshold (Error Symbols): If you select **Error Symbol Period** as the link event type, specify the threshold of received error symbols within a specific period of time. Valid error frame values are from 1 to 4294967295, and the default value is 1. Threshold (Error Frames): If you select **Error Frame** or **Error Frame Period** as the link event type, specify the threshold of error frames within a specific period of time or in specific number of received frames. Valid error frame values are from 1 to 4294967295, and the default value is 1. Threshold (Error Seconds): If you select **Error Frame Seconds** as the link event type, specify the threshold of error frame seconds. Valid values are from 1 to 900, and the default value is 1.

Window	Specify the period for the selected link event. Window (100ms): If you select **Error Symbol Period**, **Error Frame** or **Error Frame Seconds** as the link event type, specify the time period in units of 100ms (for example, 2 refers to 200ms), in which if the received errors exceed the threshold, a link event will be generated. For **Error Symbol Period** and **Error Frame**, valid values are from 10*100 to 600*100 ms. For **Error Frame Seconds**, valid values are from 100*100 to 9000*100 ms. Window (Frames): If you select **Error Frame Period** as the link event type, specify the number of frames, in which if the frame errors exceed the threshold, a link event will be generated. Valid values are from 148810 to 89286000 frames, and the default value is 1488100 frames.
Event Notification	Enable or disable notifications to report the link event. By default, all types of link event can be reported.

3. Click Apply.

9. 4. 3 Configure Remote Failure Indication

Go to Maintenance > Ethernet OAM > Remote Failure Indication to load the following page. Select one or more ports to configure the following parameters and click Apply.



Remote Failure Indication Config

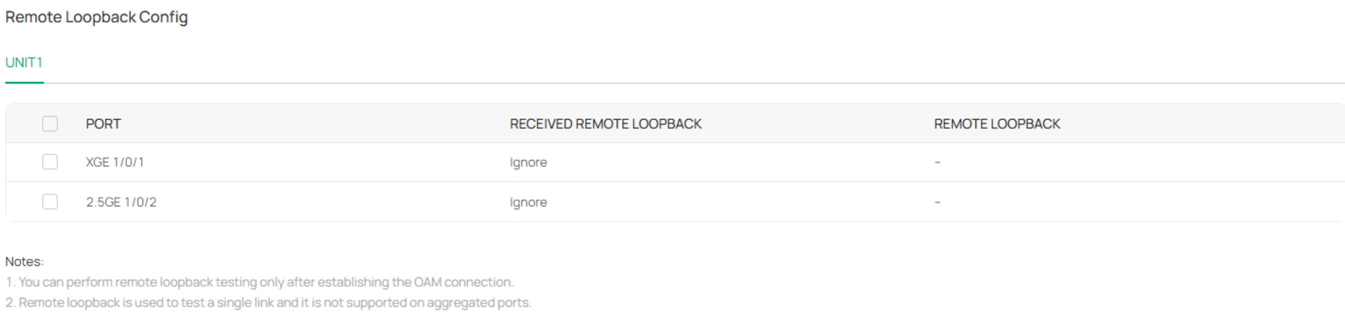
UNIT1

□	PORT	DYING GASP NOTIFICATION	CRITICAL EVENT NOTIFICATION
□	XGE 1/0/1	✓ Enable	✓ Enable
□	2.5GE 1/0/2	✓ Enable	✓ Enable

Dying Gasp Notification	With Dying Gasp Notification enabled, if the device detects an unrecoverable fault on the network, it will report this condition locally and send Information OAMPDU to notify the peer.
Critical Event Notification	With Critical Event Notification enabled, if the device detects an unspecified critical event occurs, it will report this condition locally and send Information OAMPDU to notify the peer.

9. 4. 4 Configure Remote Loopback

Go to Maintenance > Ethernet OAM > Remote Loopback to load the following page. Select one or more ports to configure the following parameters and click Apply.



Remote Loopback Config

UNIT1

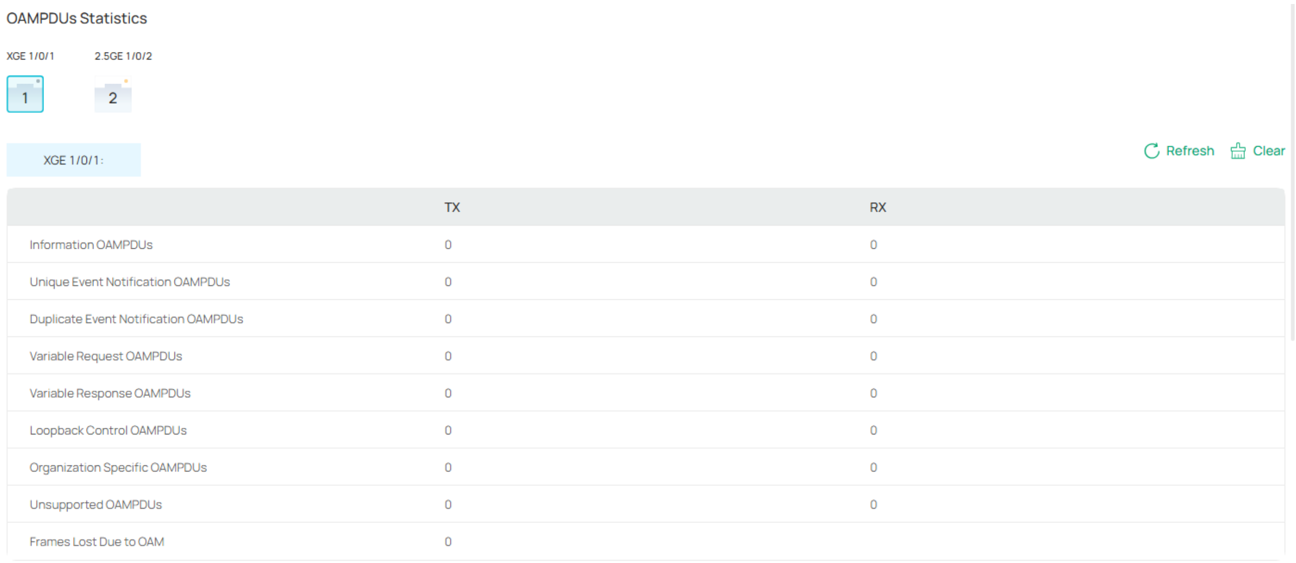
□	PORT	RECEIVED REMOTE LOOPBACK	REMOTE LOOPBACK
□	XGE 1/0/1	Ignore	-
□	2.5GE 1/0/2	Ignore	-

Notes:
1. You can perform remote loopback testing only after establishing the OAM connection.
2. Remote loopback is used to test a single link and it is not supported on aggregated ports.

Received Remote Loopback	Choose to ignore or to process the received remote loopback requests.
Remote Loopback	Start or stop the remote loopback process. The port to be configured should be in active mode and has established OAM connection with the peer. Start: Request the remote peer to start the OAM remote loopback mode. Stop: Request the remote peer to stop the OAM remote loopback mode.

9. 4. 5 View OAM Statistics

1. Go to Maintenance > Ethernet OAM > Statistics to load the following page. In the OAMPDUs Statistics section, select a port to view the number of different OAMPDUs transmitted and received on it.



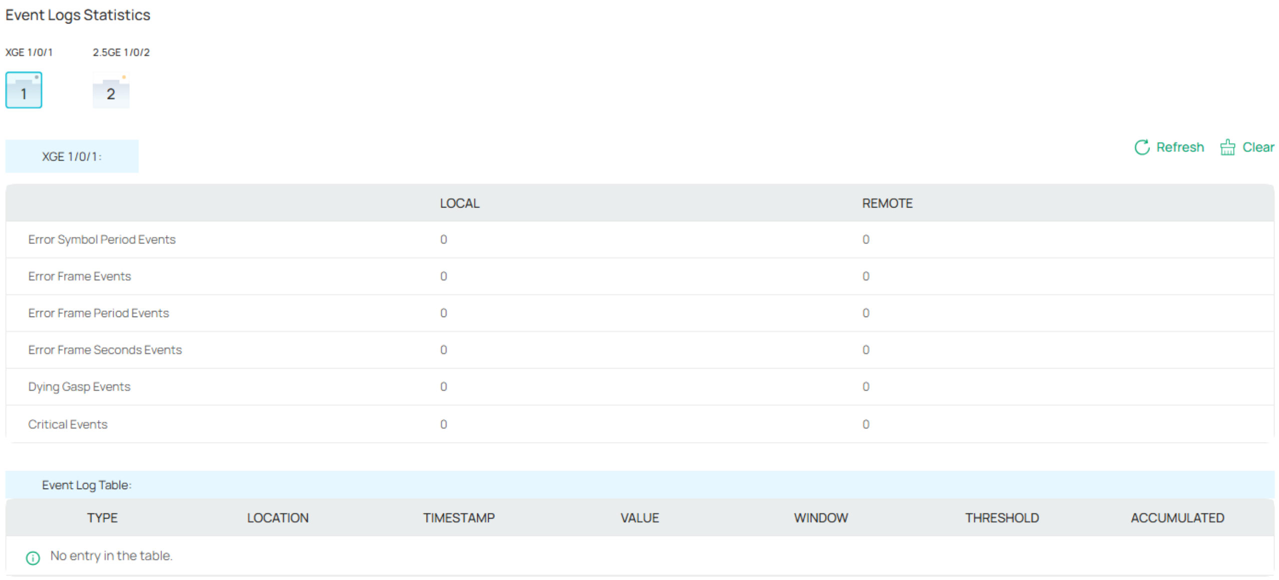
XGE 1/0/1:

	TX	RX
Information OAMPDUs	0	0
Unique Event Notification OAMPDUs	0	0
Duplicate Event Notification OAMPDUs	0	0
Variable Request OAMPDUs	0	0
Variable Response OAMPDUs	0	0
Loopback Control OAMPDUs	0	0
Organization Specific OAMPDUs	0	0
Unsupported OAMPDUs	0	0
Frames Lost Due to OAM	0	

Tx	Displays the number of OAMPDUs that have been transmitted on the port.
Rx	Displays the number of OAMPDUs that have been received on the port.

Information OAMPDUs	Displays the number of Information OAMPDUs that have been transmitted or received on the port.
Unique Event Notification OAMPDUs	Displays the number of Unique Event Notification OAMPDUs that have been transmitted or received on the port.
Duplicate Event Notification OAMPDUs	Displays the number of Duplicate Event Notification OAMPDUs that have been transmitted or received on the port.
Variable Request OAMPDUs	Displays the number of Variable Request OAMPDUs that have been transmitted or received on the port.
Variable Response OAMPDUs	Displays the number of Variable Response OAMPDUs that have been transmitted or received on the port.
Loopback Control OAMPDUs	Displays the number of Loopback Control OAMPDUs that have been transmitted or received on the port.
Organization Specific OAMPDUs	Displays the number of Organization Specific OAMPDUs that have been transmitted or received on the port.
Unsupported OAMPDUs	Displays the number of Unsupported OAMPDUs that have been transmitted or received on the port.
Frames Lost Due To OAM	Displays the number of frames that are not transmitted successfully on the OAM sublayer but not due to an internal OAM error.

2. In the Event Logs Statistics section, select a port to view the local and remote event logs on it.


Event Logs Statistics

	LOCAL	REMOTE
Error Symbol Period Events	0	0
Error Frame Events	0	0
Error Frame Period Events	0	0
Error Frame Seconds Events	0	0
Dying Gasp Events	0	0
Critical Events	0	0

Event Log Table:

TYPE	LOCATION	TIMESTAMP	VALUE	WINDOW	THRESHOLD	ACCUMULATED

No entry in the table.

Local	Displays the number of link events that have occurred on the local link.
Remote	Displays the number of link events that have occurred on the remote link.
Error Symbol Period Events	Displays the number of error symbol period link events that have occurred on the local link or remote link.

Error Frame Events	Displays the number of error frame link events that have occurred on the local link or remote link.
Error Frame Period Events	Displays the number of error frame period link events that have occurred on the local link or remote link.
Error Frame Seconds Events	Displays the number of error frame seconds link events that have occurred on the local link or remote link.
Dying Gasp Events	Displays the number of Dying Gasp link events that have occurred on the local link or remote link.
Critical Events	Displays the number of Critical Event link events that have occurred on the local link or remote link.

Additionally, you can view the detailed information of the event logs in the **Event Log Table** section.

Type	Displays the types of the link event.
Location	Displays the location where the link event occurred.
Timestamp	Displays the time reference when the link event occurred.
Value	Displays the number of symbol errors or frame errors in the period.
Window	Displays the period of the link event.
Threshold	Displays the threshold of the errors.
Accumulated Errors	Displays the number of errors that have been detected since the OAM feature was last reset.

9. 5 DLDP

Overview

DLDP (Device Link Detection Protocol) is a Layer 2 protocol that enables devices connected through fiber or twisted-pair Ethernet cables to detect whether a unidirectional link exists.

A unidirectional link occurs whenever traffic sent by a local device is received by its peer device but traffic from the peer device is not received by the local device.

Unidirectional links can cause a variety of problems, such as spanning-tree topology loops. Once detecting a unidirectional link, DLDP can shut down the related port automatically or inform users.

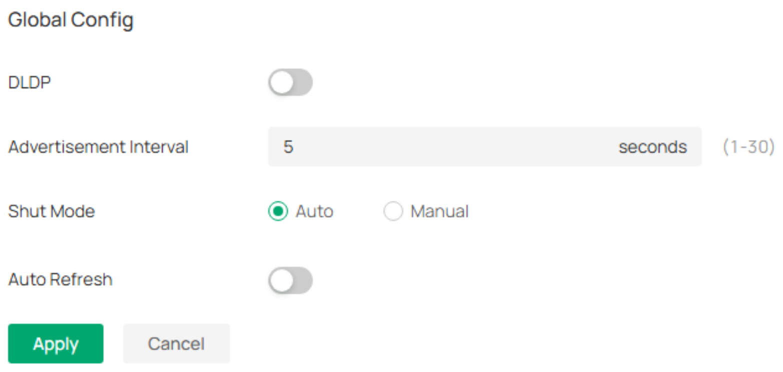
Configuration

Note:

1. A DLDP-capable port cannot detect a unidirectional link if it is connected to a DLDP-incapable port of another device.

2. To detect unidirectional links, make sure DLDP is enabled on both sides of the links.

1. Go to Maintenance > DLDP to load the following page. In the Global Config section, enable DLDP and configure the following parameters. Click Apply.



Global Config

DLDP: off

Advertisement Interval: 5 seconds (1-30)

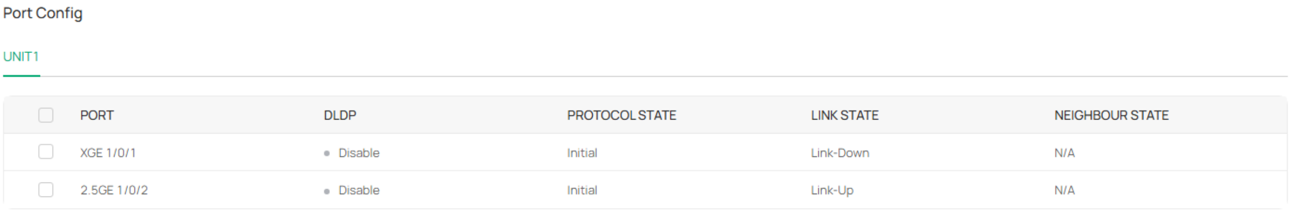
Shut Mode: ● Auto ○ Manual

Auto Refresh: off

DLDP	Enable or disable DLDP globally.
Advertisement Interval	Configure the interval to send advertisement packets. Valid values are from 1 to 30 seconds, and the default value is 5 seconds.
Shut Mode	Choose how to shut down the port when a unidirectional link is detected: Auto: When a unidirectional link is detected on a port, DLDP will generate logs and traps then shut down the port, and DLDP on this port will change to Disabled. Manual: When a unidirectional link is detected on a port, DLDP will generate logs and traps, and then users can manually shut down the unidirectional link ports.
Auto Refresh	With this option enabled, the device will automatically refresh the DLDP information.
Refresh Interval	Specify the time interval at which the device will refresh the DLDP information. Valid values are from 1 to 100 seconds, and the default value is 3 seconds.

2. In the Port Config section, select one or more ports to enable DLDP and click Apply. Then you can

view the relevant DLDP information in the table.



Port Config

UNIT1

□	PORT	DLDP	PROTOCOL STATE	LINK STATE	NEIGHBOUR STATE
□	XGE 1/0/1	● Disable	Initial	Link-Down	N/A
□	2.5GE 1/0/2	● Disable	Initial	Link-Up	N/A

DLDP	Enable or disable DLDP on the port.
Protocol State	Displays the DLDP protocol state. Initial: DLDP is disabled. Inactive: DLDP is enabled but the link is down. Active: DLDP is enabled and the link is up, or the neighbor entries in this device are empty. Advertisement: No unidirectional link is detected (the device has established bidirectional links with all its neighbors) or DLDP has remained in an Active status for more than 5 seconds. Probe: In this state, the device will send out Probe packets to detect whether the link is unidirectional. The port enters this state from the Active state if it receives a packet from an unknown neighbor. Disable: A unidirectional link is detected.
Link State	Displays the link state. Link-Down: The link is down. Link-Up: The link is up.
Neighbour State	Displays the neighbour state. Unknown: Link detection is in progress. Unidirectional: The link between the port and the neighbor is unidirectional. Bidirectional: The link between the port and the neighbor is bidirectional.

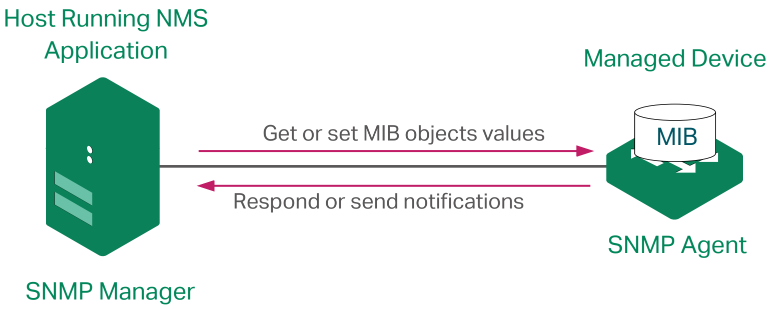
9. 6 SNMP

Overview

SNMP (Simple Network Management Protocol) is a standard network management protocol, widely used on TCP/IP networks. It facilitates device management using NMS (Network Management System) applications. With SNMP, network managers can view or modify the information of network devices, and timely troubleshoot according to notifications sent by those devices.

As the following figure shows, the SNMP system consists of an SNMP manager, an SNMP agent, and a MIB (Management Information Base).

The SNMP manager is a host that runs NMS applications. The agent and MIB reside on the managed device. By configuring SNMP on the device, you define the relationship between the manager and the agent.


Host Running NMS Application
Managed Device
Get or set MIB objects values
MIB
Respond or send notifications
SNMP Agent
SNMP Manager

Configuration

To complete SNMP configurations, follow these steps:

1) Enable SNMP globally.

2) Create an SNMP view.

3) Create SNMP communities (For SNMP v1/v2c)

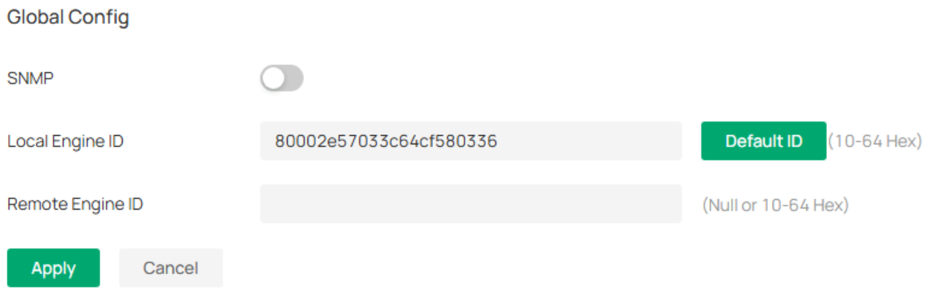
4) Create SNMP groups and users (For SNMP v3)

5) Configure Notifications

6) Configure RMON

9. 6. 1 Enable SNMP Globally

Go to Maintenance > SNMP > Global Config to load the following page. In the Global Config section, enable SNMP globally and configure the following parameters. Click Apply.



Global Config

SNMP ○

Local Engine ID 80002e57033c64cf580336 Default ID (10-64 Hex)

Remote Engine ID (Null or 10-64 Hex)

Apply Cancel

SNMP	Enable or disable SNMP globally.
Local Engine ID	Set the engine ID of the local SNMP agent (the device) with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. By default, the device generates the engine ID using TP-Link's enterprise number (80002e5703) and its own MAC address. The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent.
Remote Engine ID	Set the engine ID of the remote SNMP manager with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. If no remote SNMP manager is needed, you can leave this field empty. The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device that receives Inform messages from the device.

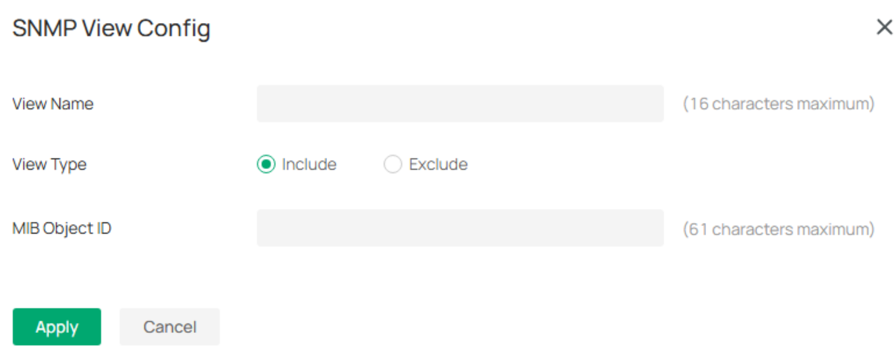
9. 6. 2 Create an SNMP View

Overview

An SNMP view is a subnet of a MIB. NMS manages MIB objects based on the view. The system has a default view named viewDefault. You can create a new one or edit the default view according to your needs.

Configuration

Go to Maintenance > SNMP > Global Config to load the following page. In the SNMP View Config section, click + Add and configure the following parameters. Click Create.



SNMP View Config

View Name (16 characters maximum)

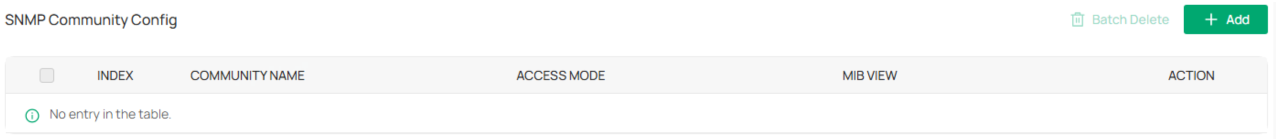
View Type ● Include ○ Exclude

MIB Object ID (61 characters maximum)

View Name	Set the view name with 1 to 16 characters. A complete view consists of all MIB objects that have the same view name.
View Type	Set the view to include or exclude the related MIB object. Include: The NMS can view or manage the function indicated by the object. Exclude: The NMS cannot view or manage the function indicated by the object.
MIB Object ID	Enter a MIB Object ID to specify a specific function of the device. When a MIB Object ID is specified, all its child Object IDs are specified. For specific ID rules, refer to the device related MIBs.

9. 6. 3 Create SNMP Communities (For SNMP v1/v2c)

Go to Maintenance > SNMP > SNMP v1/v2c to load the following page. Click + Add and configure the following parameters. Click Create.



SNMP Community Config

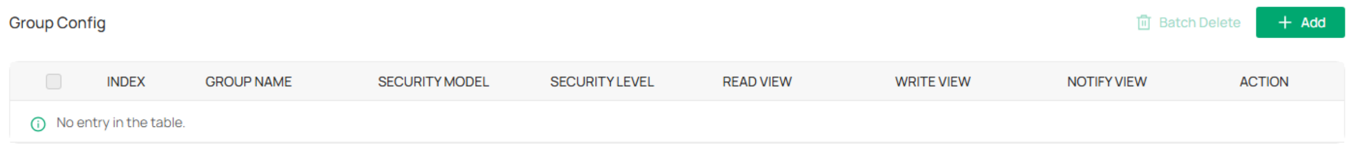
□	INDEX	COMMUNITY NAME	ACCESS MODE	MIB VIEW	ACTION

No entry in the table.

Community Name	Configure the community name. This community name is used like a password and the NMS can access the specified MIB objects of the device using the same community name.
Access Mode	Specify the access right to the related view. Read Only: The NMS can view but not modify parameters of the specified view. Read & Write: The NMS can view and modify parameters of the specified view.
MIB View	Choose an SNMP view that allows the community to access.

9. 6. 4 Create SNMP Groups and Users (For SNMP v3)

1. Go to Maintenance > SNMP > SNMP v3 to load the following page. In the Group Config section, click + Add and configure the following parameters. Click Create.



Group Config

□	INDEX	GROUP NAME	SECURITY MODEL	SECURITY LEVEL	READ VIEW	WRITE VIEW	NOTIFY VIEW	ACTION

No entry in the table.

Group Name

Set the SNMP group name using 1 to 16 characters.

The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group.

Security Model

Displays the security model. SNMPv3 uses v3, the most secure model.

Security Level

Set the security level for the SNMPv3 group.

NoAuthNoPriv**:** No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them.

AuthNoPriv**:** An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them.

AuthPriv**:** An authentication algorithm and a privacy algorithm are applied to check and encrypt packets.

Read View

Choose a view to allow parameters to be viewed but not modified by the NMS. The view is necessary for any group.

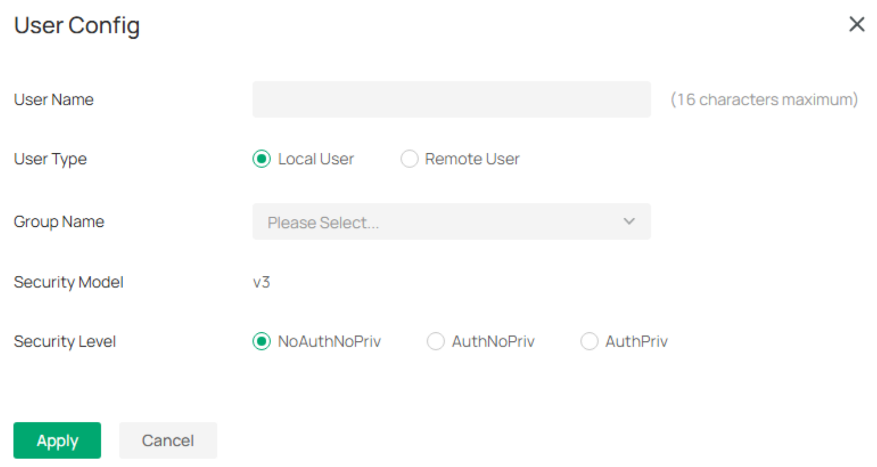
Write View

Choose a view to allow parameters to be modified by the NMS. The view in Write View should also be added to Read View.

Notify View

Choose a view to allow it to send notifications to the NMS.

2. In the User Config section, click + Add and configure the following parameters. Click Create.



User Config

User Name: (16 characters maximum)

User Type: ● Local User ○ Remote User

Group Name: Please Select...

Security Model: v3

Security Level: ● NoAuthNoPriv ○ AuthNoPriv ○ AuthPriv

User Name

Set the SNMP user name using 1 to 16 characters. For different entries, user names cannot be the same.

User Type	Choose a user type based on the location of the user. Local User: The user resides on the local engine, which is the SNMP agent of the device. Remote User: The user resides on the NMS. Before configuring a remote user, you need to set the remote engine ID first. The remote engine ID and user password are used when computing the authentication and privacy digests.
Group Name	Choose the name of the group that the user belongs to. Users with the same Group Name, Security Model and Security Level will be in the same group.
Security Model	Displays the security model. SNMPv3 uses v3, the most secure model.
Security Level	Set the security level. The security level from lowest to highest is: NoAuthNoPriv, AuthNoPriv, AuthPriv. The security level of the user should not be lower than the group it belongs to. NoAuthNoPriv: No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. AuthNoPriv: An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. AuthPriv: An authentication algorithm and a privacy algorithm are applied to check and encrypt packets.

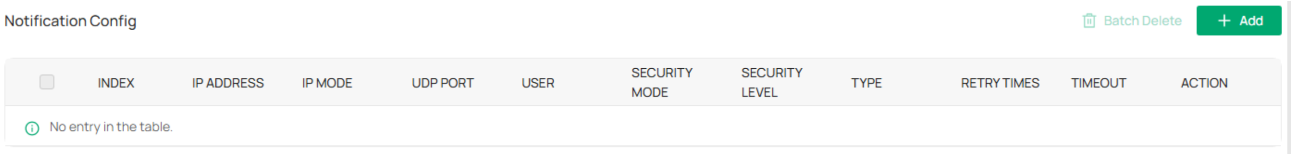
9. 6. 5 Configure Notifications

Overview

With Notification enabled, the device can send notifications to the NMS about important events relating to the device’s operation. This facilitates the monitoring and management of the NMS.

Configuration

1. Go to Maintenance > SNMP > Notification to load the following page. In the Notification Config section, click + Add and configure the following parameters. Click Create.



Notification Config

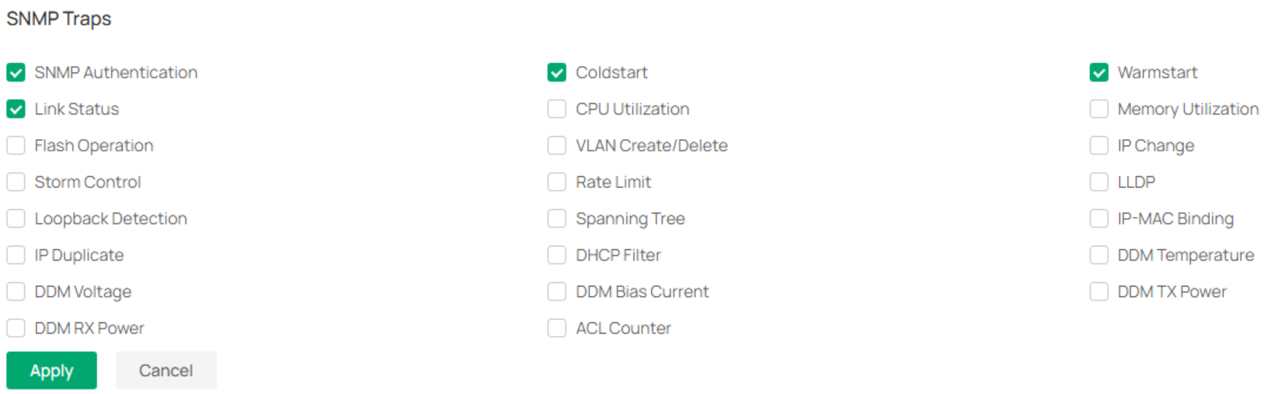
□	INDEX	IP ADDRESS	IP MODE	UDP PORT	USER	SECURITY MODE	SECURITY LEVEL	TYPE	RETRY TIMES	TIMEOUT	ACTION

No entry in the table.

IP Mode	Choose an IP mode for the NMS host.
IP Address	If you set IP Mode as IPv4, specify an IPv4 address for the NMS host. If you set IP Mode as IPv6, specify an IPv6 address for the NMS host.

UDP Port	Specify a UDP port on the NMS host to receive notifications. For security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected.
User	Choose the user name or community name used by the NMS host.
Security Mode	If a community name (created for SNMPv1/v2c) is selected in User, specify the security mode as v1 or v2c. If a user name (created for SNMPv3) is selected in User, here displays the security mode as v3. **Note**: The NMS host should use the corresponding SNMP version.
Security Level	If Security mode is v3, here displays the security level of the user.
Type	Choose a notification type for the NMS host. For SNMPv1, the supported type is Trap. For SNMPv2c and SNMPv3, you can configure the type as Trap or Inform. Trap: The device will send Trap messages to the NMS host when certain events occur. When the NMS host receives a Trap message, it will not send a response to the device. Thus the device cannot tell whether a message is received or not, and the messages that are not received will not be resent. Inform: The device will send Inform messages to the NMS host when certain events occur. When the NMS host receives an Inform message, it sends a response to the device. If the device does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap.
Retry Times	Set the retry times for Informs. The device will resend the Inform message if it does not receive any response from the NMS host within the timeout interval. It will stop sending Inform messages when the retry time reaches the limit.
Timeout	Set the time that the device waits for a response from the NMS host after sending an inform message.

2. In the SNMP Traps section, click + Add and configure the following parameters. Select the traps to be enabled according to your needs. With a trap enabled, the device will send the corresponding trap message to the NMS when the trap is triggered. Click Apply.



SNMP Traps

☑ SNMP Authentication
☑ Link Status
☐ Flash Operation
☐ Storm Control
☐ Loopback Detection
☐ IP Duplicate
☐ DDM Voltage
☐ DDM RX Power

☑ Coldstart
☐ CPU Utilization
☐ VLAN Create/Delete
☐ Rate Limit
☐ Spanning Tree
☐ DHCP Filter
☐ DDM Bias Current
☐ ACL Counter

☑ Warmstart
☐ Memory Utilization
☐ IP Change
☐ LLDP
☐ IP-MAC Binding
☐ DDM Temperature
☐ DDM TX Power

SNMP Authentication	Triggered when a received SNMP request fails the authentication.

Coldstart	Indicates that the SNMP entity is reinitializing itself such that its configurations may be changed. The trap can be triggered when you reboot the device.
Warmstart	Indicates that the SNMP entity is reinitializing itself with its configurations unchanged. For a device running SNMP, the trap can be triggered if you disable and then enable SNMP without changing any parameters.
Link Status	Enable or disable Link Status Trap globally. The trap includes the following two sub-traps: Linkup Trap: Indicates that a port status changes from linkdown to linkup. Linkdown Trap: Indicates that a port status changes from linkup to linkdown. Link Status Trap can be triggered when it is enabled both globally and on the port, and you connect a new device to the port or disconnect a device from the port. By default, the trap is enabled both globally and on all ports, which means that link status changes on any ports will trigger the trap.
CPU Utilization	Triggered when the CPU utilization exceeds 80%.
Memory Utilization	Triggered when the memory utilization exceeds 80%.
Flash Operation	Triggered when flash is modified during operations such as backup, reset, firmware upgrade, and configuration import.
VLAN Create/Delete	Triggered when certain VLANs are created or deleted successfully.
IP Change	Monitors the changes of interfaces' IP addresses. The trap can be triggered when the IP address of any interface is changed.
Storm Control	Monitors whether the storm rate has reached the limit that you have set. The trap can be triggered when the Strom Control feature is enabled and broadcast/multicast/unknown-unicast frames are sent to the port with a rate higher than what you have set.
Rate Limit	Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.
LLDP	The trap includes the following sub-traps: LLDP RemTablesChange: Indicates that the device senses an LLDP topology change. The trap can be triggered when adding or removing a remote device, and when the information of some remote devices is aged out or cannot be stored into the device because of insufficient resources. This trap can be used by an NMS to trigger LLDP remote systems table maintenance polls. LLDP TopologyChange: Indicates that the device senses an LLDP-MED topology change (the topology change of media endpoints). The trap can be triggered when adding or removing a media endpoint that supports LLDP, such as an IP Phone. An LLDP Remtableschange trap will be also triggered every time LLDP Topologychange trap is triggered.

Loopback Detection	Triggered when the Loopback Detection feature is enabled and a loopback is detected or cleared.
Spanning Tree	Indicates spanning tree changes. The trap can be triggered in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a TCN (Topology Change Notification) BPDU or a Configuration BPDU with the TC (Topology Change) bit set.
IP-MAC Binding	Triggered in the following two situations: the ARP Inspection feature is enabled and the device receives an illegal ARP packet; or the IPv4 Source Guard feature is enabled and the device receives an illegal IP packet.
IP Duplicate	Triggered when the device detects an IP conflict.
DHCP Filter	Triggered when the DHCPv4 Filter feature is enabled and the device receives DHCP packets from an illegal DHCP server.
DDM Temperature	Monitors the temperature of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold. **Note**: DDM Temperature is only available on certain devices.
DDM Voltage	Monitors the voltage of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold. **Note**: DDM Voltage is only available on certain devices.
DDM Bias Current	Monitors the bias current of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold. **Note**: DDM Bias Current is only available on certain devices.
DDM TX Power	Monitors the TX Power of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold. **Note**: DDM TX Power is only available on certain devices.
DDM RX Power	Monitors the RX Power of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold. **Note**: DDM RX Power is only available on certain devices.
ACL Counter	Monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in the ACL rule settings enabled, the device will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

9. 6. 6 Configure RMON

Overview

RMON (Remote Network Monitoring) together with the SNMP system allows the network manager to monitor remote network devices efficiently. RMON reduces traffic flow between the NMS and managed devices, which is convenient to manage large networks.

RMON includes two parts: the NMS and the Agents running on every network device. The NMS is usually a host that runs the management software to manage Agents of network devices. The Agent is usually a network device that collects traffic statistics (such as the total number of packets on a network segment during a certain time period, or total number of correct packets that are sent to a host). Based on SNMP protocol, the NMS collects network data by communicating with Agents. However, the NMS cannot obtain every datum of RMON MIB because the device resources are limited. Generally, the NMS can only get information of the following four groups: Statistics, History, Event and Alarm.

- **Statistics:**

  Collects Ethernet statistics (like the total received bytes, the total number of broadcast packets, and the total number of packets with specified size) on an interface.

- **History:**

  Collects a history group of statistics on Ethernet ports for a specified polling interval.

- **Event:**

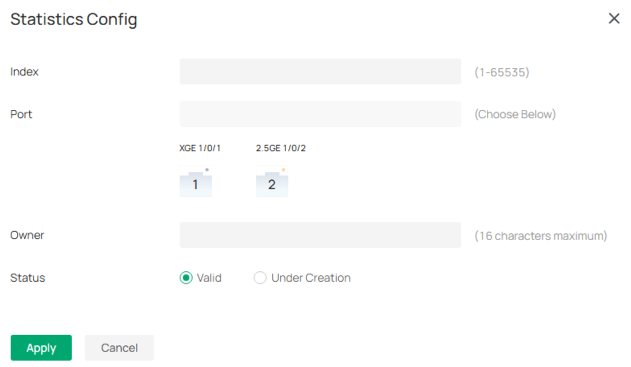
  Specifies the action to be taken when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

- **Alarm:**

  Monitors a specific MIB object for a specified interval, and triggers an event at a specified value (rising threshold or falling threshold).

Configuration

1. Go to Maintenance > SNMP > RMON. In the Statistics Config section, click + Add and configure the following parameters. Click Create.



Statistics Config ×

Index (1-65535)

Port (Choose Below)

XGE 1/0/1 2.5GE 1/0/2

1 2

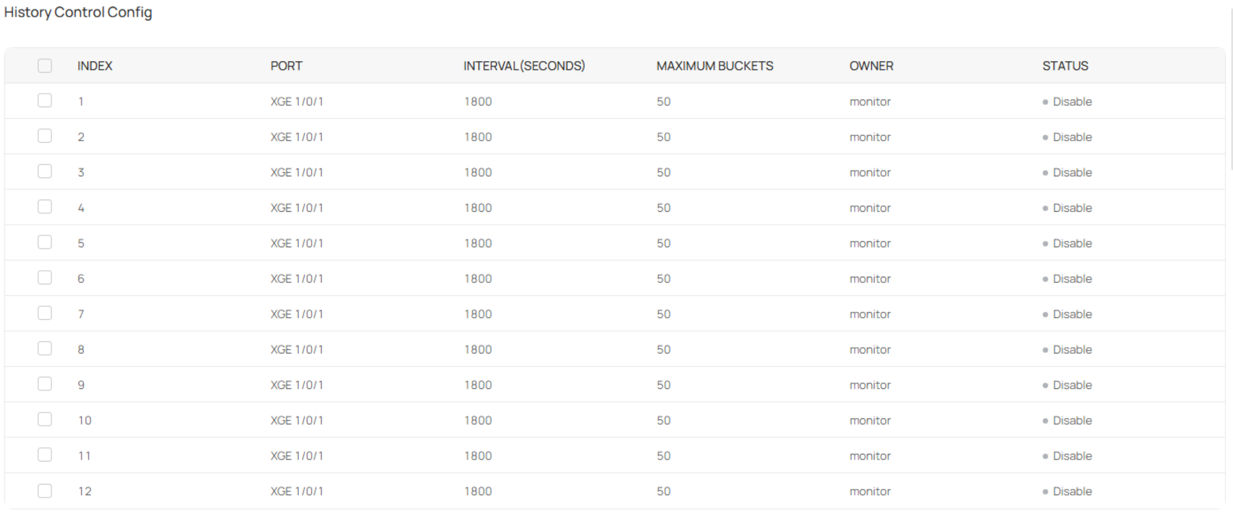
Owner (16 characters maximum)

Status ● Valid ○ Under Creation

Apply Cancel

Index	Enter the index of the entry.
Port	Specify an Ethernet port to be monitored in the entry. You can click **Choose** to choose a port from the list or manually enter the port number, for example, 1/0/1 in the input box.
Owner	Enter the owner name of the entry with1 to 16 characters.
Status	Set the entry as Valid or Under Creation. By default, it is Valid. The device starts to collect Ethernet statistics for a Statistics entry since the entry status is configured as valid. Valid: The entry is created and valid. Under Creation: The entry is created but invalid.

2. In the History Control Config section, select a History entry and configure the following parameters. Click Apply.



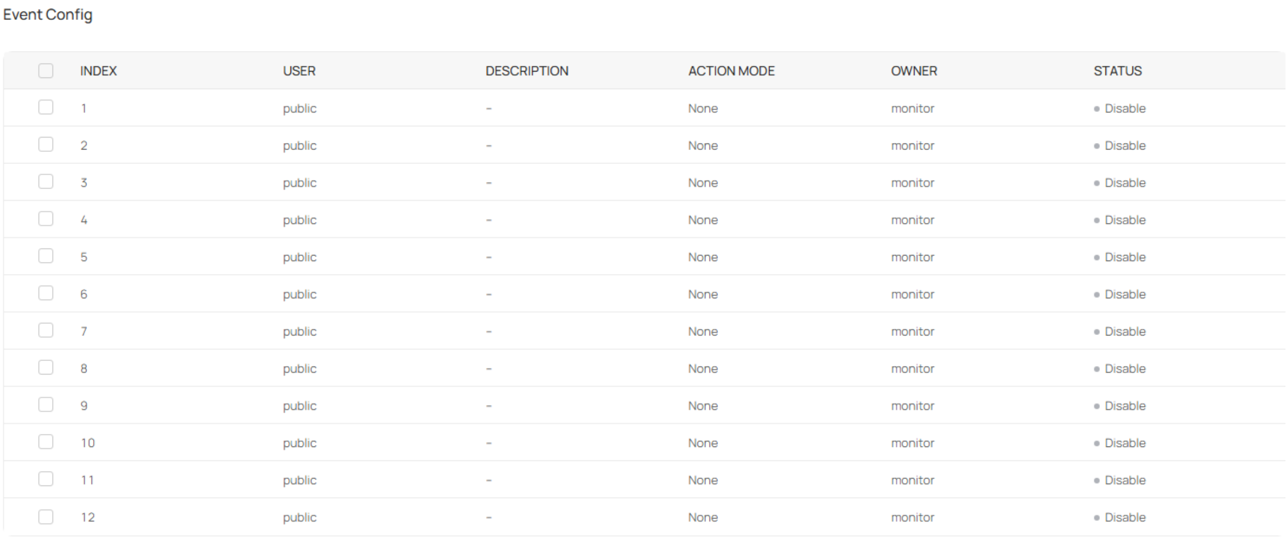
History Control Config

□	INDEX	PORT	INTERVAL (SECONDS)	MAXIMUM BUCKETS	OWNER	STATUS
□	1	XGE 1/0/1	1800	50	monitor	● Disable
□	2	XGE 1/0/1	1800	50	monitor	● Disable
□	3	XGE 1/0/1	1800	50	monitor	● Disable
□	4	XGE 1/0/1	1800	50	monitor	● Disable
□	5	XGE 1/0/1	1800	50	monitor	● Disable
□	6	XGE 1/0/1	1800	50	monitor	● Disable
□	7	XGE 1/0/1	1800	50	monitor	● Disable
□	8	XGE 1/0/1	1800	50	monitor	● Disable
□	9	XGE 1/0/1	1800	50	monitor	● Disable
□	10	XGE 1/0/1	1800	50	monitor	● Disable
□	11	XGE 1/0/1	1800	50	monitor	● Disable
□	12	XGE 1/0/1	1800	50	monitor	● Disable

Index	Displays the index of History entries. The device supports up to 12 History entries.
Port	Specify a port to be monitored.
Interval (seconds)	Specify the number of seconds in each polling cycle. Valid values are from 10 to 3600 seconds. Every history entry has its own timer. For the monitored port, the device samples packet information and generates a record in every interval.
Maximum Buckets	Set the maximum number of records for the History entry. Valid values are from 10 to 130. When the number of records exceeds the limit, the earliest record will be overwritten.
Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.

Status	Enable or disable the entry. By default, it is disabled. Enable: The entry is enabled. Disable: The entry is disabled.

3. In the Event Config section, select an Event entry and configure the following parameters. Click Apply.



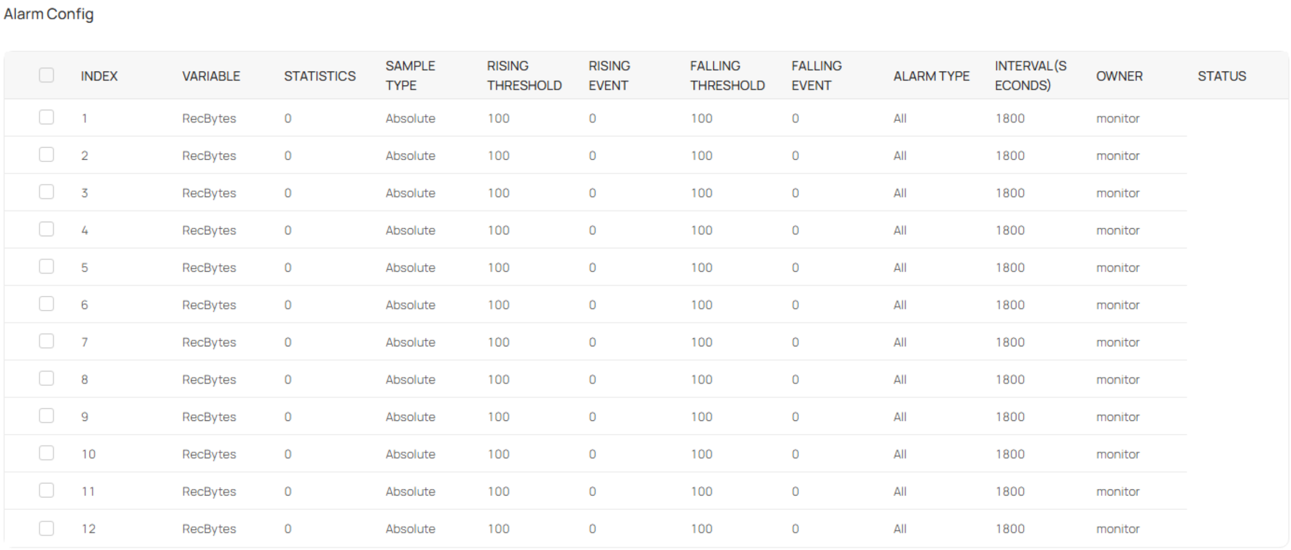
Event Config

□	INDEX	USER	DESCRIPTION	ACTION MODE	OWNER	STATUS
□	1	public	-	None	monitor	● Disable
□	2	public	-	None	monitor	● Disable
□	3	public	-	None	monitor	● Disable
□	4	public	-	None	monitor	● Disable
□	5	public	-	None	monitor	● Disable
□	6	public	-	None	monitor	● Disable
□	7	public	-	None	monitor	● Disable
□	8	public	-	None	monitor	● Disable
□	9	public	-	None	monitor	● Disable
□	10	public	-	None	monitor	● Disable
□	11	public	-	None	monitor	● Disable
□	12	public	-	None	monitor	● Disable

Index	Displays the index of Event entries. The device supports up to 12 Event entries.
User	Choose an SNMP user name or community name for the entry. Only the specified user can access the log messages or receive the notification messages related to the event.
Description	Enter an brief description of this event to make it easier to be identified.
Action Mode	Specify the action for the device to take when the event is triggered. None: No action. Log: The device records the event in the log, and the NMS should initiate requests to get notifications. Notify: The device sends notifications to the NMS. Log & Notify: The device records the event in the log and sends notifications to the NMS.
Owner	Enter the owner name of the entry with 1 to 16 characters.
Status	Enable or disable the entry. Enable: The entry is enabled. Disable: The entry is disabled.

4. In the Alarm Config section, select an Alarm entry and configure the following parameters. Click

Apply.



Alarm Config

□	INDEX	VARIABLE	STATISTICS	SAMPLE TYPE	RISING THRESHOLD	RISING EVENT	FALLING THRESHOLD	FALLING EVENT	ALARM TYPE	INTERVAL(SECONDS)	OWNER	STATUS
□	1	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	2	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	3	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	4	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	5	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	6	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	7	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	8	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	9	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	10	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	11	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	
□	12	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	

Index

Displays the index of Alarm entries. The device supports up to 12 Alarm entries.

Variable

Set the alarm variable to be monitored. The device will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered.

RecBytes: Total number of received bytes.

RecPackets: Total number of received packets.

BPackets: Total number of broadcast packets.

MPackets: Total number of multicast packets.

CRC&Align ERR: Packets that contain FCS Error or Alignment Error, within a size of 64 to 1518 bytes.

Undersize: Packets that are smaller than 64 bytes.

Oversize: Packets that are larger than 1518 bytes.

Jabbers: Packets that are sent when port collisions occur.

Collisions: Collision times in the network segment.

64, 65-127, 128-255, 256-511, 512-1023, 1024-1518: Total number of packets of the specified size.

Statistics

Associate the Alarm entry with a Statistics entry. Then the device monitors the specified variable of the Statistics entry.

Sample Type

Specify the sampling method of the specified variable.

Absolute: Compare the sampling value against the preset threshold.

Delta: The device obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold.

Rising Threshold	Specify the rising threshold of the variable. Valid values are from 1 to 2147483647. When the sampling value or the difference value exceeds the threshold, the system will trigger the corresponding Rising Event. **Note**: The rising threshold should be larger than the falling threshold.
Rising Event	Specify the index of the Event entry that will be triggered when the sampling value or the difference value exceeds the preset threshold. The Event entry specified here should be enabled first.
Falling Threshold	Set the falling threshold of the variable. Valid values are from 1 to 2147483647. When the sampling value or the difference value is below the threshold, the system will trigger the corresponding Falling Event. **Note**: The falling threshold should be less than the rising threshold.
Falling Event	Specify the index of the Event entry that will be triggered when the sampling value or the difference value is below the preset threshold. The Event entry specified here should be enabled first.
Alarm Type	Specify the alarm type for the entry. Rising: The alarm is triggered only when the sampling value or the difference value exceeds the rising threshold. Falling: The alarm is triggered only when the sampling value or the difference value is below the falling threshold. All: The alarm is triggered when the sampling value or the difference value exceeds the rising threshold or is below the falling threshold.
Interval (seconds)	Set the sampling interval. Valid values are from 10 to 3600 seconds.
Owner	Enter the owner name of the entry with 1 to 16 characters.
Status	Enable or disable the entry. Enable: The entry is enabled. Disable: The entry is disabled.

9. 7 Logs

Overview

The device generates messages in response to events, faults, or errors occurred, as well as changes in configuration or other occurrences. You can check system messages for debugging and network management.

System logs can be saved in various destinations, such as the log buffer, log file or remote log servers, depending on your configuration. Logs saved in the log buffer and log file are called local logs, and logs saved in remote log servers are called remote logs. Remote logs facilitate you to remotely monitor the running status of the network.

You can set the severity level of the log messages to control the type of log messages saved in each destination.

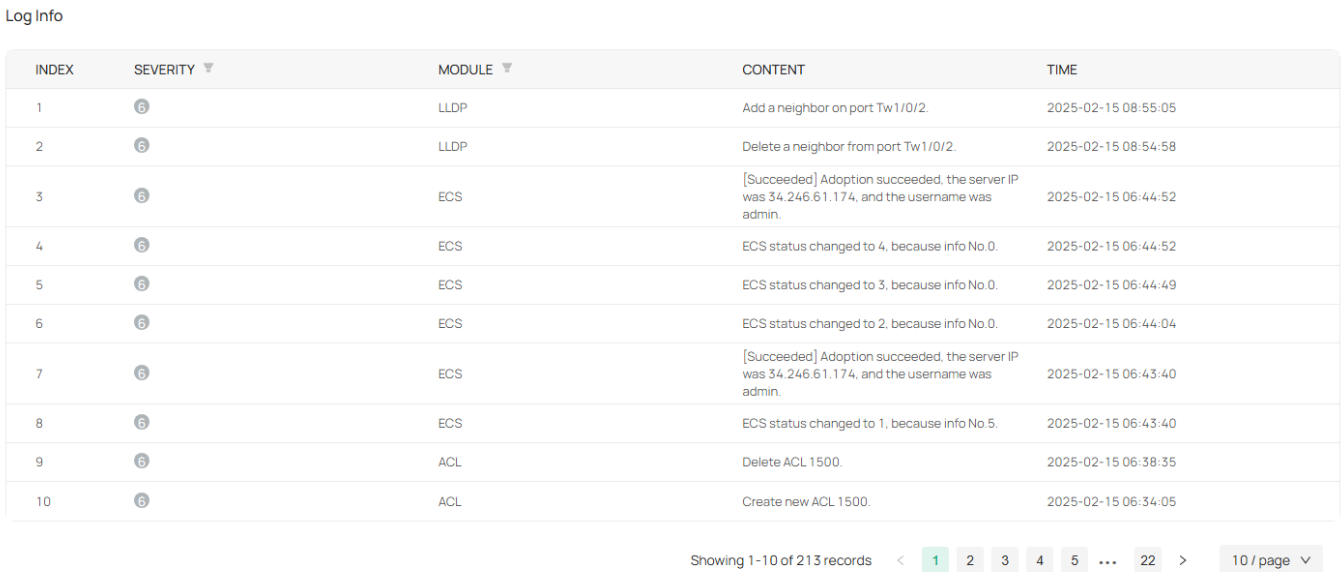
Configuration

System logs configurations include:

- **Viewing the log table.**
- **Configure the local logs.**
- **Configure the remote logs.**
- **Backing up the logs.**

9. 7. 1 View the Log Table

Go to Maintenance > Logs > Log Table to load the following page. Select a module and a severity to view the corresponding log information.



Log Info

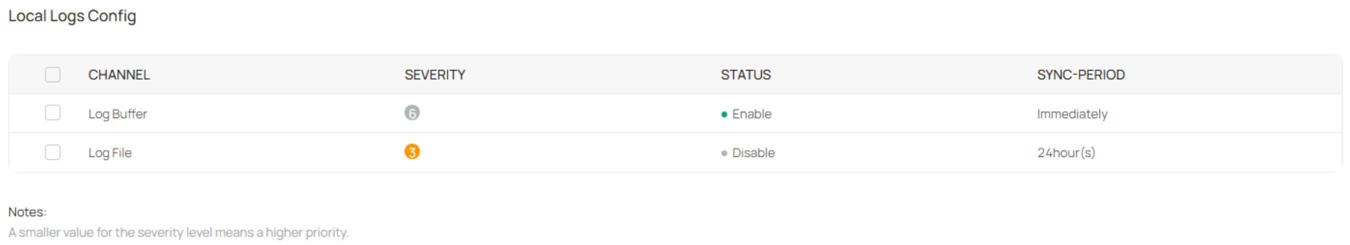
INDEX	SEVERITY	MODULE	CONTENT	TIME
1	6	LLDP	Add a neighbor on port Tw1/0/2.	2025-02-15 08:55:05
2	6	LLDP	Delete a neighbor from port Tw1/0/2.	2025-02-15 08:54:58
3	6	ECS	[Succeeded] Adoption succeeded, the server IP was 34.246.61.174, and the username was admin.	2025-02-15 06:44:52
4	6	ECS	ECS status changed to 4, because info No.0.	2025-02-15 06:44:52
5	6	ECS	ECS status changed to 3, because info No.0.	2025-02-15 06:44:49
6	6	ECS	ECS status changed to 2, because info No.0.	2025-02-15 06:44:04
7	6	ECS	[Succeeded] Adoption succeeded, the server IP was 34.246.61.174, and the username was admin.	2025-02-15 06:43:40
8	6	ECS	ECS status changed to 1, because info No.5.	2025-02-15 06:43:40
9	6	ACL	Delete ACL 1500.	2025-02-15 06:38:35
10	6	ACL	Create new ACL 1500.	2025-02-15 06:34:05

Time	Displays the time the log event occurred.

Module	Select a module from the drop-down list to display the corresponding log information.
Severity	Select a severity level to display the log information whose severity level value is the same or smaller.
Content	Displays the detailed information of the log event.

9. 7. 2 Configure the Local Logs

Go to Maintenance > Logs > Local Logs to load the following page. Select a channel and configure the following parameters. Click Apply.



Local Logs Config

☐	CHANNEL	SEVERITY	STATUS	SYNC-PERIOD
☐	Log Buffer	6	● Enable	Immediately
☐	Log File	3	● Disable	24hour(s)

Notes:
A smaller value for the severity level means a higher priority.

Channel	Local logs includes 2 channels: log buffer and log file. Log buffer indicates the RAM for saving system logs. The channel is enabled by default. Information in the log buffer is displayed on the MAINTENANCE > Logs > Log Table page. It will be lost when the device is restarted. Log file indicates the flash sector for saving system logs. Information in the log file will not be lost after the device is restarted and can be exported on the MAINTENANCE > Logs > Back Up Logs page.
Severity	Specify the severity level of the log messages that are saved to the selected channel. Only log messages with a severity level value that is the same or lower than this will be saved. There are eight severity levels marked from 0 to 7. A lower value indicates a higher severity.
Status	Enable or disable the channel.
Sync-Periodic	By default, the log information is saved in the log buffer immediately, and synchronized to the log file every 24 hours.

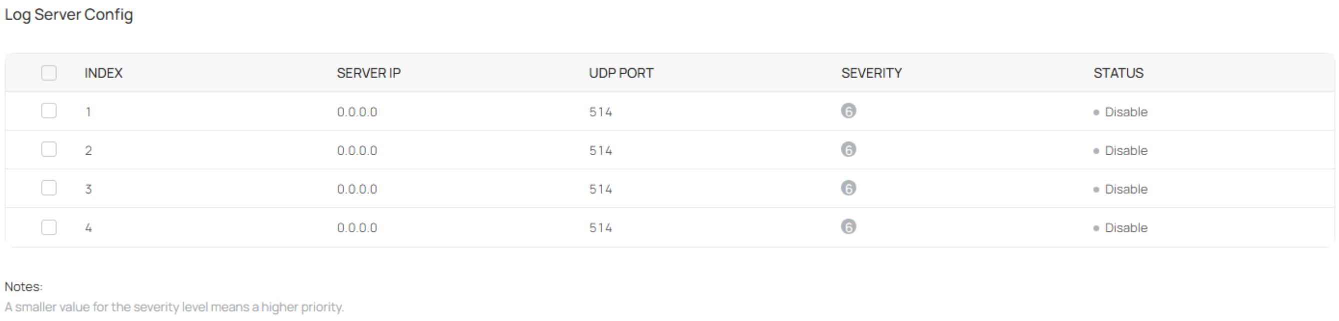
9. 7. 3 Configure the Remote Logs

Overview

You can configure up to four hosts to receive the device's system logs. These hosts are called Log Servers. The device will forward the log message to the servers once a log message is generated. To display the logs, the servers should run a log server software that complies with the syslog standard.

Configuration

Go to Maintenance > Logs > Remote Logs to load the following page. Select a log server entry and configure the following parameters. Click Apply.



Log Server Config

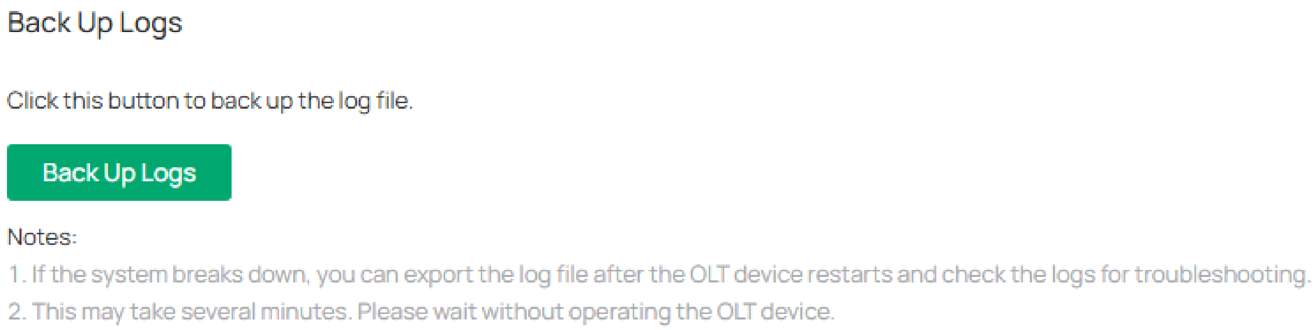
□	INDEX	SERVER IP	UDP PORT	SEVERITY	STATUS
□	1	0.0.0.0	514	6	● Disable
□	2	0.0.0.0	514	6	● Disable
□	3	0.0.0.0	514	6	● Disable
□	4	0.0.0.0	514	6	● Disable

Notes:
A smaller value for the severity level means a higher priority.

Server IP	Specify an IP address of the log server.
UDP Port	Displays the UDP port used by the server to receive the log messages. The device uses standard port 514 to send log messages.
Severity	Specify the severity level of the log messages sent to the selected log server. Only log messages with a severity level value that is the same or lower than this will be saved.
Status	Enable or disable the log server.

9. 7. 4 Back Up Logs

Go to Maintenance > Logs > Back Up Logs to load the following page. Click Back Up Logs to save the system logs as a file on your computer. If the switch system breaks down, you can check the file for troubleshooting.



Back Up Logs

Click this button to back up the log file.

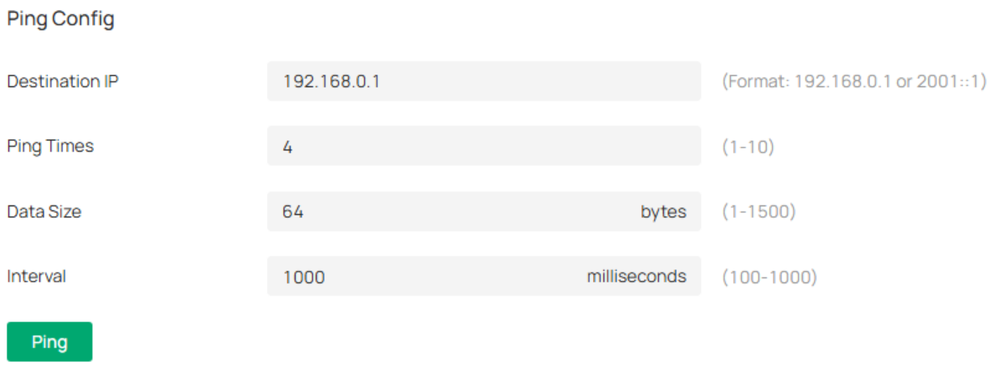
Notes:
1. If the system breaks down, you can export the log file after the OLT device restarts and check the logs for troubleshooting.
2. This may take several minutes. Please wait without operating the OLT device.

9. 8 Diagnostics

The network diagnostics feature provides Ping testing and Tracert testing. You can test connectivity to other devices.

9. 8. 1 Troubleshooting with Ping Testing

1. Go to Maintenance > Diagnostics > Ping Test to load the following page. You can use the Ping tool to test connectivity to remote hosts. In the Ping Config section, configure the following parameters and click Ping to start the test.



Ping Config

Destination IP: 192.168.0.1 (Format: 192.168.0.1 or 2001::1)

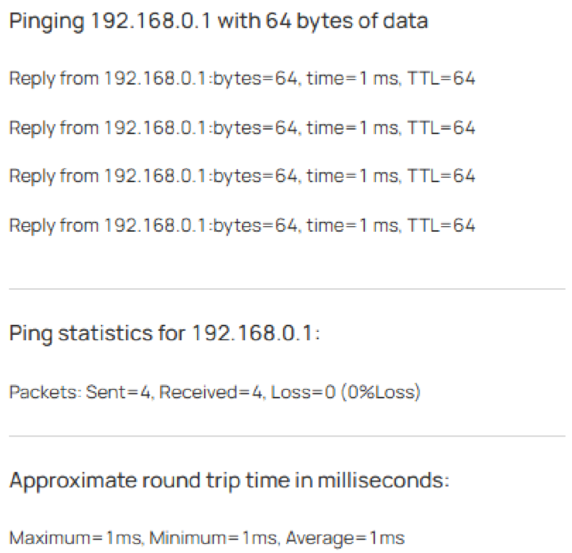
Ping Times: 4 (1-10)

Data Size: 64 bytes (1-1500)

Interval: 1000 milliseconds (100-1000)

Destination IP	Enter the IP address of the destination node for Ping test. Both IPv4 and IPv6 are supported.
Ping Times	Enter the number of times test data will be sent for Ping testing. It is recommended to use the default value of 4.
Data Size	Enter the size of the data sent for Ping testing. It is recommended to keep the default value of 64 bytes.
Interval	Specify the interval at which ICMP request packets are sent. It is recommended to keep the default value of 1000 milliseconds.

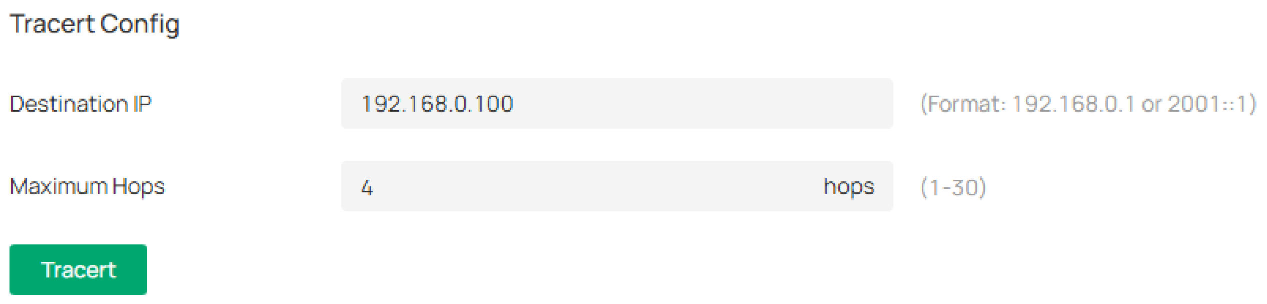
2. In the Ping Result, check the test results.



```
Pinging 192.168.0.1 with 64 bytes of data

Reply from 192.168.0.1:bytes=64, time=1 ms, TTL=64

Reply from 192.168.0.1:bytes=64, time=1 ms, TTL=64

Reply from 192.168.0.1:bytes=64, time=1 ms, TTL=64

Reply from 192.168.0.1:bytes=64, time=1 ms, TTL=64

Ping statistics for 192.168.0.1:

Packets: Sent=4, Received=4, Loss=0 (0%Loss)

Approximate round trip time in milliseconds:

Maximum=1ms, Minimum=1ms, Average=1ms
```

9. 8. 2 Troubleshooting with Tracert Testing

1. Go to Maintenance > Diagnostics > Tracert Test to load the following page. You can use the Tracert tool to find the path from the device to the destination, and test connectivity between devices along the path. In the Tracert Config section, configure the following parameters and click Tracert to start the test. You can click Stop to stop the process at any time.



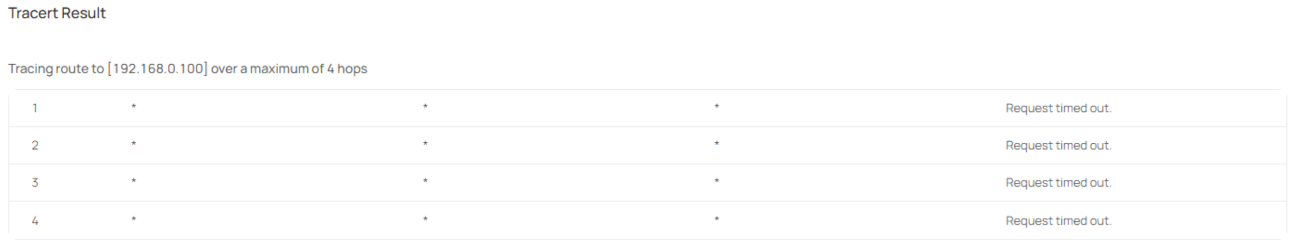
Tracert Config

Destination IP: 192.168.0.100 (Format: 192.168.0.1 or 2001::1)

Maximum Hops: 4 hops (1-30)

Destination IP	Enter the IP address of the destination device. Both IPv4 and IPv6 are supported.
Maximum Hops	Specify the maximum number of the route hops the test data can pass through.

2. In the Tracert Result, check the test results.



Tracert Result

```
Tracing route to [192.168.0.100] over a maximum of 4 hops
1    *    *    *    Request timed out.
2    *    *    *    Request timed out.
3    *    *    *    Request timed out.
4    *    *    *    Request timed out.
```

Chapter 10

Manage System

In System, you can view the system information and configure the system parameters and features of the OLT. The chapter includes the following sections:

10. 1 Configure System Settings and View System Info

Overview

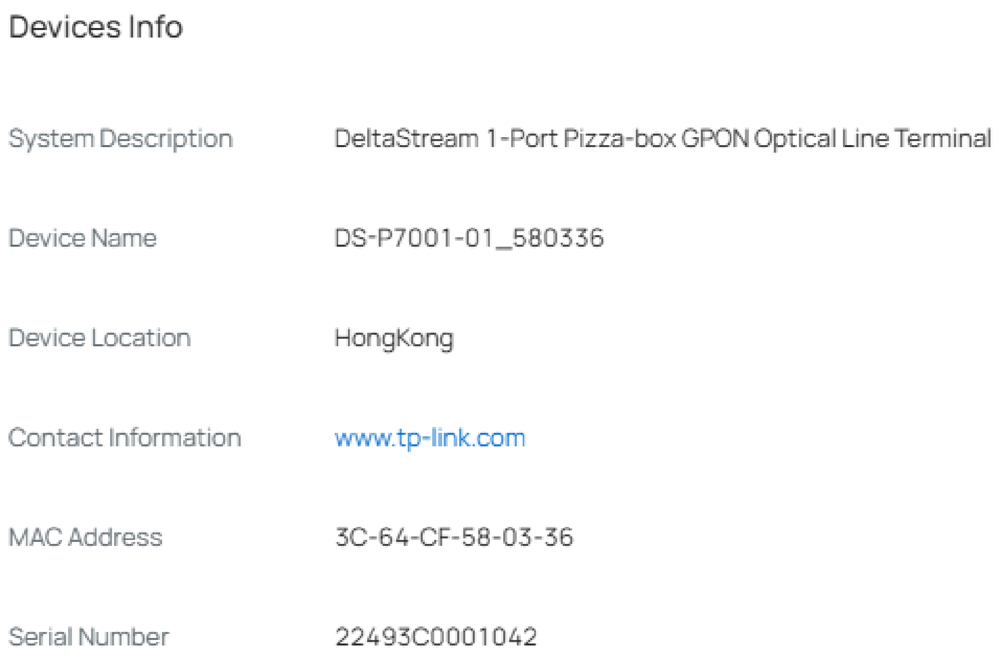
You can view the port status and system information, and configure the device description, system time, and daylight saving time.

10. 1. 1 System Summary

Configuration

- **View the System Information**

Go to System > System Info > System Summary > System Info to load the following page. You can view the system information of the OLT.



Devices Info

System Description DeltaStream 1-Port Pizza-box GPON Optical Line Terminal

Device Name DS-P7001-01_580336

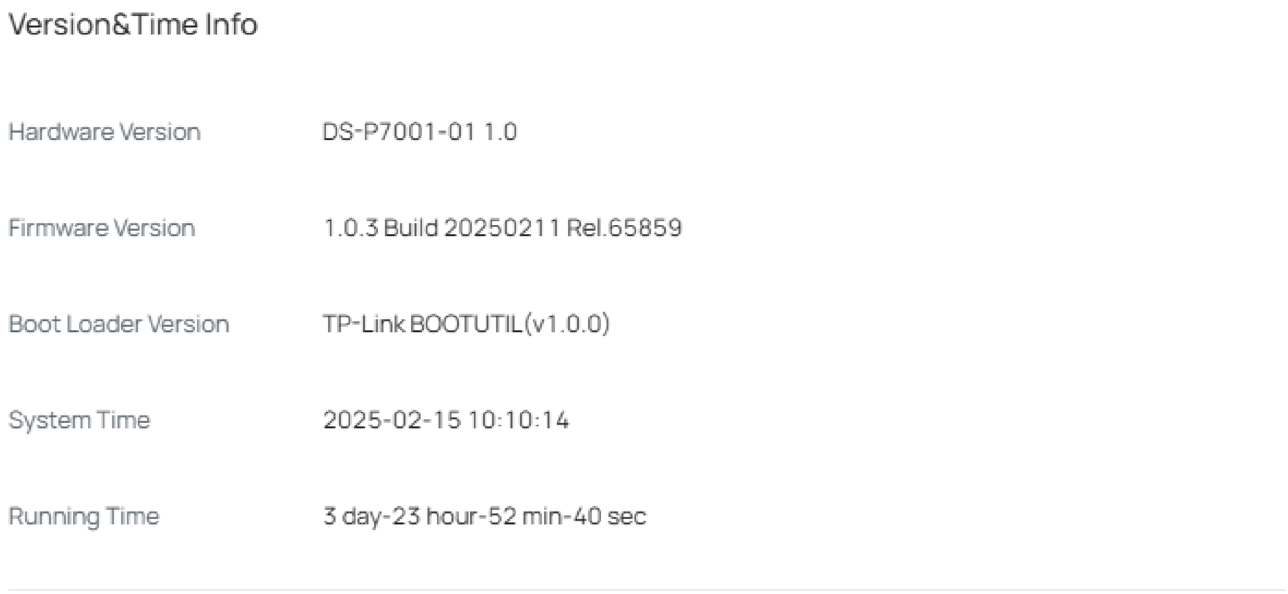
Device Location HongKong

Contact Information www.tp-link.com

MAC Address 3C-64-CF-58-03-36

Serial Number 22493C0001042

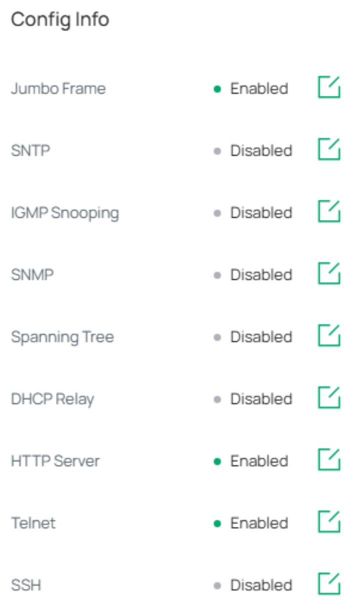
System Description	Displays the system description of the OLT.
Device Name	Displays the name of the OLT. You can edit it on the Device Description page.
Device Location	Displays the location of the OLT. You can edit it on the Device Description page.
Contact Information	Displays the contact information of the OLT. You can edit it on the Device Description page.
MAC Address	Displays the MAC address of the OLT.
Serial Number	Displays the serial number of the OLT.



Version&Time Info

Hardware Version	DS-P7001-01 1.0
Firmware Version	1.0.3 Build 20250211 Rel.65859
Boot Loader Version	TP-Link BOOTUTIL(v1.0.0)
System Time	2025-02-15 10:10:14
Running Time	3 day-23 hour-52 min-40 sec

Hardware Version	Displays the hardware version of the OLT.
Firmware Version	Displays the firmware version of the OLT.
Boot Loader Version	Displays the boot loader version of the OLT.
System Time	Displays the system time of the OLT.
Running Time	Displays the running time of the OLT.



Config Info

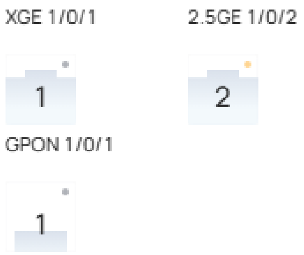
Jumbo Frame	● Enabled	✎
SNTP	● Disabled	✎
IGMP Snooping	● Disabled	✎
SNMP	● Disabled	✎
Spanning Tree	● Disabled	✎
DHCP Relay	● Disabled	✎
HTTP Server	● Enabled	✎
Telnet	● Enabled	✎
SSH	● Disabled	✎

Jumbo Frame	Displays whether Jumbo Frame is enabled. You can click ✎ to jump to the Jumbo Frame configuration page.

SNTP	Displays whether the OLT gets system time from NTP Server. You can click ✎ to jump to the System Time configuration page.
IGMP Snooping	Displays whether IGMP Snooping is enabled. You can click ✎ to jump to the IGMP Snooping configuration page.
SNMP	Displays whether SNMP is enabled. You can click ✎ to jump to the SNMP configuration page.
Spanning Tree	Displays whether Spanning Tree is enabled. You can click ✎ to jump to the Spanning Tree configuration page.
DHCP Relay	Displays whether DHCP Relay is enabled. You can click ✎ to jump to the DHCP Relay configuration page.
HTTP Server	Displays whether HTTP server is enabled. You can click ✎ to jump to the HTTP configuration page.
Telnet	Displays whether Telnet is enabled. You can click ✎ to jump to the Telnet configuration page.
SSH	Displays whether SSH is enabled. You can click ✎ to jump to the SSH configuration page.

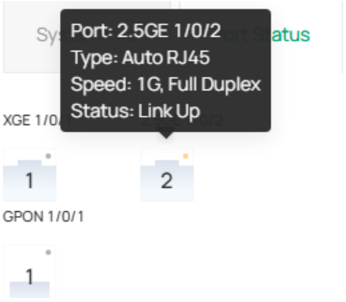
- **View the Port Status**

Go to System > System Info > System Summary > Port Status to load the following page. The color of the dot on the upper right indicates the status of each port.

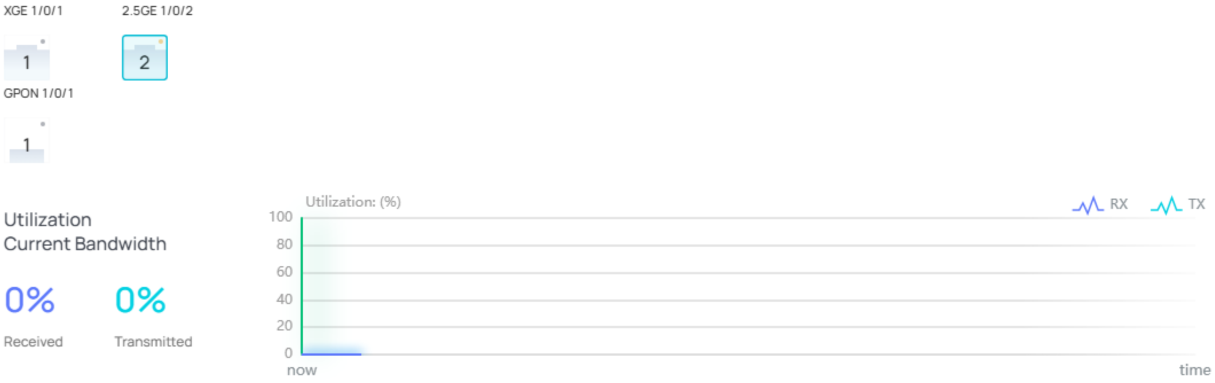


Grey	Indicates the port is not connected to a device.
Green	Indicates the port is transmitting and receiving data at the highest speed.
Yellow	Indicates the port is transmitting and receiving data, but not at the highest speed.

You can move your cursor to a port icon to view the detailed information of the port, and view the bandwidth utilization of each port by clicking the port icon.



Port: 2.5GE 1/0/2
Type: Auto RJ45
Speed: 1G, Full Duplex
Status: Link Up



Utilization
Current Bandwidth

0% Received

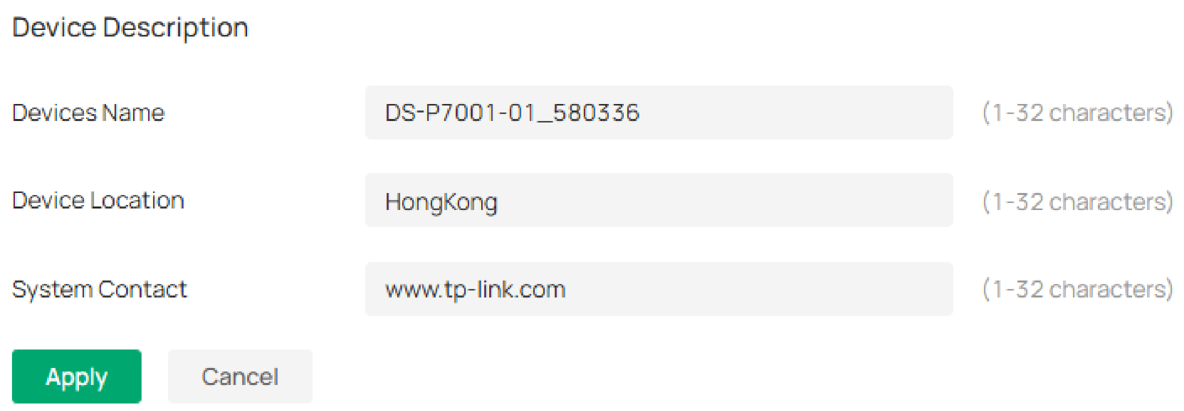
0% Transmitted

Port	Displays the port number.
Type	Displays the type of the port.
Speed	Displays the maximum transmission rate and duplex mode of the port.
Status	Displays the connection status of the port.
Received/RX	Displays the bandwidth utilization of receiving packets on this port.
Transmitted/TX	Displays the bandwidth utilization of sending packets on this port.

10. 1. 2 Device Description

Configuration

Go to System > System Info > Device Description to load the following page. Configure the parameters. Click Apply.



Device Description

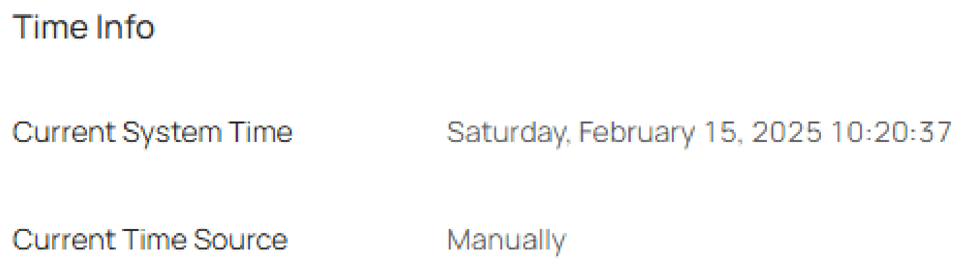
Devices Name	DS-P7001-01_580336	(1-32 characters)
Device Location	HongKong	(1-32 characters)
System Contact	www.tp-link.com	(1-32 characters)

Device Name	Specify a name for the OLT.
Device Location	Enter the location of the OLT.
System Contact	Enter the contact information.

10. 1. 3 System Time

Configuration

1. Go to System > System Info > System Time to load the following page. In Time Info, you can view the current time information.

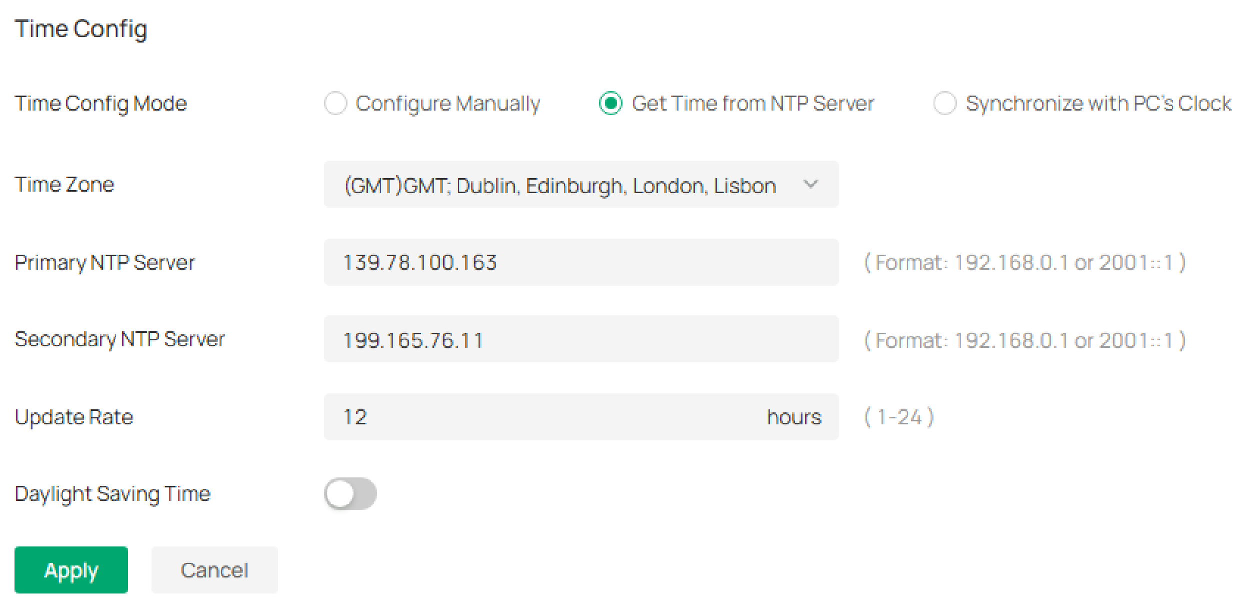


Time Info

Current System Time	Saturday, February 15, 2025 10:20:37
Current Time Source	Manually

Current System Time	Displays the current date and time of the OLT.
Current Time Source	Displays how the OLT gets the current time, which you can configure in the Time Config Mode

2. In Time Config, you can choose one method in the Time Config Mode to set the system time and configure the parameters. Click Apply.



Time Config

Time Config Mode: ○ Configure Manually ● Get Time from NTP Server ○ Synchronize with PC's Clock

Time Zone: (GMT)GMT; Dublin, Edinburgh, London, Lisbon

Primary NTP Server: 139.78.100.163 (Format: 192.168.0.1 or 2001::1)

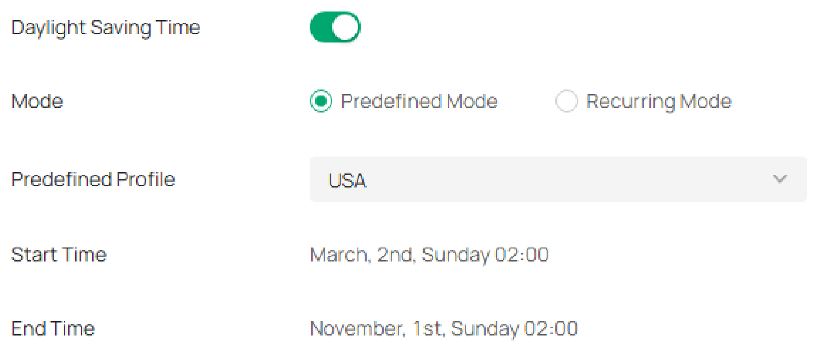
Secondary NTP Server: 199.165.76.11 (Format: 192.168.0.1 or 2001::1)

Update Rate: 12 hours (1-24)

Daylight Saving Time: ○

Manual	Set the system time manually. Date: Specify the date of the system. Time: Specify the time of the system.
Get Time from NTP Server	Get the system time from an NTP server. Make sure the NTP server is accessible on your network. If the NTP server is on the internet, connect the OLT to the internet first. Time Zone: Select your local time zone. Primary Server: Enter the IP Address of the primary NTP server. Secondary Server: Enter the IP Address of the secondary NTP server. Once the primary NTP server is down, the EAP can get the system time from the secondary NTP server. Update Rate: Specify the interval the OLT fetching time from NTP server, which ranges from 1 to 24 hours.
Synchronize with PC's Clock	Synchronize the system time with the clock of your currently logged-in host.

3. (Optional) In Time Config, you can enable Daylight Saving Time and choose a mode based on needs. Configure parameters. Click Apply.



Daylight Saving Time: ●

Mode: ● Predefined Mode ○ Recurring Mode

Predefined Profile: USA

Start Time: March, 2nd, Sunday 02:00

End Time: November, 1st, Sunday 02:00

Predefined Mode	If you select Predefined Mode, choose a predefined DST schedule for the OLT. USA: Select the Daylight Saving Time of the USA. It is from 2: 00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November. Australia: Select the Daylight Saving Time of Australia. It is from 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April. Europe: Select the Daylight Saving Time of Europe. It is from 1: 00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October. New Zealand: Select the Daylight Saving Time of New Zealand. It is from 2: 00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.
Recurring Mode	If you select Recurring Mode, specify a cycle time range for the Daylight Saving Time of the OLT. This configuration will be used every year. Offset: Specify the time to set the clock forward by. Start Time: Specify the start time of Daylight Saving Time. The interval between start time and end time should be more than 1 day and less than 1 year (365 days). End Time: Specify the end time of Daylight Saving Time. The interval between start time and end time should be more than 1 day and less than 1 year (365 days).

10. 2 Manage Users

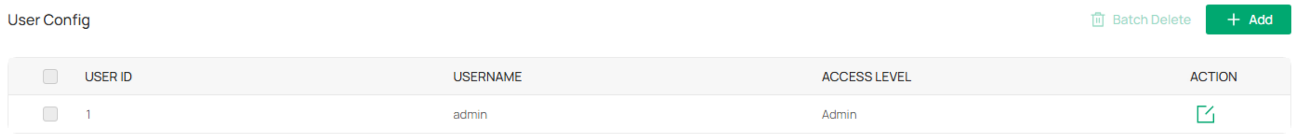
Overview

You can manage the user accounts for login to the OLT. There are four types of users: User, Power User, Opeator, and Admin, and they have different access levels, and you can create different user accounts according to your needs.

There is a default Admin account which cannot be deleted. The default username and password of this account are both admin. The other created accounts can be edited and deleted based on needs.

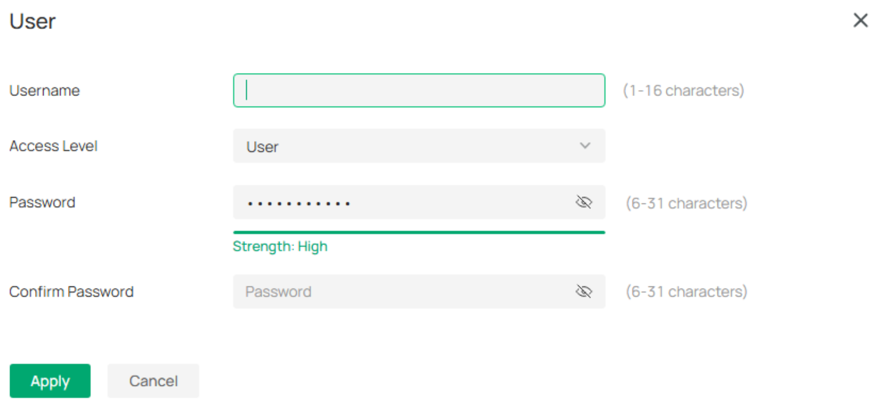
Configuration

1. Go to System > User Management to load the following page. Click +Add on the upper right and configure the parameters. Click Create.



User Config

□	USER ID	USERNAME	ACCESS LEVEL	ACTION
□	1	admin	Admin	☑



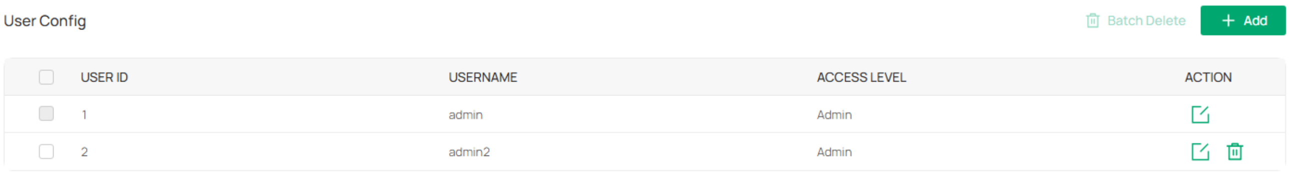
User

Username		(1-16 characters)
Access Level	User	
Password	••••••••••• Strength: High	(6-31 characters)
Confirm Password	Password	(6-31 characters)

Username	Specify a username for the account. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.
Access Level	Select the access level. There are four options provided: **Admin**: Admin can edit, modify and view all the settings of different functions. **Operator**: Operator can edit, modify and view most of the settings of different functions. **Power User**: Power User can edit, modify and view some of the settings of different functions. **User**: User can only view the settings without the right to edit or modify.

Password	Specify a password for the account. It contains 6–31 alphanumeric characters (case-sensitive) and symbols. No spaces are allowed.
Confirm Password	Renter the password.

2. View the existing accounts in the table. Click ☑ to edit the access level and password of the accounts, and click 🗑 to delete the account.



□	USER ID	USERNAME	ACCESS LEVEL	ACTION
□	1	admin	Admin	☑
□	2	admin2	Admin	☑ 🗑

10. 3 Use System Tools

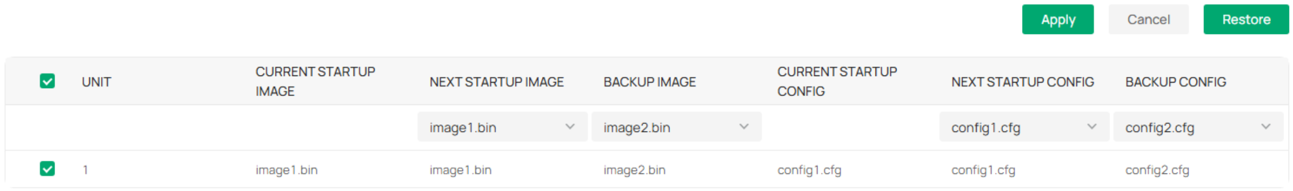
Overview

You can configure the boot file of the OLT, backup and restore the configurations, update the firmware, reset the OLT, and reboot the OLT.

10. 3. 1 Boot Config

Configuration

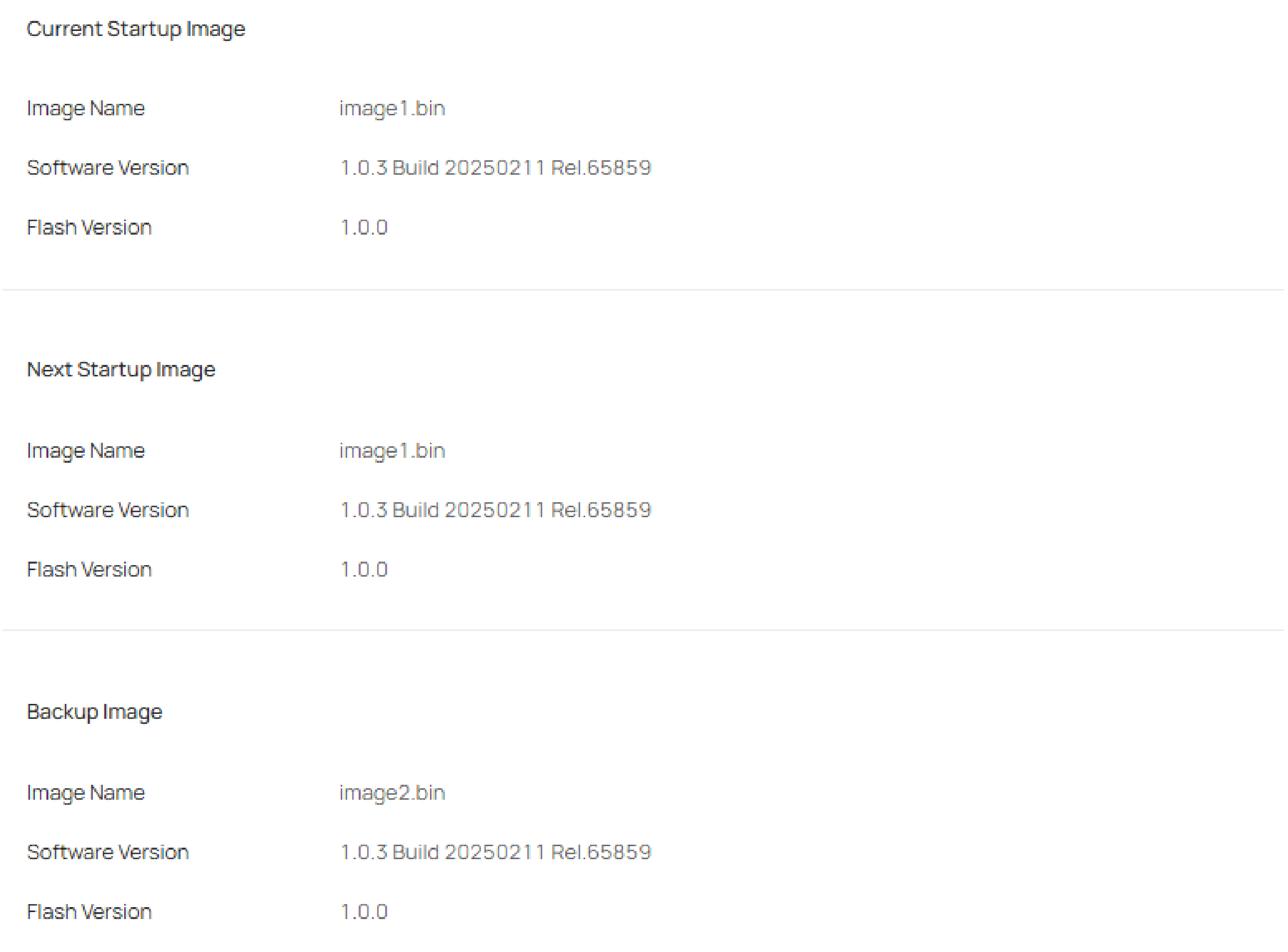
1. Go to System > System Tools > Boot Config to load the following page. Select one or multiple units to configure the parameters. Click Apply.



☑	UNIT	CURRENT STARTUP IMAGE	NEXT STARTUP IMAGE	BACKUP IMAGE	CURRENT STARTUP CONFIG	NEXT STARTUP CONFIG	BACKUP CONFIG
			image1.bin	image2.bin		config1.cfg	config2.cfg
☑	1	image1.bin	image1.bin	image2.bin	config1.cfg	config1.cfg	config2.cfg

Slot ID	Displays the number of the unit.
Current Startup Image	Displays the current startup image.
Next Startup Image	Select the next startup image. When the OLT is powered on, it will try to start up with the next startup image. The next startup image and backup image should not be the same.
Backup Image	Select the backup image. When the OLT fails to start up with the next startup image, it will try to start up with the backup image. The next startup and backup image should not be the same.
Current Startup Config	Displays the current startup configuration.
Next Startup Config	Specify the next startup configuration. When the OLT is powered on, it will try to start up with the next startup configuration. The next startup configuration and backup configuration should not be the same.
Backup Config	Specify the backup configuration. When the OLT fails to start up with the next startup configuration, it will try to start up with the backup configuration. The next startup and backup configuration should not be the same.

2. Go to System > System Tools > Boot Config > Image Table to view the information of the current startup image, next startup image and backup image



Current Startup Image

Image Name	image1.bin
Software Version	1.0.3 Build 20250211 Rel.65859
Flash Version	1.0.0

Next Startup Image

Image Name	image1.bin
Software Version	1.0.3 Build 20250211 Rel.65859
Flash Version	1.0.0

Backup Image

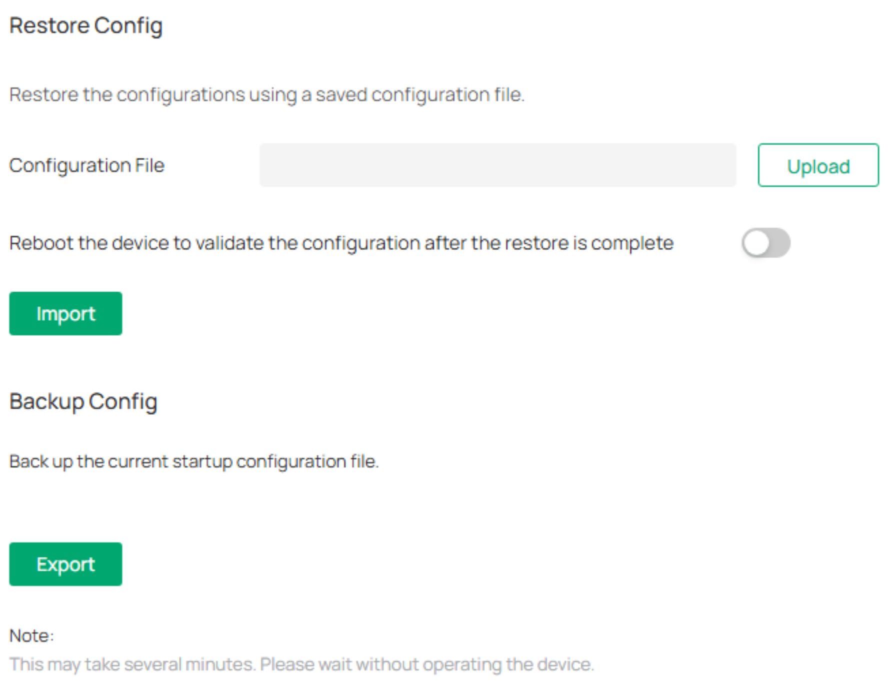
Image Name	image2.bin
Software Version	1.0.3 Build 20250211 Rel.65859
Flash Version	1.0.0

Image Name	Displays the name of the image.
Software Version	Displays the software version of the image.
Flash Version	Displays the flash version of the image.

10. 3. 2 Restore the Configurations of the OLT

Configuration

1. Go to System > System Tools > Restore & Backup > Restore Config to load the following page. Click Upload to choose a desired configuration to be restored.



Restore Config

Restore the configurations using a saved configuration file.

Configuration File

Reboot the device to validate the configuration after the restore is complete ○

Backup Config

Back up the current startup configuration file.

Note:
This may take several minutes. Please wait without operating the device.

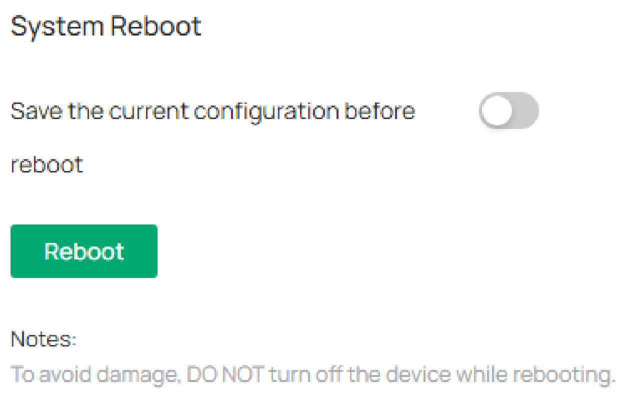
2. Choose whether to reboot the device after restoring is completed. The configurations will take effect after the OLT is rebooted.
3. Click Import to import the configuration file. The restoring process will take several minutes, please wait without any operation.
4. Click Export to save the current configuration file of the OLT.

10. 3. 3 Reboot the OLT

Configuration

- **Manual Reboot**

1. Go to System > System Tools > System Reboot to load the following page. In System Reboot, Choose whether to save the current configuration before reboot.



System Reboot

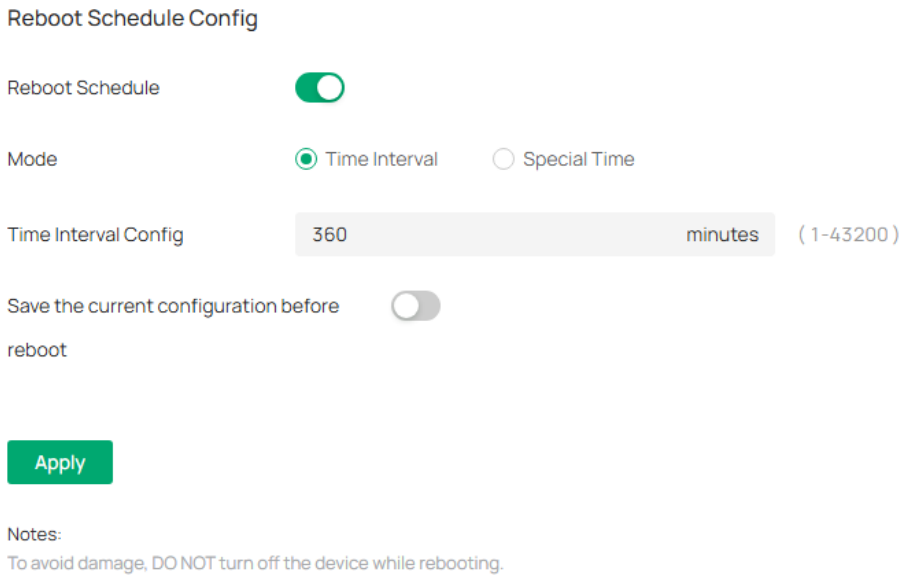
Save the current configuration before reboot ○

Notes:
To avoid damage, DO NOT turn off the device while rebooting.

2. Click Reboot.

- **Scheduled Reboot**

1. Go to System > System Tools > System Reboot to load the following page. In Reboot Schedule Config, Enable the Reboot Schedule, and choose a mode for the scheduled reboot.
2. Choose whether to save the current configuration before the reboot. Click Apply.



Reboot Schedule Config

Reboot Schedule: On

Mode: ● Time Interval ○ Special Time

Time Interval Config: 360 minutes (1-43200)

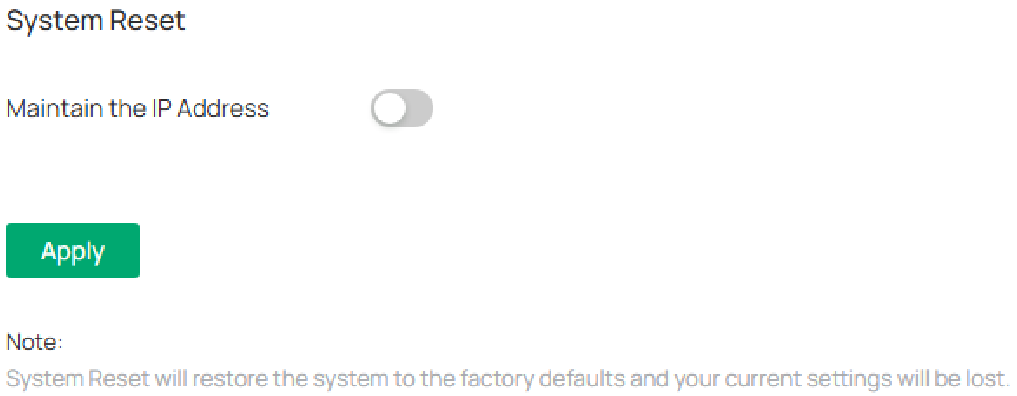
Save the current configuration before reboot: Off

Notes:
To avoid damage, DO NOT turn off the device while rebooting.

10. 3. 4 Reset the OLT

Configuration

1. Go to System > System Tools > System Reset to load the following page. Choose whether to maintain the IP address of the OLT after resetting all the configurations to factory default. Click Reset.



System Reset

Maintain the IP Address: Off

Note:
System Reset will restore the system to the factory defaults and your current settings will be lost.

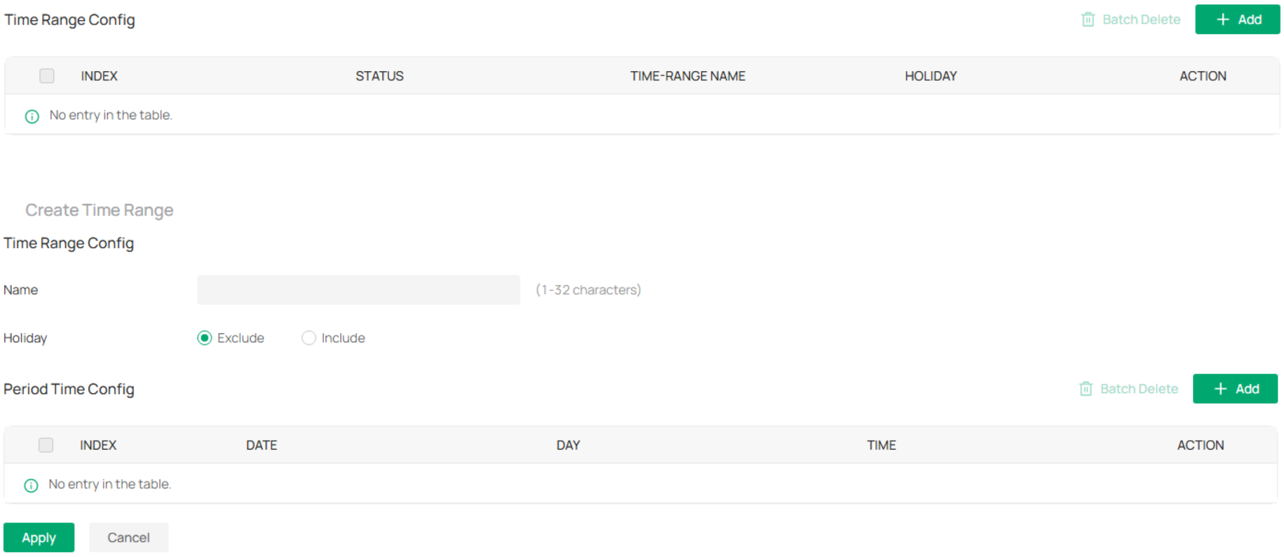
10. 4 Configure Time Range

Overview

Time Range allows you to customize time-related configurations. You can set different time range templates which can be applied to different configurations, saving you from repeatedly setting up the same information.

Configuration

1. Go to System > System Tools > Time Range > Time Range Config. Click +Add on the upper right to load the following page. Configure the parameters.



Time Range Config

□	INDEX	STATUS	TIME-RANGE NAME	HOLIDAY	ACTION
No entry in the table.					

Create Time Range

Time Range Config

Name (1-32 characters)

Holiday ● Exclude ○ Include

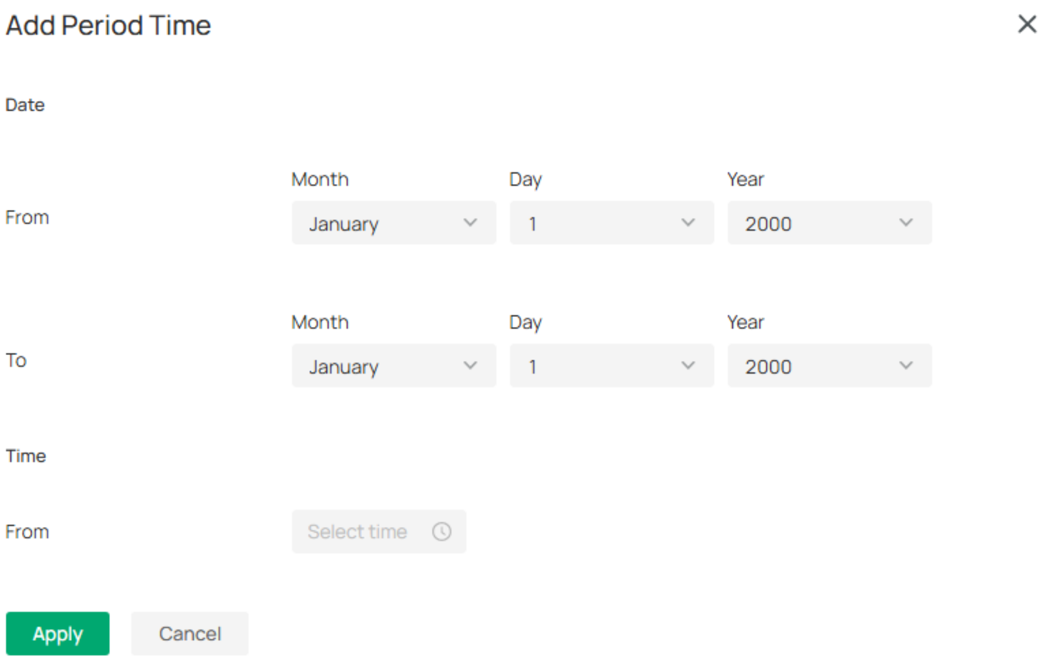
Period Time Config

□	INDEX	DATE	DAY	TIME	ACTION
No entry in the table.					

Name	Specify a name for the entry.
Holiday	Select to include or exclude the holiday in the time range. Exclude**:** The time range will not take effect on holiday. Include**:** The time range will not be affected by holiday. To configure Holiday, refer to Step 3 in this section.

2. In Period Time Config, click +Add on the upper right to load the following page. Configure the parameter. Click Create.

   You can add multiple entries of time period based on needs. The final time period is the sum of all the periods in the table.


Add Period Time

Date

From: Month January, Day 1, Year 2000

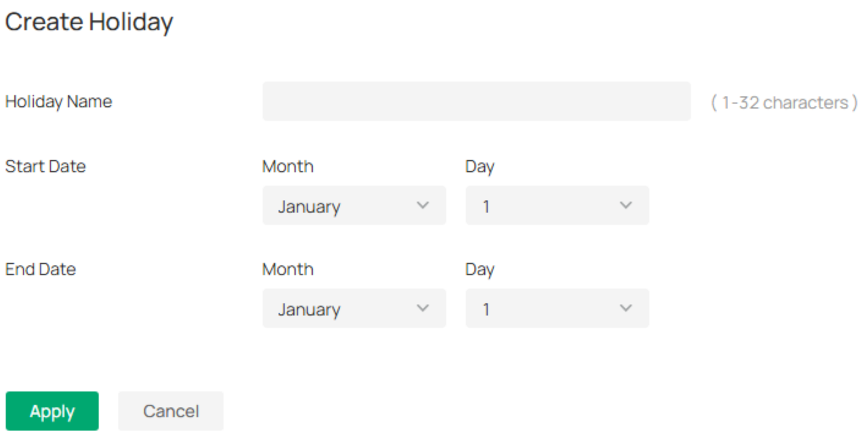
To: Month January, Day 1, Year 2000

Time

From: Select time

Date	Specify the start date and end date of this time range.
Time	Specify the start time and end time of a day.
Day of Week	Select days of a week as the period of this time range.

3. Go to System > System Tools > Time Range > Holiday Config. Click +Add on the upper right to load the following page. Configure the parameters. Click Create.


Create Holiday

Holiday Name: (1-32 characters)

Start Date: Month January, Day 1

End Date: Month January, Day 1

Holiday Name	Specify a name for the entry.
Start Date	Specify the start date of the holiday time range.
End Date	Specify the end date of the holiday time range.

10. 5 Configure DDM

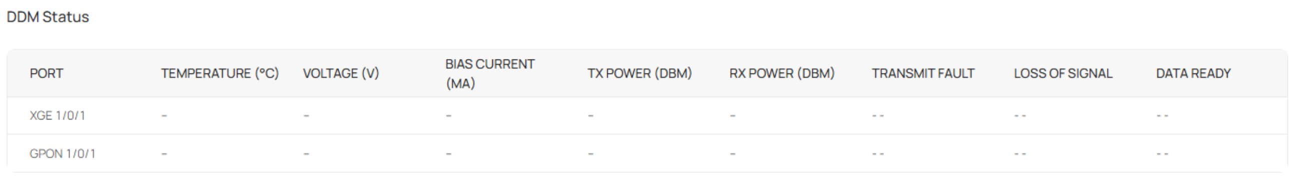
Overview

The DDM (Digital Diagnostic Monitoring) function is used to monitor the status of the SFP modules inserted into the SFP ports on the OLT. The user can choose to shut down the monitored SFP port automatically when the specified parameter exceeds the alarm threshold or warning threshold. The monitored parameters include: Temperature, Voltage, Bias Current, Tx Power and Rx Power.

Configuration

10. 5. 1 View the DDM Status

Go to System > DDM > DDM Status to load the following page. You can view the current operating parameters for the SFP modules inserted into the SFP ports.



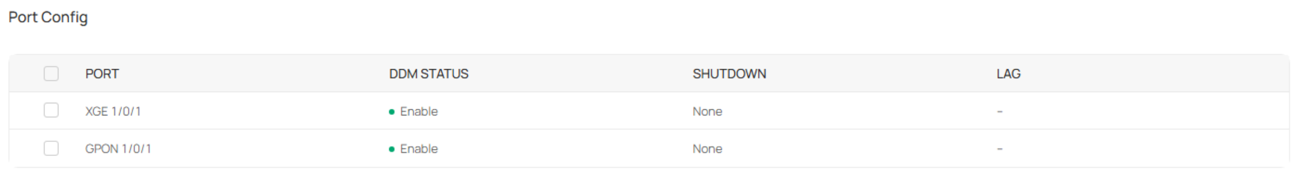
DDM Status

PORT	TEMPERATURE (°C)	VOLTAGE (V)	BIAS CURRENT (MA)	TX POWER (DBM)	RX POWER (DBM)	TRANSMIT FAULT	LOSS OF SIGNAL	DATA READY
XGE 1/0/1	-	-	-	-	-	--	--	--
GPON 1/0/1	-	-	-	-	-	--	--	--

Temperature	The current temperature of the SFP module inserted into this port.
Voltage	The current voltage of the SFP module inserted into this port.
Bias Current	The current bias current of the SFP module inserted into this port.
Tx Power	The current Tx power of the SFP module inserted into this port.
Rx Power	The current Rx power of the SFP module inserted into this port.
Transmit Fault	Reports remote SFP module signal loss. The values are True, False and No Signal.
Loss of Signal	Reports local SFP module signal loss. The values are True and False.
Data Ready	Indicates whether SFP module is operational. The values are True and False.

10. 5. 2 Configure the DDM

Go to System > DDM > DDM Config to load the following page. Select one or multiple ports to configure the parameters. Click Apply.



Port Config

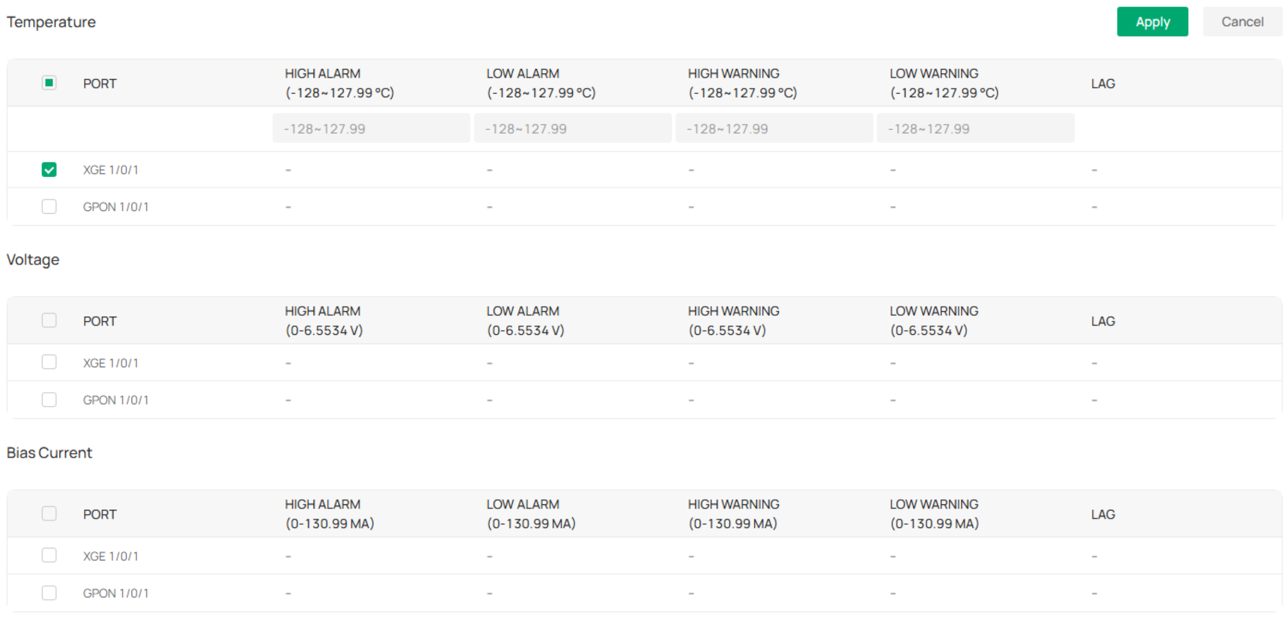
□	PORT	DDM STATUS	SHUTDOWN	LAG
□	XGE 1/0/1	● Enable	None	-
□	GPON 1/0/1	● Enable	None	-

DDM Status	Enable or disable DDM feature on the SFP port.
Shutdown	Specify whether to shut down the port when the alarm threshold or warning threshold is exceeded. Alarm: Shut down the port when the alarm threshold is exceeded. Warning: Shut down the port when the warning threshold is exceeded. None: The port will not be shut down even if the alarm threshold or warning threshold is exceeded. This is the default option.
LAG	Displays the LAG number which the port belongs to.

10. 5. 3 Configure the Thresholds

Go to System > DDM > Threshold Config to load the following page. Select one or multiple ports to configure the parameters for Temperature, Voltage, Bias Current, Tx Power and Rx Power. Click Apply.

For simplicity, here we will take Temperature as an example.



Temperature

Apply Cancel

■	PORT	HIGH ALARM (-128~127.99 °C)	LOW ALARM (-128~127.99 °C)	HIGH WARNING (-128~127.99 °C)	LOW WARNING (-128~127.99 °C)	LAG
		-128~127.99	-128~127.99	-128~127.99	-128~127.99	
☑	XGE 1/0/1	-	-	-	-	-
□	GPON 1/0/1	-	-	-	-	-

Voltage

□	PORT	HIGH ALARM (0-6.5534 V)	LOW ALARM (0-6.5534 V)	HIGH WARNING (0-6.5534 V)	LOW WARNING (0-6.5534 V)	LAG
□	XGE 1/0/1	-	-	-	-	-
□	GPON 1/0/1	-	-	-	-	-

Bias Current

□	PORT	HIGH ALARM (0-130.99 MA)	LOW ALARM (0-130.99 MA)	HIGH WARNING (0-130.99 MA)	LOW WARNING (0-130.99 MA)	LAG
□	XGE 1/0/1	-	-	-	-	-
□	GPON 1/0/1	-	-	-	-	-

High Alarm	Specify the high temperature threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm	Specify the low temperature threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning	Specify the high temperature threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.

Low Warning	Specify the low temperature threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.
LAG	Displays the LAG number which the port belongs to.