GPON OLT WEB USER MANUAL

Version V2.5
Release Date 2025-7-30

CONTENTS

Chapter 1 System Description

1.1 Overview

1.1.1 OLT Introduction

The Web management user manual is for the OLT listed in Table 1.1-1. After you have completed installation, connection and commissioning of the equipment, you can start on configuring various services and functions for the equipment.

Products		4 ports GPON OLT-B	4 ports GPON OLT-B1	8 ports GPON OLT-B	8 ports GPON OLT-B1
Chassis	Racks	1U 19 inch standard box	1U 19 inch standard box	1U 19 inch standard box	1U 19 inch standard box
1G/10G Uplink Port	QTY	4	2	8	4
	Copper	2*10/100/1000M auto-negotiation	N/A	4*10/100/1000M auto-negotiation	N/A
	SFP(Indep-endent)	2*SFP+ (SFP+ is compatible with 10GE)	2*SFP+ (SFP+ is compatible with 10GE)	2*SFP and 2*SFP+ (SFP+ is compatible with 10GE)	2*SFP and 2*SFP+ (SFP+ is compatible with 10GE)
GPON Port	QTY	4	4	8	8
	Physical Interface	SFP Slots	SFP Slots	SFP Slots	SFP Slots
Management Ports		1*10/100BASE-T out-band port(AUX), 1*CONSOLE port			
Management Mode		SNMP, WEB, Telnet and CLI			

Products		16 ports GPON OLT -B	8 ports GPON OLT -WEO
Chassis	Racks	1U 19 inch standard box	Outdoor non-standard box
1G/10G Uplink Port	QTY	8	6
	Copper	4*10/100/1000M auto-negotiation	1*10/100/1000M auto-negotiation
	SFP(Indep-endent)	4*SFP+ (SFP+ is compatible with 10GE)	2*SFP and 2*SFP+ (SFP+ is compatible with 10GE)

GPON Port	QTY	16	8
	Physical Interface	SFP Slots	SFP Slots
Management Ports		1*10/100BASE-T out-band port(AUX), 1*CONSOLE port	
Management Mode		SNMP, WEB, Telnet and CLI	

Table 1.1-1 GPON Series OLT Interfaces

1.1.2 OS Requirement

For OLT management, it supports or requires the following operation system.

CPU	Memory	DISK	Video Card	Operating System
Frequency above 2GHz	2GB Or above	10GB disk space	65000 color resolving capability 1024*768 and above	Windows 10 Windows 11

Table 1.1-2 Operation System Requirement

1.2 Connection

Connect the OLT AUX port to IP network. The OLT default management IP is 192.168.8.200.
Please set your PC IP to 192.168.8.X (e.g.192.168.8.123).

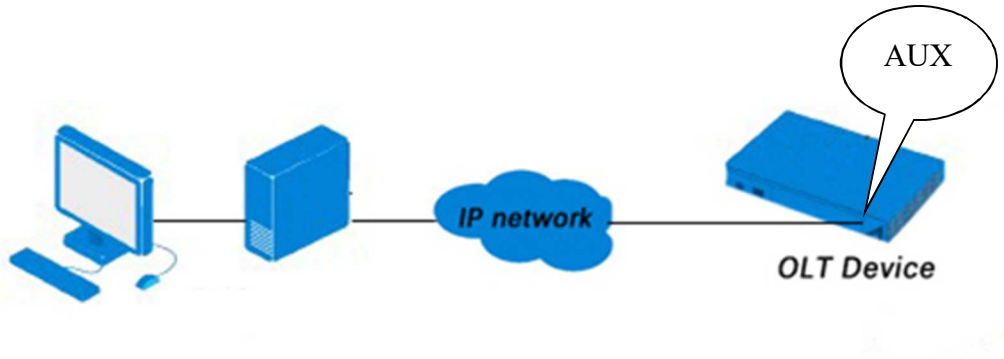


Figure 1.2-1 Access the OLT Web

Chapter 2 OLT Information

2.1 Login

Follow the steps to login:
1. Conform “1.2 Connection” to connect;
2. The device default IP address is 192.168.8.200;
3. Open your web browser, type the device IP in address bar;
4. Entry of the username and password will be prompted. Enter the default login User Name and Password. The default username and password is "**admin/Xpon@Olt9417#**".

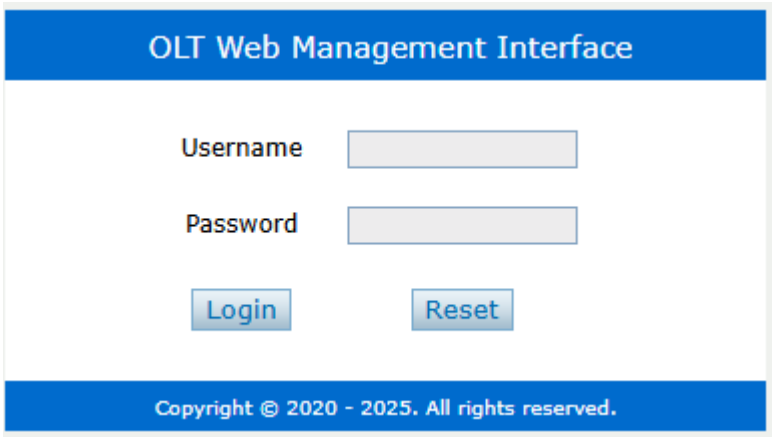


Figure 2.1-1: Login

2.2 Device Information

The OLT ports connection status are shown in the top of the interface, and about the OLT basic information.

OLT Information→Device Information

This part shows the OLT information such as system name, serial number, hardware version, firmware version, MAC address and system time. The system name can be modified if need.

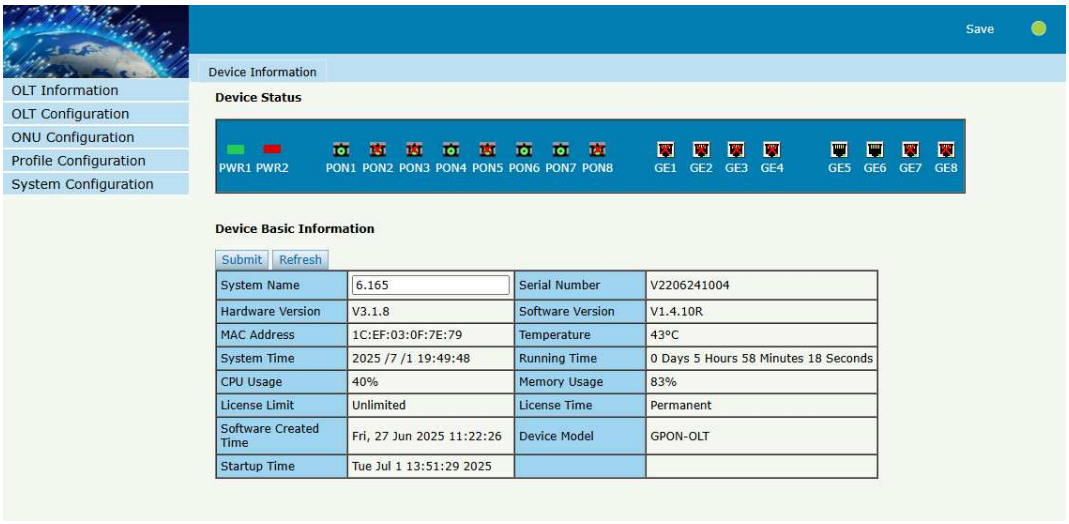


Figure 2.2-1: Device Information

On the upper-right corner of the device information interface, there are quick-access buttons for certain functions. By clicking the "Save" button, you can store the current running configuration of the device. If the configuration is not saved, it will be lost in the event of a device reboot.

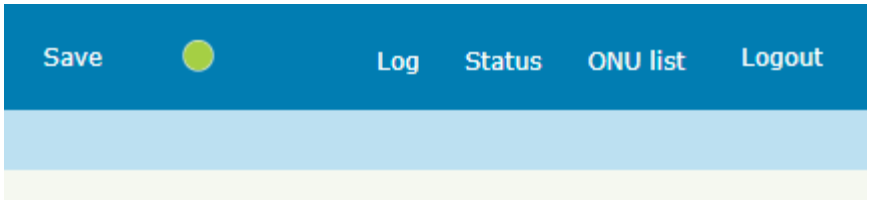


Figure 2.2-2: Quick-Access Button

Chapter 3 OLT Configuration

This section is about the basic service of OLT configuration.

3.1 VLAN

OLT equipment is fully compliant with the IEEE802.1Q VLAN standard and has the following main features:

- Support Port-based VLAN and IEEE802.1Q VLAN.
- Support full 4K VLAN group, VID range 1~4094.

All uplink ports support VLAN division.
VLAN 1 is their default VLAN. So it works in Untag mode by default.

3.1.1 VLAN Management

OLT Configuration→VLAN
In this user interface, you can create/delete new VLAN.

Figure 3.1-1: Create New VLAN

3.1.2 VLAN Port

OLT Configuration→VLAN→VLAN Port
You can assign ports to the created VLAN and configure different processing methods.

Only when a VLAN is assigned will the port forward the packet carrying this VLAN Tag.

Forbidden: After forbidding VLAN, this port will not forward packets carrying this VLAN Tag.

Tag: If the VLAN carried by the packet matches the port VLAN, it can be forwarded from that port while maintaining the original VLAN Tag.

Untag: If the VLAN carried by the packet matches the port VLAN, the packet will have its VLAN Tag stripped and then be forwarded from that port.

The uplink port can be configured with three working modes: Access, Hybrid, and Trunk.

Access: In this mode, the port can only be assigned one VLAN and can only operate in Untag mode. It is usually used to connect terminal devices such as PC and printer, ensuring that these devices are directly connected to the designated VLAN.

Hybrid: In this mode, the port can configure multiple VLAN as Tag mode or Untag mode.

Trunk: In this mode, the port can configure multiple VLAN as Tag mode, but only one VLAN can be configured as Untag mode.

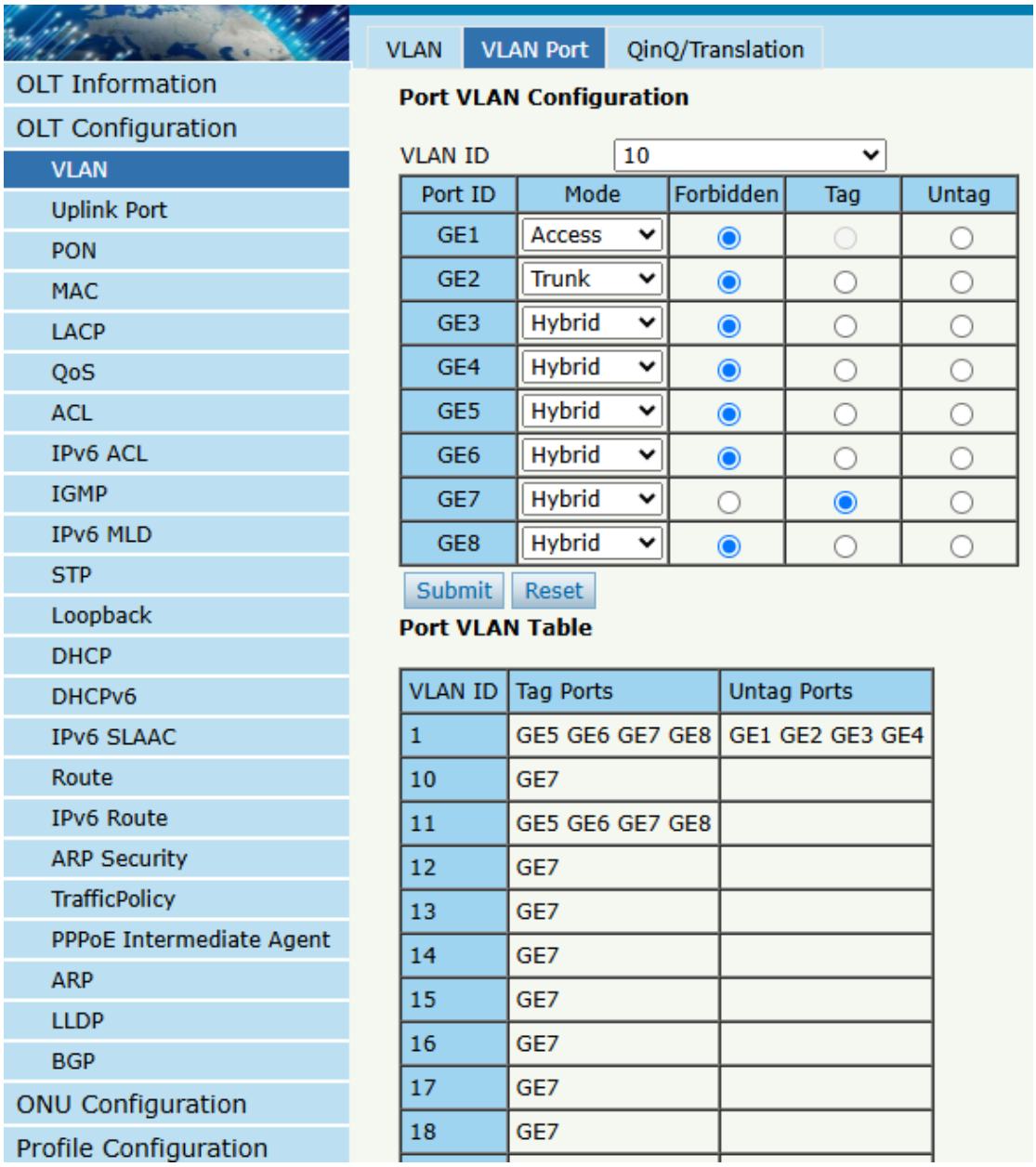


Figure 3.1-2: Add VLAN Port

3.1.3 QinQ/Translation

OLT Configuration→VLAN→QinQ/Translation
In this user interface, VLAN QinQ and VLAN translation can be configured. VLAN QinQ and translation are effective for ingress.

QinQ (formally known as 802.1Q-in-802.1Q, or alternatively referred to as VLAN Stacking or Double VLAN) is a technology that enhances network virtualization capabilities through the superposition of two layers of VLAN tags. It is primarily utilized to address the limitation of VLAN ID insufficiency in large-scale network deployments.

Customer VLAN: It is the inner VLAN tag.

Service VLAN: It is the outer VLAN tag. In QinQ mode, the port will add the Service VLAN tag to the outer layer of the received packet VLAN tag that matches the Customer VLAN. In the VLAN translation mode, the port will translate the VLAN tags of the packets that match the Customer VLAN into the Service VLAN.

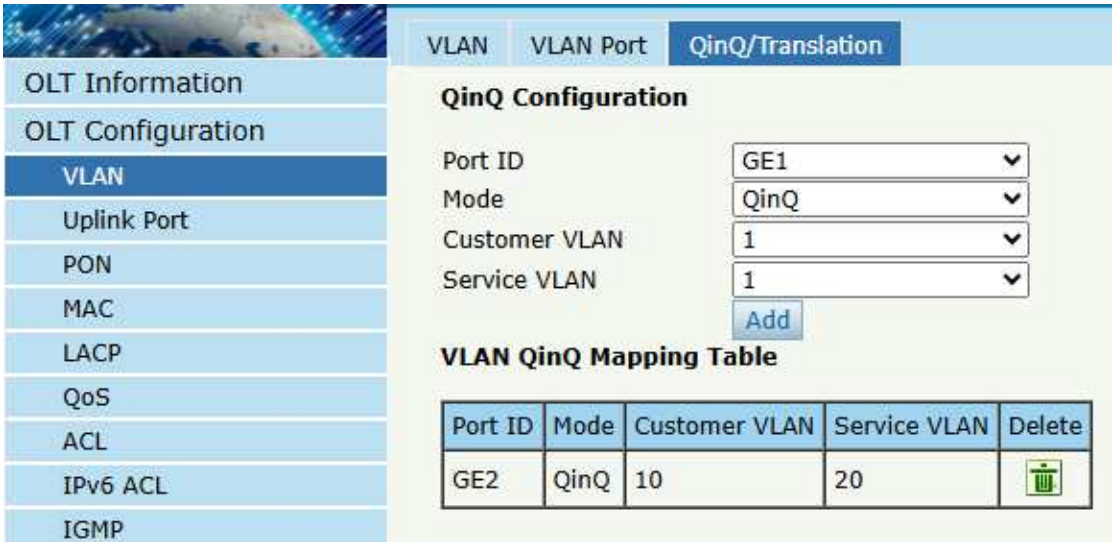


Figure 3.1-3: QinQ/Translation Configuration

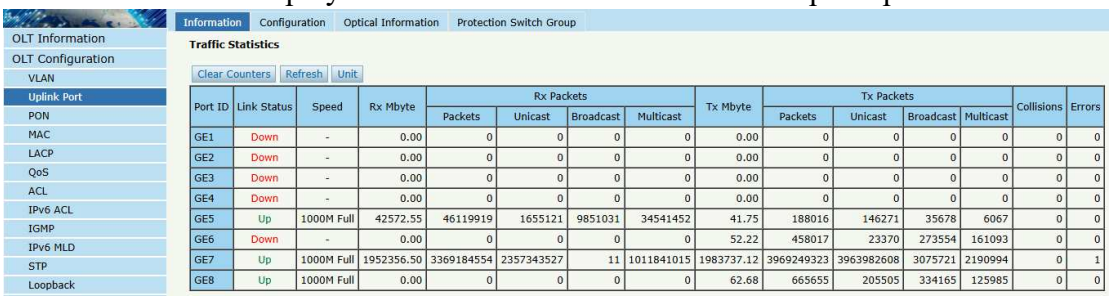
3.2 Uplink Port

GE ports traffic statistics and basic configuration setting.

3.2.1 Information

OLT Configuration→Uplink Port→Information

This user interface displays traffic statistics and link status of uplink ports.



Port ID	Link Status	Speed	Rx Mbyte	Rx Packets				Tx Mbyte	Tx Packets				Collisions	Errors
				Packets	Unicast	Broadcast	Multicast		Packets	Unicast	Broadcast	Multicast		
GE1	Down	-	0.00	0	0	0	0	0.00	0	0	0	0	0	0
GE2	Down	-	0.00	0	0	0	0	0.00	0	0	0	0	0	0
GE3	Down	-	0.00	0	0	0	0	0.00	0	0	0	0	0	0
GE4	Down	-	0.00	0	0	0	0	0.00	0	0	0	0	0	0
GE5	Up	1000M Full	42572.55	46119919	1655121	9851031	34541452	41.75	188016	146271	35678	6067	0	0
GE6	Down	-	0.00	0	0	0	0	52.22	458017	23370	273554	161093	0	0
GE7	Up	1000M Full	1952356.50	3369184554	2357343527	11	1011841015	1983737.12	3969249323	3963982608	3075721	2190994	0	1
GE8	Up	1000M Full	0.00	0	0	0	0	62.68	665655	205505	334165	125985	0	0

Figure 3.2-1: GE Traffic Statistics

3.2.2 Configuration

OLT Configuration→Uplink Port→Information

This user interface is used to configure port related functions and characteristic parameters of uplink port, such as port attributes, PVID, flow control, rate limit, storm inhibition, port isolation and so on.

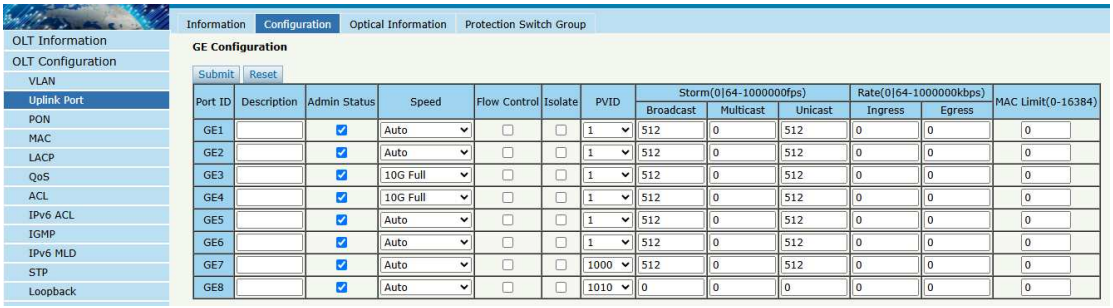


Figure 3.2-2: Uplink Ports Configuration

Illustrations of each parameter:

Parameters	Illustration
Port ID	GE port has two types, fiber SFP (GE1 to GE4) and copper (GE5 to GE8).
Description	Descriptions or remarks of port.
Admin Status	Active or inactive status of port. It is Enabled by default.
Speed	Configuring Port Rate.
Flow Control	Enable or disable flow control function of uplink port to control congestion. If this function is to be used, it is required that the peer device also support flow control. It is disabled by default.
Isolate	If isolation is enabled on the ports, packet cannot be forwarded between them.
PVID	Default VLAN ID of the port. The port will add PVID tags to the received packets that do not carry VLAN tag. PVID defaults to 1.
Broadcast	Broadcast storm inhibition.
Multicast	Multicast storm inhibition.
Unknown Unicast	Unknown unicast storm inhibition.
Ingress Rate	Limit the traffic rate in the direction of ingress. 0 represents no limit.
Egress Rate	Limit the traffic rate in the direction of egress. 0 represents no limit.

MAC limit	Number of MAC address can be learn in the port.

Table 3.2-1 Uplink Port Parameter

3.2.3 Optical Information

OLT Configuration→Uplink Port→Optical Information

This page is used to view the optical information of the uplink interface, including Temperature(Degree)/Voltage(V)/Bias Current(mA)/Transmit Power(dBm)/Received Power(dBm)/Vendor Name/Wavelength(nm)/Vendor SN.

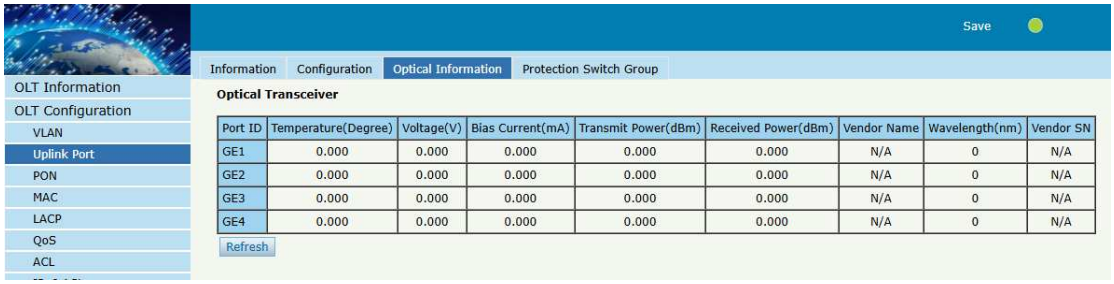


Figure3.2-3: Optical Information

3.2.4 Protection Switch Group

OLT Configuration→Uplink Port→Protection Switch Group

The Protection Switch Group is used for backup function between the two selected uplink ports. When the master port abnormally goes down, it can be switched to the standby port to continue working.

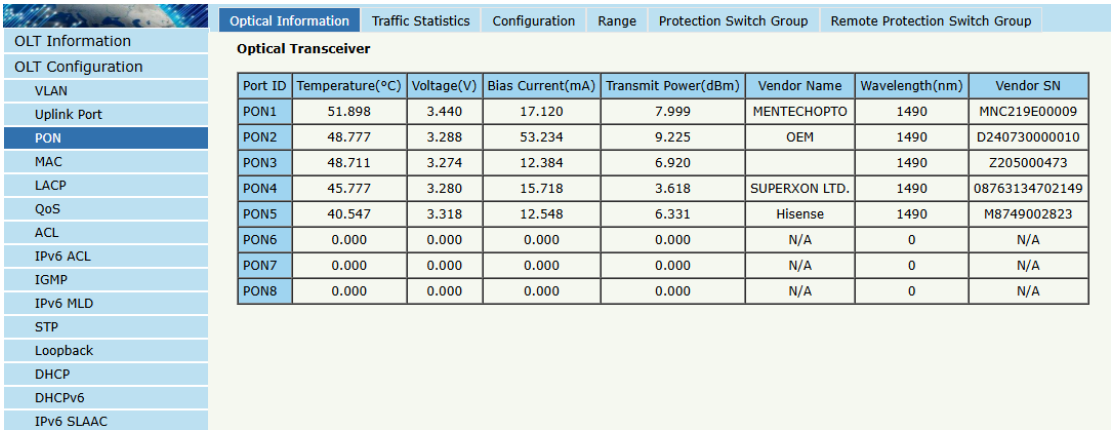
Figure3.2-4: Protection Switch Group

3.3 PON

3.3.1 Optical Information

OLT Configuration→PON→Optical Information

This user interface is used to displays parameters of PON port, such as PON module port current temperature, Voltage, current, transmit power.



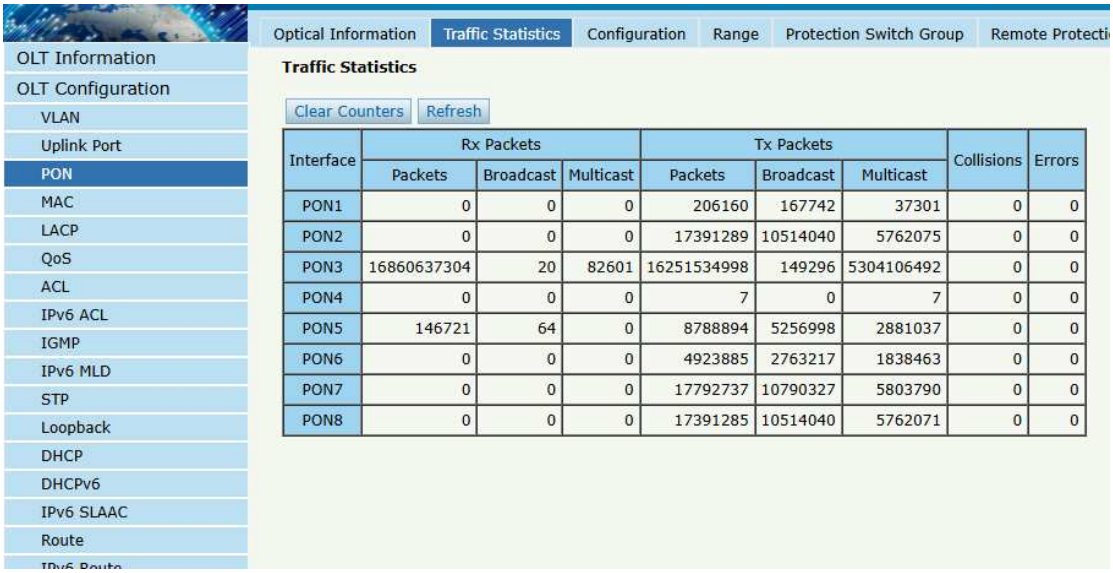
Port ID	Temperature(°C)	Voltage(V)	Bias Current(mA)	Transmit Power(dBm)	Vendor Name	Wavelength(nm)	Vendor SN
PON1	51.898	3.440	17.120	7.999	MENTECHOPTO	1490	MNC219E00009
PON2	48.777	3.288	53.234	9.225	OEM	1490	D240730000010
PON3	48.711	3.274	12.384	6.920		1490	Z205000473
PON4	45.777	3.280	15.718	3.618	SUPERXON LTD.	1490	08763134702149
PON5	40.547	3.318	12.548	6.331	Hisense	1490	M8749002823
PON6	0.000	0.000	0.000	0.000	N/A	0	N/A
PON7	0.000	0.000	0.000	0.000	N/A	0	N/A
PON8	0.000	0.000	0.000	0.000	N/A	0	N/A

Figure 3.3-1: PON Information

3.3.2 Traffic Statistics

OLT Configuration→PON→Traffic Statistics

This user interface displays traffic statistics of PON ports.



Interface	Rx Packets			Tx Packets			Collisions	Errors
	Packets	Broadcast	Multicast	Packets	Broadcast	Multicast		
PON1	0	0	0	206160	167742	37301	0	0
PON2	0	0	0	17391289	10514040	5762075	0	0
PON3	16860637304	20	82601	16251534998	149296	5304106492	0	0
PON4	0	0	0	7	0	7	0	0
PON5	146721	64	0	8788894	5256998	2881037	0	0
PON6	0	0	0	4923885	2763217	1838463	0	0
PON7	0	0	0	17792737	10790327	5803790	0	0
PON8	0	0	0	17391285	10514040	5762071	0	0

Figure 3.3-2: PON Traffic Statistics

3.3.3 Configuration

OLT Configuration→PON→Configuration

This user interface is used to configure port status and other basic parameters,such as storm inhibition, rate limit, port isolation, P2P and so on .

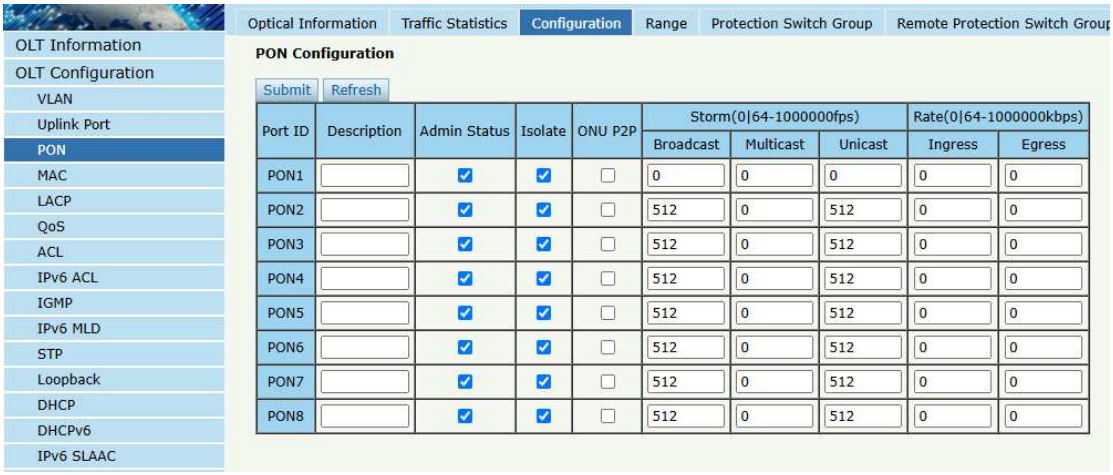


Figure 3.3-3: PON configuration

Illustrations of each parameter:

Parameters	Illustration
Description	Descriptions or remarks of port.
Admin Status	Active or inactive status of port. It is Enabled by default.
Isolate	If isolation is enabled on the ports, packet cannot be forwarded between them. All ports are enabled to be isolated by default.
ONU P2P	After enabling ONU P2P, ONU registered under the same PON port can communicate with each other. The ONU P2P of the PON port is enabled by default.
Broadcast	Broadcast storm inhibition.
Multicast	Multicast storm inhibition.
Unknown Unicast	Unknown unicast storm inhibition.
Ingress Rate	Limit the traffic rate in the direction of ingress. 0 represents no limit.
Egress Rate	Limit the traffic rate in the direction of egress. 0 represents no limit.

Table 3.3-1 PON Port Parameter

3.3.4 Range

OLT Configuration→PON→Range

When ONU is more than 20km away from OLT, you need to configure PON distance range. Onus outside the distance range will not be able to register. The difference between minimum and maximum should not be more than 20km. The unit is 100m.

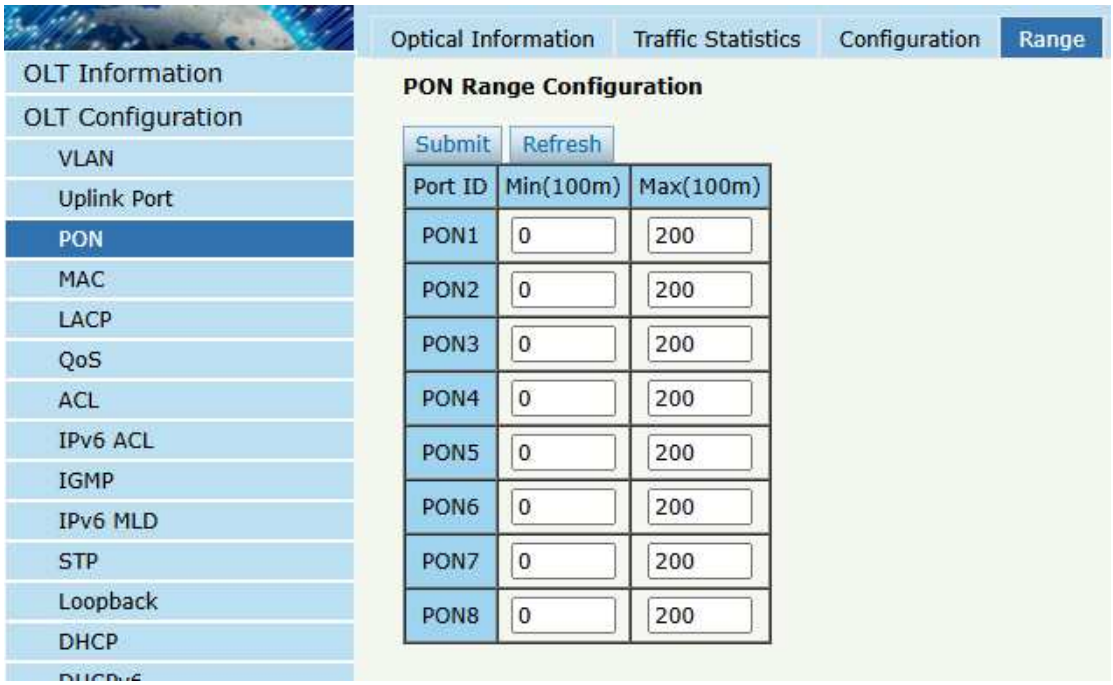


Figure 3.3-4: PON Range Configuration

3.3.5 Protection Switch Group

OLT Configuration→PON→Protection Switch Group

This user interface is used to configure PSG parameters base on Type B. You can configure a Work PON and a Standby PON and connect them to a 2: N optical splitter. When the ONU is registered on the Work PON, the registration information and PON configuration is synchronized to the Standby PON. If the Work PON link is faulty, the ONU automatically registers with another PON.

Note: The ONU list of the two target PON ports must be empty in order to successfully configure PSG.

Illustrations of partial parameter:

Parameters	Illustration
Active PON	The Active PON is a PON port that can be used to register ONU. After enabling PSG, the Work PON is also the Active PON , and ONU can be registered. If the Work PON link is faulty, the Standby PON will serve as the new Active PON .

Change Active PON	You can manually switch the active PON port.
Lock Mode	After enabling the lock mode, even if there is a link faulty or manual switching occurs, the Active PON port cannot be switched.
Revertive	After enabling Revertive, if no ONU is online under the Active PON , the other PON port will become a new Active PON .
Revertive Time	If there is still no ONU online after waiting for one cycle at the current Active PON port, the other PON port will become the new Active PON.

Table 3.3-2 PSG Parameter

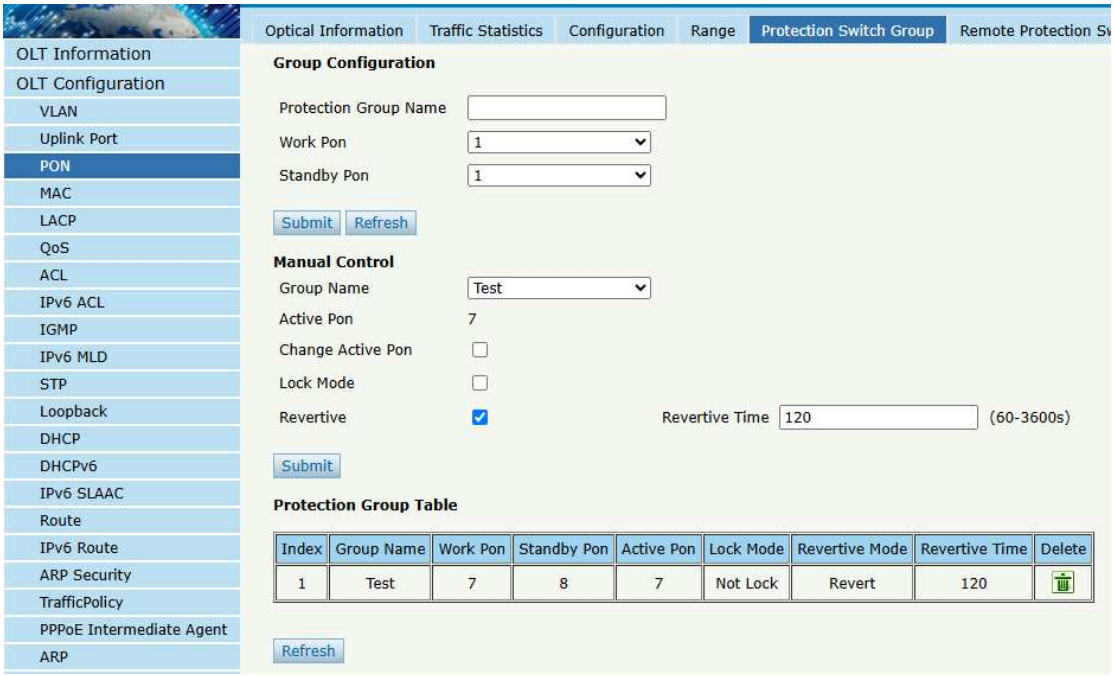


Figure 3.3-5: PON Protection Switch Group Configuration

3.3.6 Remote Protection Switch Group

OLT Configuration→PON→Remote Protection Switch Group

This user interface is used to configure PSG parameters based on Type B or Type C. You can configure local PON and remote PON on different devices and connect them to a 2: N splitter. When the ONU registers on the local PON, the registration information and PON configuration are synchronized to remote PON. If the working PON link fails, the ONU will automatically register with the backup PON of another device.

Notice:

1.Please ensure that the remote PON protection function is used in a stable network

environment.
2.When first creating PON protection groups, ensure no existing OLT profiles. Master/slave OLT must clear PON configurations. Follow correct sequence for configuration consistency!
3.Type-C protection groups not support manual control!
4.If the group is in disconnected state, it is recommended not to set configurations, as this may cause master-backup configuration desynchronization or configuration set failure.

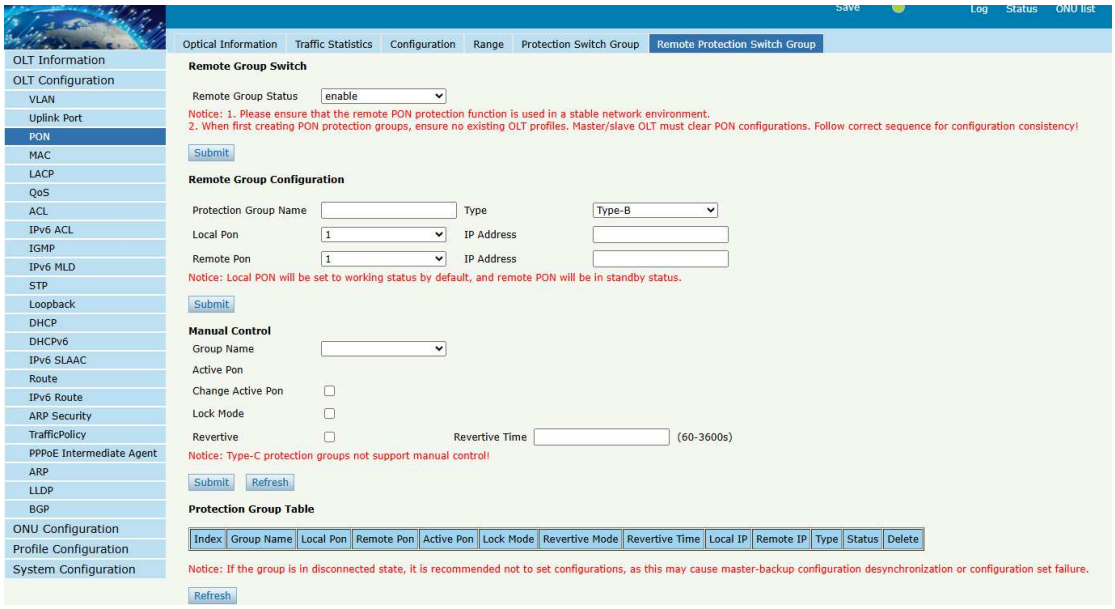


Figure 3.3-6: PON Remote Protection Switch Group Configuration

3.4 MAC

In this section, you can check MAC address table of OLT, set MAC aging time and add MAC address manually.

3.4.1 MAC Table

OLT Configuration→MAC→MAC Table
This table displays MAC addresses that OLT has learn at PON ports and GE ports.

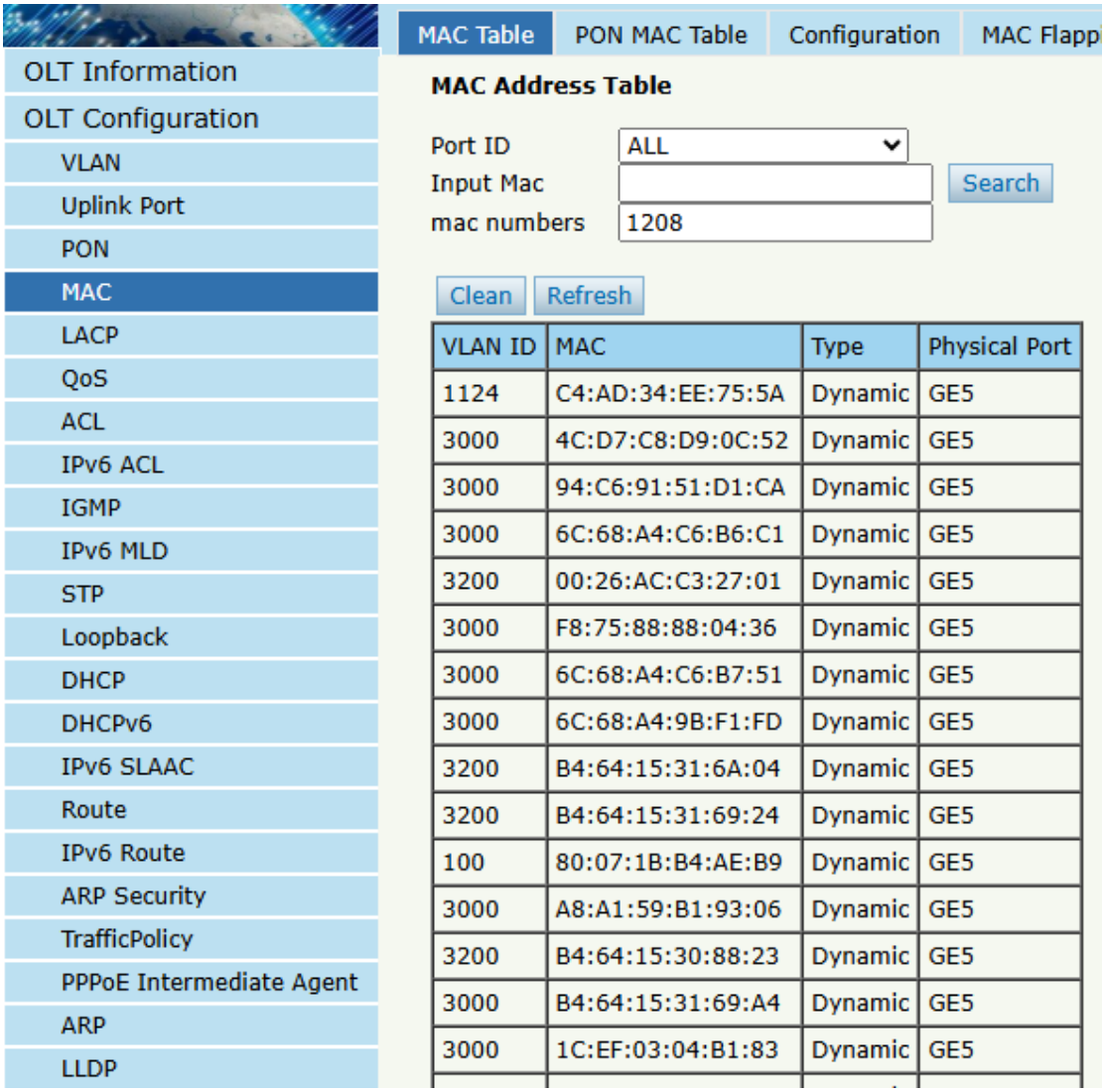


Figure 3.4-1: MAC Address Table

3.4.2 PON MAC Table

OLT Configuration→MAC→PON MAC Table

This table displays MAC addresses that OLT has learn at PON ports.

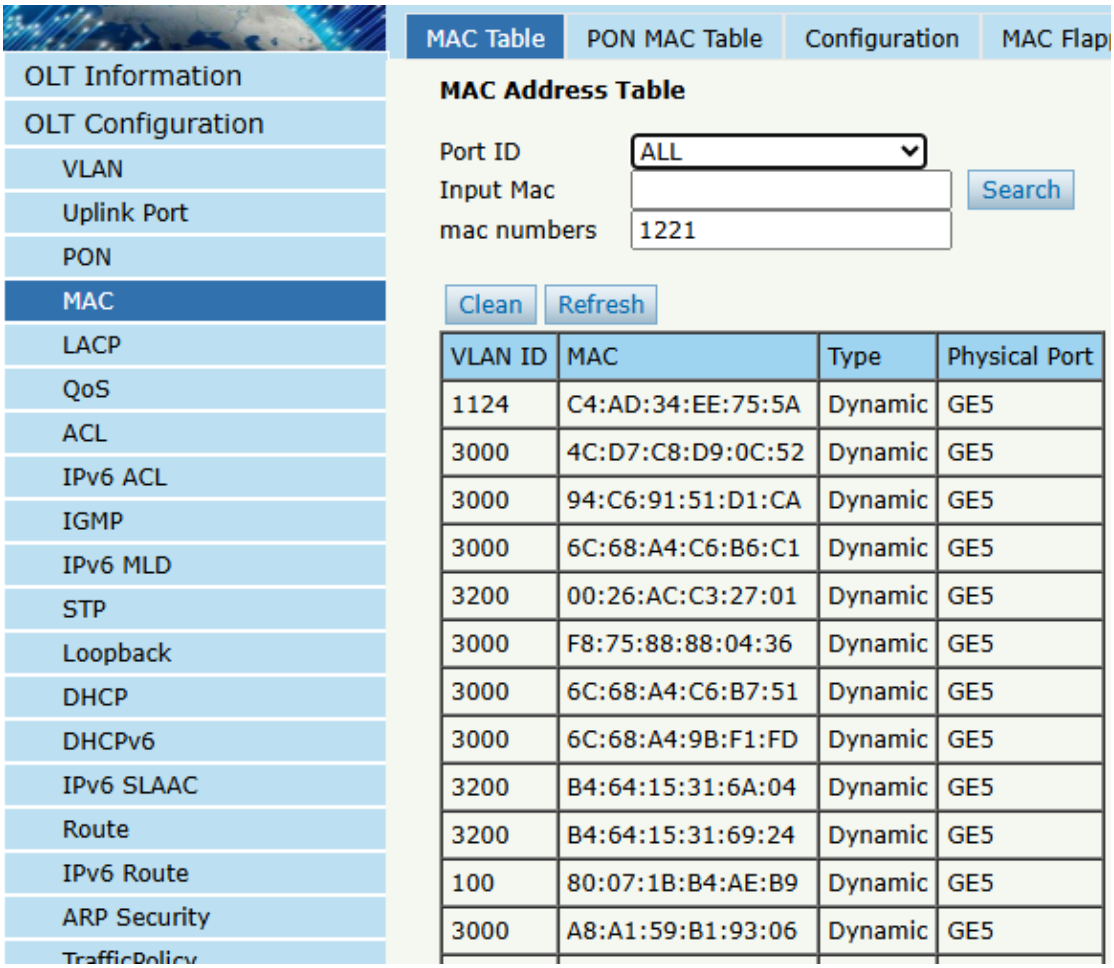


Figure 3.4-2: PON MAC Table

3.4.3 Configuration

OLT Configuration→MAC→Configuration

The default MAC aging time of OLT is 300s, user can change the value between 10~1000000s. Also, user can add MAC address to the OLT manually. Static MAC addresses do not age.

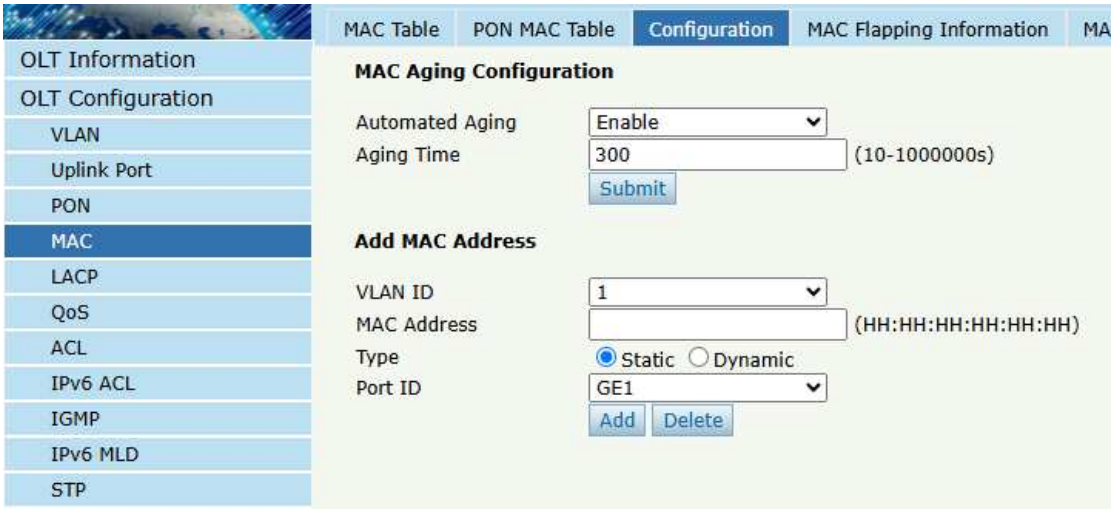


Figure 3.4-3: MAC Configuration

3.4.4 MAC Flapping Information

This interface displays information learned on multiple ports for the same MAC if you enable MAC Flapping switch. This means that there may be loops in your network environment.

MAC Address	VLAN	Source port	Current Port	Begin Time	Last Time	Times
80:07:1B:98:81:4D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:56	2021/07/23 13:26:28	2/0
80:07:1B:98:81:7D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 13:26:28	2/0
80:07:1B:98:81:35	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 13:26:28	2/0
80:07:1B:98:83:7D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 13:26:28	2/0
80:07:1B:98:80:D5	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 11:09:57	1/0
80:07:1B:98:81:15	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 13:26:29	2/0
80:07:1B:98:81:5D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 13:26:29	2/0
80:07:1B:98:82:7D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:57	2021/07/23 11:09:57	1/0
80:07:1B:98:83:0D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:58	2021/07/23 13:26:29	2/0
80:07:1B:98:83:25	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:58	2021/07/23 13:26:30	2/0
80:07:1B:98:81:95	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:58	2021/07/23 13:26:30	2/0
80:07:1B:98:80:E5	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:59	2021/07/23 13:26:30	2/0
80:07:1B:98:82:55	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:59	2021/07/23 13:26:30	2/0
80:07:1B:98:81:3D	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:59	2021/07/23 11:09:59	1/0
80:07:1B:98:81:25	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:59	2021/07/23 13:26:27	2/0
80:07:1B:98:80:FD	3000	GPON 0/1	GE 0/1	2021/07/23 11:09:59	2021/07/23 13:26:30	2/0
80:07:1B:98:82:5D	3000	GPON 0/1	GE 0/1	2021/07/23 11:10:00	2021/07/23 11:10:00	1/0
80:07:1B:98:81:B5	3000	GPON 0/1	GE 0/1	2021/07/23 13:26:27	2021/07/23 13:26:27	1/0
80:07:1B:98:81:05	3000	GPON 0/1	GE 0/1	2021/07/23 13:26:28	2021/07/23 13:26:28	1/0
80:07:1B:98:82:0D	3000	GPON 0/1	GE 0/1	2021/07/23 13:26:28	2021/07/23 13:26:28	1/0

Figure 3.4-4: MAC Flapping Information

3.4.5 MAC Flapping Configuration

You can enable MAC Flapping Configuration in this interface.
Illustrations of partial parameter:

Parameters	Illustration
Range	You can choose to enable MAC flapping detection on the uplink port or the PON port.
Mode	You can configure the processing actions of the interface after MAC Flapping occurs. **Only-alarm:** OLT only displays the MAC flapping alarm. **Auto-recovery:** After MAC Flapping occurs, OLT will generate an alarm and the port will be shutdown. It can be automatically restored after the MAC Flapping time ages. **Manual-recovery:** After MAC Flapping occurs, OLT will generate an alarm and the port will be shutdown. It can only be restored manually.
Interval	Configure the detection time interval of MAC Flapping. If the set number of MAC flapping attempts is reached within this period, the port will be shutdown.
Suppression Threshold	Set the number of MAC Flapping times within the period.
Suppression Age Time	Set the aging time of MAC Flapping.

Table 3.4-1 MAC Flapping Parameter

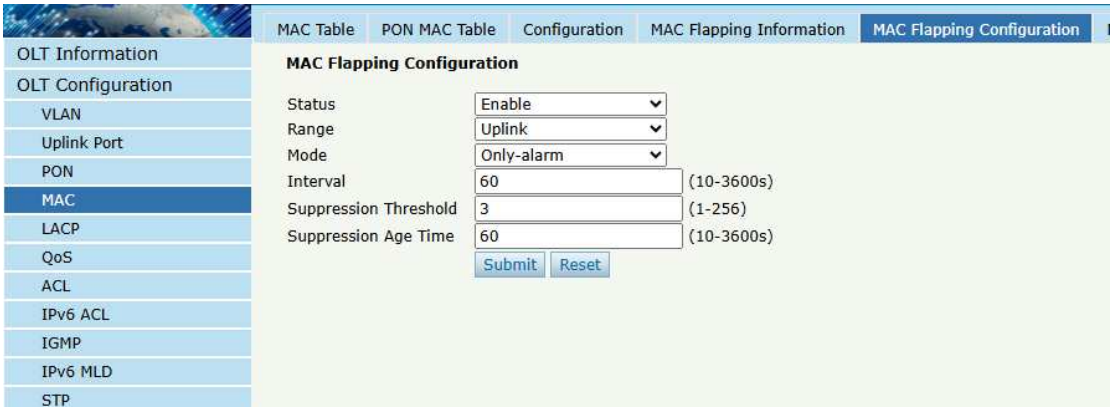


Figure 3.4-5: MAC Flapping Configuration

3.4.6 MAC Flapping Port Configuration

This user interface is used to enable MAC Flapping Configuration for specific port.

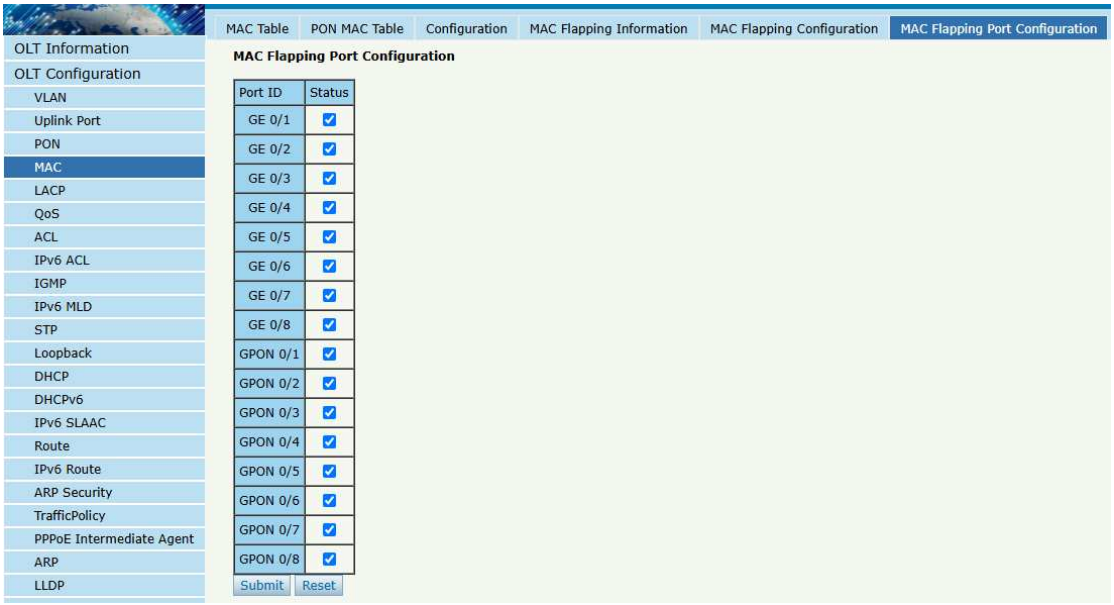


Figure 3.4-6: MAC Flapping Port Configuration

3.5 LACP

The Link Aggregation Control Protocol is a network protocol used for the dynamic management of Ethernet link aggregation. Its function is to bundle multiple physical network ports (such as switch ports) into a logical link to enhance bandwidth, redundancy and load balancing capabilities. For example, two 1Gbps ports are aggregated into a 2Gbps logical link.

3.5.1 Static LACP

OLT Configuration→LACP→Static LACP

To assign and configure an uplink physical interface to a channel group, select load balance for LACP function. When a traffic link can't be used suddenly, the traffic link will switch to another link automatically. The group range is from 1 to 4. Each group can add 4 ports maximally. Only GE ports can be added in the channel groups.

There are several load balancing strategies for users to select, including src-mac, dst-mac, src-ip, dst-ip, src-dst-mac, and src-dst-ip. The OLT calculates based on these strategies using hash algorithms and decides how to distribute data traffic across multiple links. For example, when using src-mac strategy, traffic with different source MAC addresses will be distributed to different links to prevent overloading on a

single link.

Static LACP actually aggregates different ports through manual configuration without protocol interaction, and it lacks dynamic negotiation capabilities.

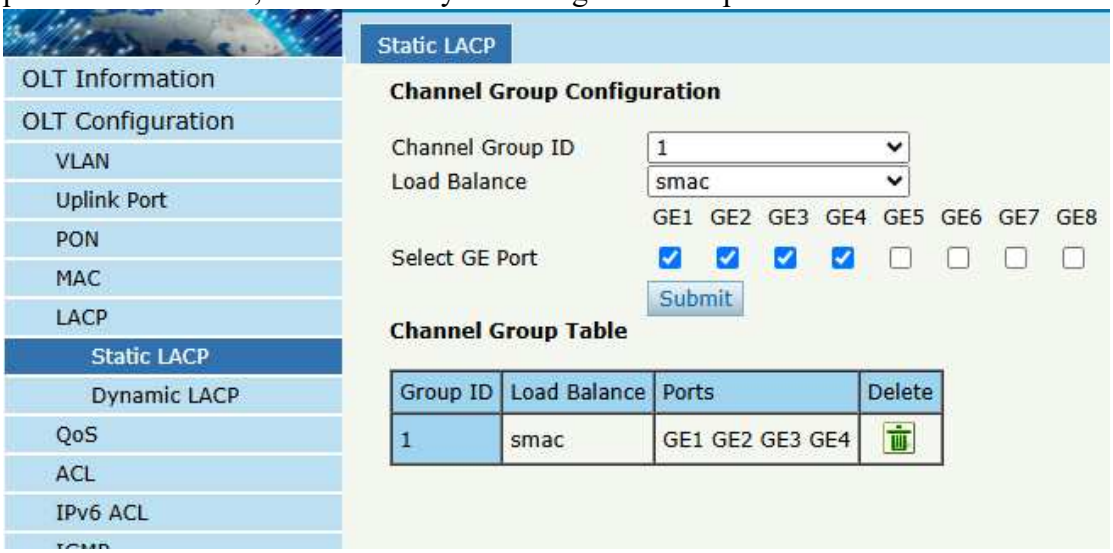


Figure 3.5-1: Create Static LACP

3.5.2 Dynamic LACP

Dynamic LACP automatically manages aggregation groups through protocol interaction, supports dynamic addition/removal of ports, and provides link status monitoring.

3.5.2.1 Information

OLT Configuration→LACP→Dynamic LACP→Information

This interface displays dynamic LACP information. Only the port which is link-up can be shown in the table.

In the Channel Group Port Information table, Actor is the local information and Partner is the port information of the peer device.

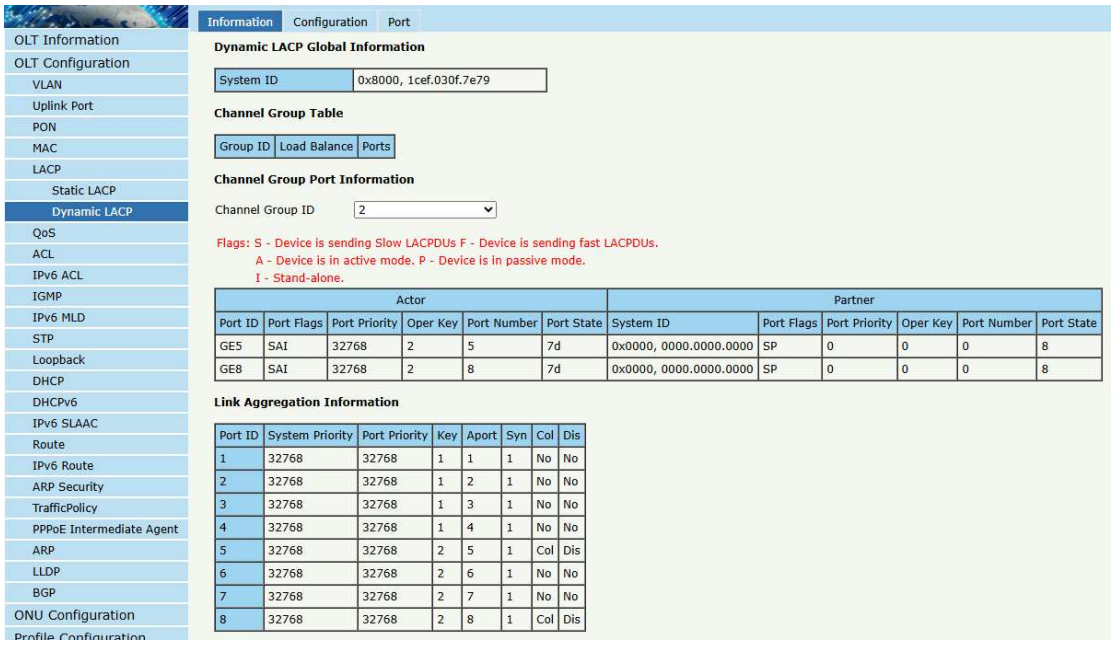


Figure 3.5-2: Dynamic LACP Information

Illustrations of partial parameter:

Parameters	Illustration
System ID	The MAC address of this device. When electing the reference port, first compare the system Priorities at both devices. The smaller the value, the higher the priority. If the priorities are the same, compare the system MAC addresses. The smaller the MAC address, the smaller the device ID, and the higher the priority.
System Priority	The smaller the value, the higher the priority.
Port Priority	For the election reference port. First, compare the port priorities. The smaller the priority value, the smaller the port ID. If the priorities are the same, compare the port numbers. The smaller the port number, the smaller the port ID. The port with the smallest port ID and the same attribute class configuration as the corresponding aggregation interface is taken as the reference port.
Oper Key	It is the Key that identifies whether ports can be aggregated. Only ports with the same key can join the same aggregation group.

Table 3.5-1 Dynamic LACP Parameter

3.5.2.2 Configuration

OLT Configuration→LACP→Dynamic LACP→Configuration

You can configure the system priority in this interface and specify the load balance policy for the channel Group.

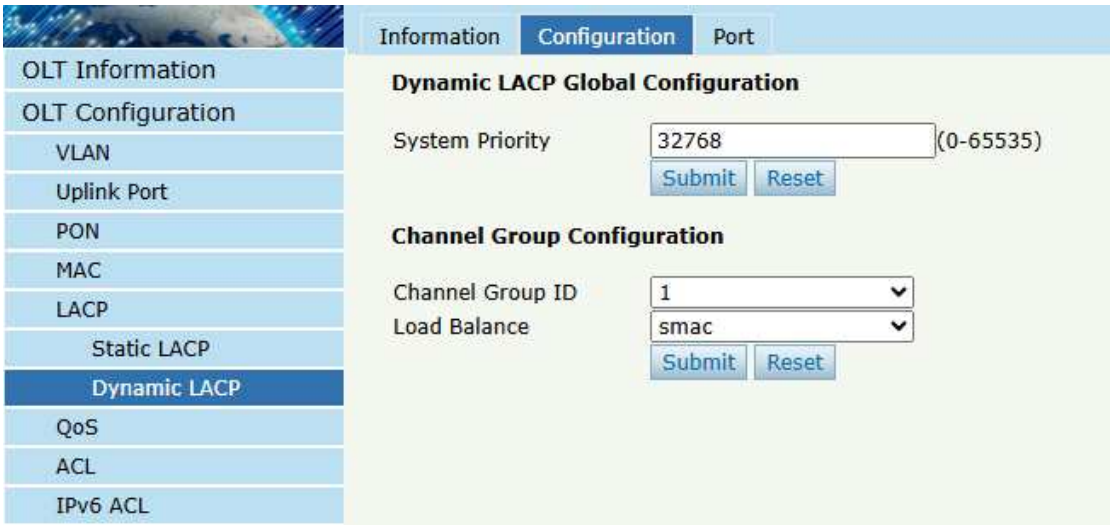


Figure 3.5-3: Dynamic LACP Configuration

3.5.2.3 Port

OLT Configuration→LACP→Dynamic LACP→Port

You can enable or disable the LACP protocol of the port in this interface. The working mode of port LACP is divided into two types: ACTIVE and PASSIVE. In ACTIVE mode, the device actively sends LACPDU to request the establishment of aggregation. In PASSIVE mode, the device only responds to the received LACPDU and does not actively initiate negotiations. Therefore, if the LACP working mode of the member ports within the dynamic aggregation group is PASSIVE and the LACP working mode of the opposite device is also PASSIVE, LACPDUs cannot be sent from both devices. If the LACP working mode of either end of the two devices is ACTIVE, LACPDU can be sent from both devices.

The LACP timeout interval also determines the frequency at which the opposite device transmits LACPDUs. LACP timeouts are categorized into two types: short timeout (3 seconds) and long timeout (90 seconds). If the LACP timeout is configured as a short timeout, the opposite device will transmit LACPDUs at a higher frequency (one LACPDU per second). Conversely, if the LACP timeout is set to a long timeout, the opposite end will transmit LACPDUs at a lower frequency (one LACPDU every 30 seconds).

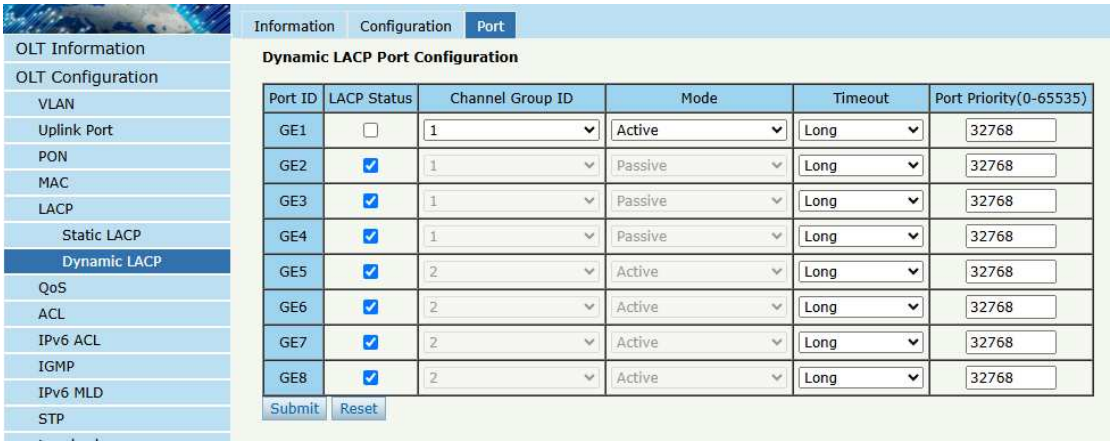


Figure 3.5-4: Dynamic LACP Port Configuration

3.6 QoS

OLT Configuration→QoS

When bandwidth is not enough or there is congestion in the network, queue scheduling can make sure high priority data traffic passes through the device firstly. Traffic will map to queues according to their priorities and transmit in the queues.

OLT supports eight queues altogether. Queue scheduling mode includes strict priority (SP), weighted round robin (WRR) and hybrid mode (SP-WRR).

Strict priority scheduling guarantees high priority traffic occupy as much as bandwidth. The lower priority traffics pass though only when there is remaining bandwidth.

WRR is a weight-based scheduling algorithm. Users can assign a weight value to each queue, reflecting the proportion of bandwidth it should obtain. Through weight allocation, both fairness and priority are taken into account to avoid the monopoly of bandwidth by a single queue.

In Strict-WRR queue scheduling, Q7 is the queue with the highest priority. As long as there is data in this queue, the scheduler will send all its data packets first until the queue is empty. Other low-priority queues allocate the remaining bandwidth according to the weights.

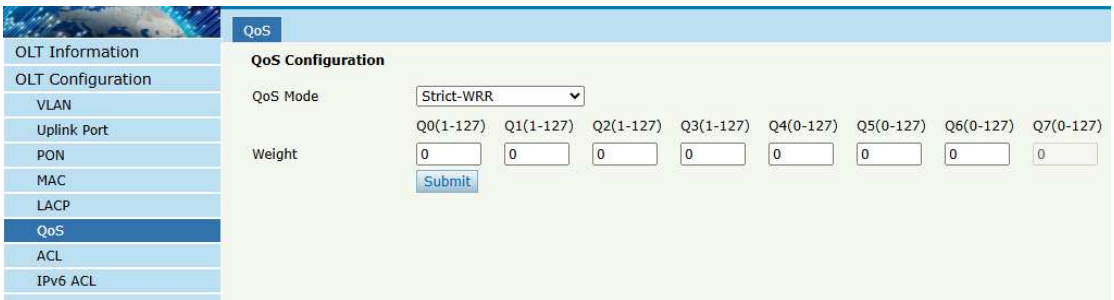


Figure 3.6-1: QoS Configuration

3.7 ACL

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

3.7.1 IP Filter

OLT Configuration→ACL→IP Filter
The filter is basic on the IP address, including source IP address and destination IP address.

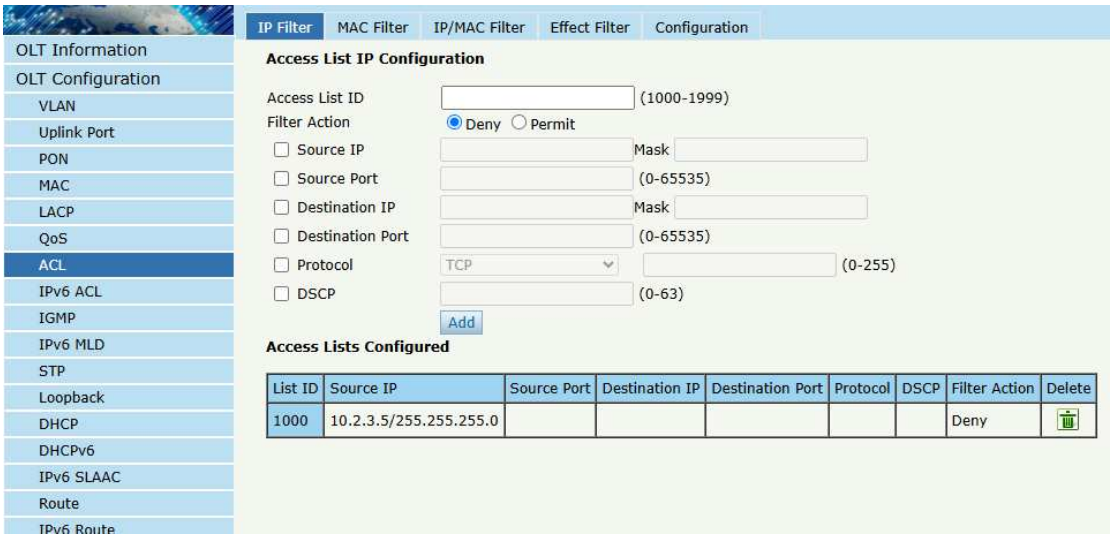


Figure 3.7-1: IP Filter

3.7.2 MAC Filter

OLT Configuration→ACL→MAC Filter
The filter is basic on the MAC address, including source MAC address and destination MAC address.

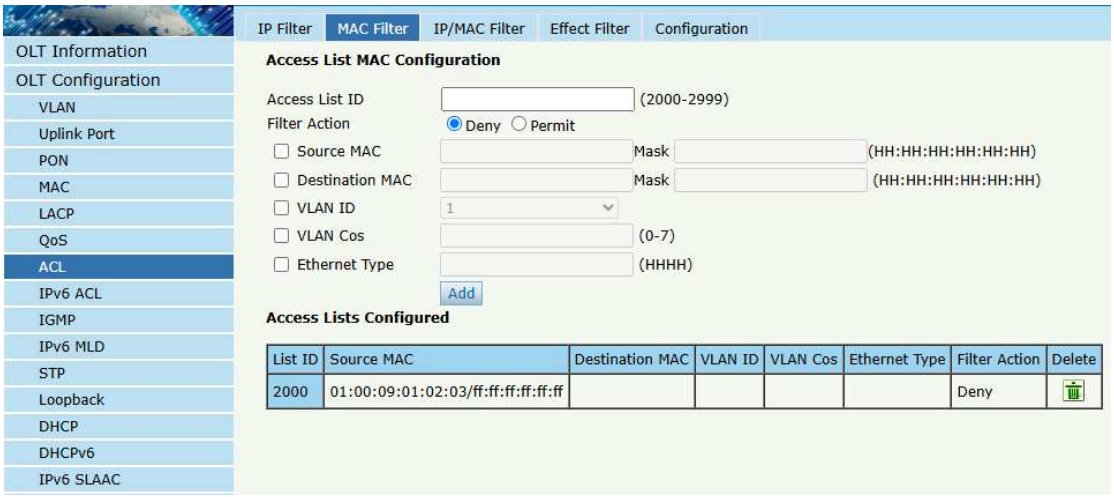


Figure 3.7-2: MAC Filter

3.7.3 IP/MAC Filter

OLT Configuration→ACL→IP/MAC Filter

This filter mix the IP address and MAC address, include source MAC address and destination MAC address, source IP address and destination IP address. Its filtering action also supports Traffic Classifier. Rules of this type are available for call by traffic policies. Users can speed the traffic that matches the rules and remark the priority labels.

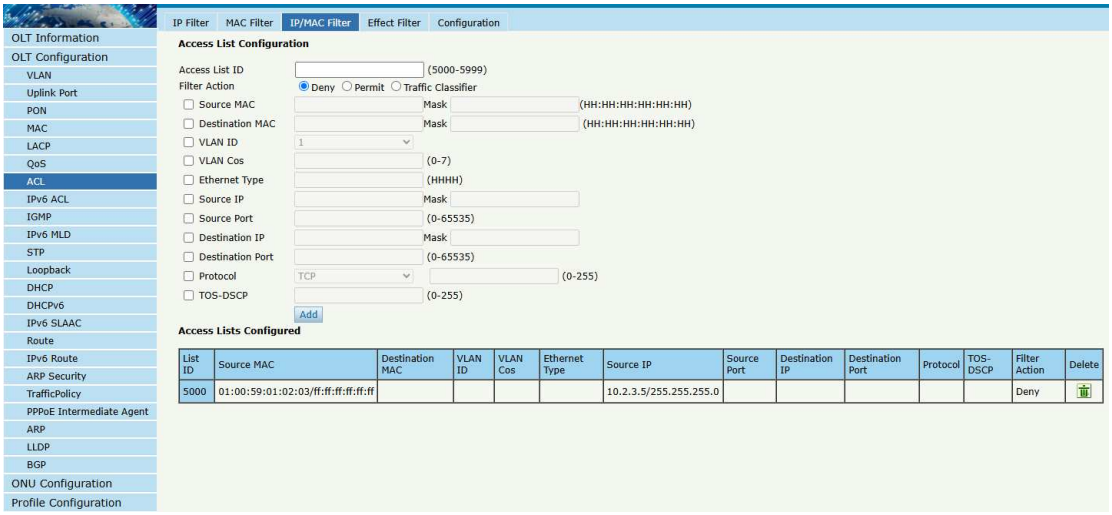


Figure 3.7-3: IP/MAC Filter

3.7.4 Effect Filter

OLT Configuration→ACL→Effect Filter

Bind the access list to the ports then it can take effect. Each access list can be bound several ports.

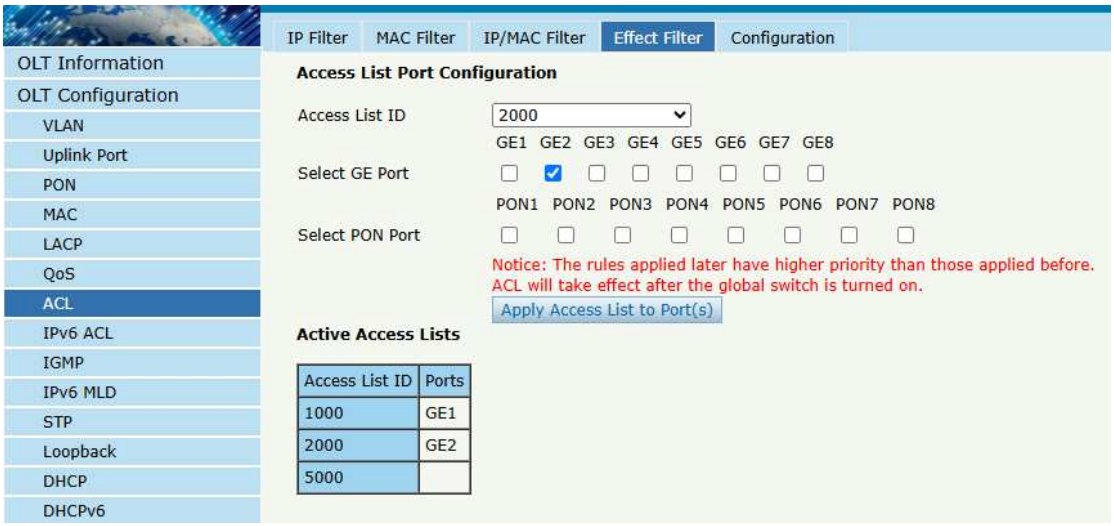


Figure 3.7-4: Bind Security Filter

3.7.5 Configuration

OLT Configuration→ACL→Configuration

This page is used to configure the effective switch and effective time period of ACL rules.

Notice:

1. This switch is used to enable or disable the ACL at any time, does not affect the timing function.
2. The function will be turned off if the effective and ineffective times are the same.

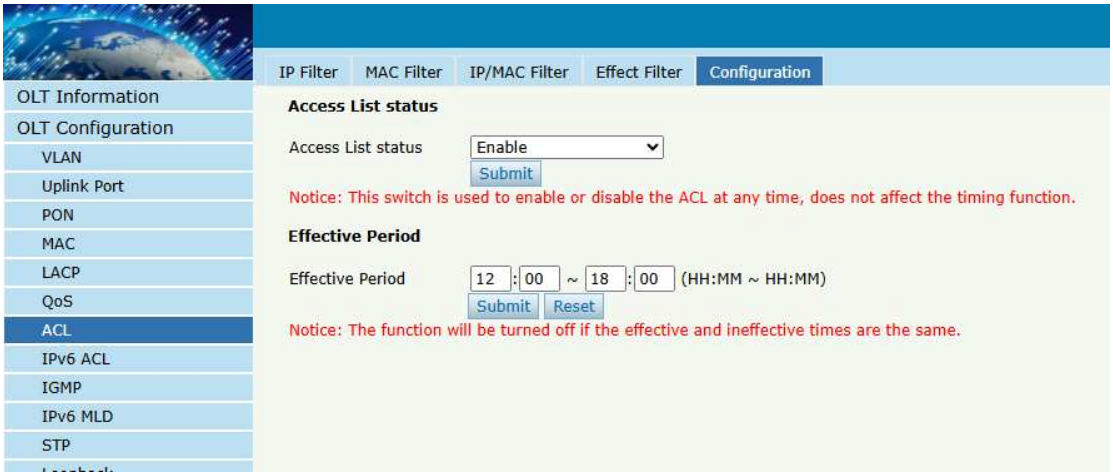


Figure 3.7-5: Configuration

3.8 IPv6 ACL

This part is about IPv6 security configuration of OLT. IPv6 ACL can permit or deny data passing or accessing by IPv6 packets.

3.8.1 IPv6 Filter

OLT Configuration→IPv6 ACL→ IPv6 Filter

The filter is based on the IPv6 address, including source IPv6 address and destination IPv6 address.

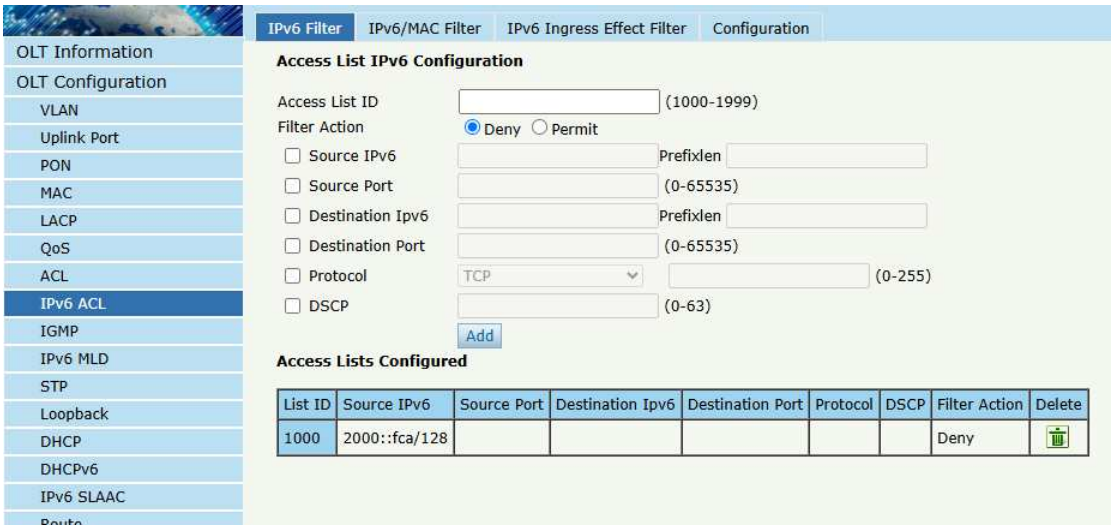


Figure 3.8-1: IPv6 Filter

3.8.2 IPv6/MAC Filter

OLT Configuration→IPv6 ACL→IPv6/MAC Filter

This filter mixes IPv6 address, MAC address and other parameters, including source IPv6 address and destination IPv6 address, source MAC address and destination MAC address, VLAN, Ethernet type, protocol, TCP/UDP port, and so on.

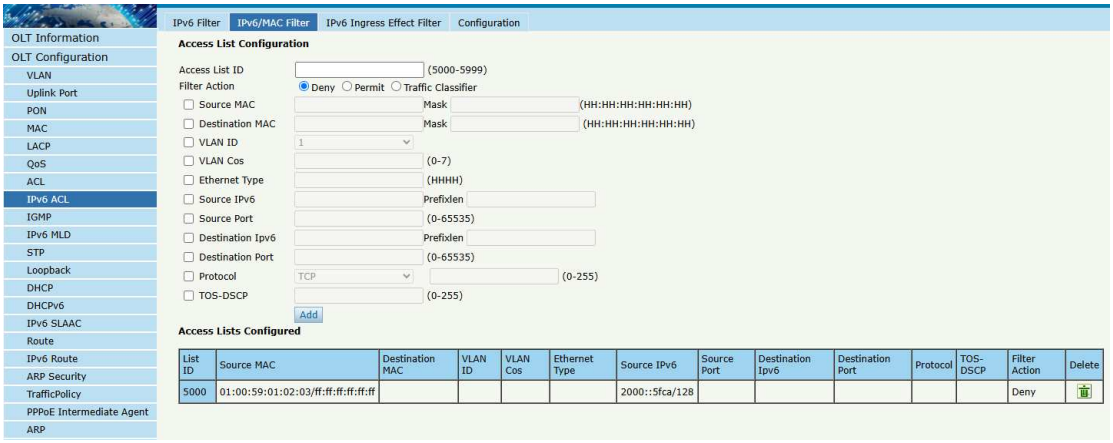


Figure 3.8-2: IPv6/MAC Filter

3.8.3 IPv6 Ingress Effect Filter

OLT Configuration → IPv6 ACL →IPv6 Ingress Effect Filter

Bind access list to ports so that the ACL rules can take effect. Each access list can be bound to several ports.

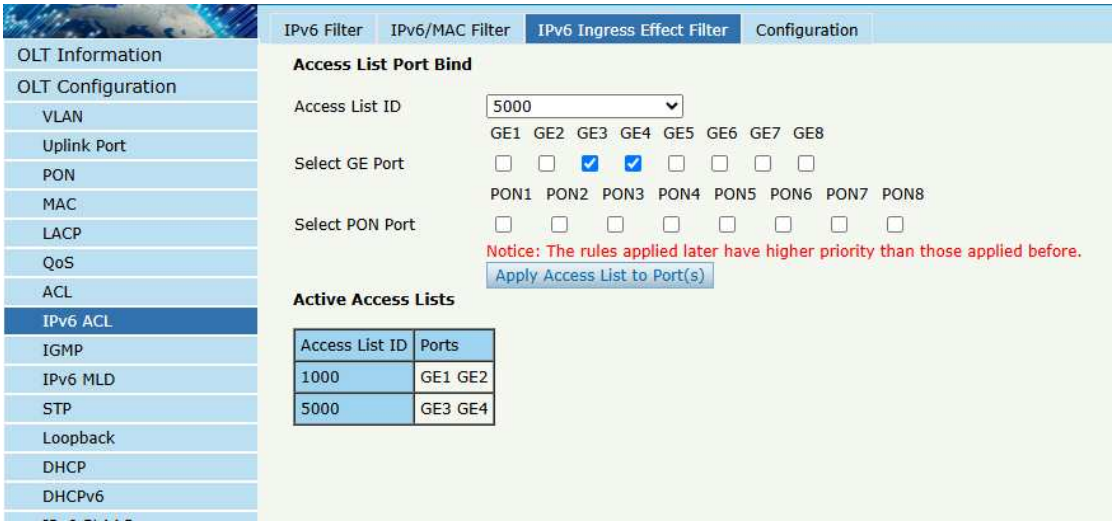


Figure 3.8-3: Bind IPv6 ACL Rule

3.8.4 Configuration

OLT Configuration→IPv6 ACL→Configuration

This page is used to configure the effective switch and effective time period of IPv6 ACL rules.

Notice:

1. This switch is used to enable or disable the ACL at any time, does not affect the timing function.
2. The function will be turned off if the effective and ineffective times are the same.

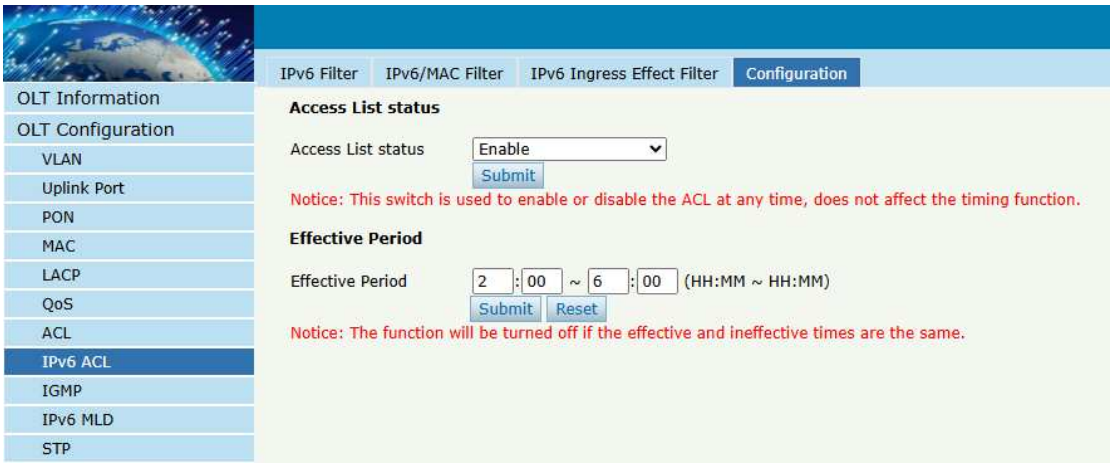


Figure 3.8-4: Configuration

3.9 IGMP

3.9.1 Group Member

OLT Configuration→IGMP→Group Member

After OLT enables IGMP Snooping, this page displays the IGMP member group information monitored by OLT.

Figure 3.9-1: Group Member

3.9.2 Global

OLT Configuration →IGMP→Global

IGMP basic configuration mainly contains parameters of query packet. When IGMP status is enabled, OLT works at IGMP snooping mode. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to "listen in" on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which devices need which IP multicast streams. Multicast may be filtered from the ports which do not need them and thus controls which ports receive specific multicast traffic. When IGMP status is disabled, OLT works at transparent mode.

Illustrations of each parameter:

Parameters	Illustration
Member Port Timeout	Configure the aging time of the dynamic member port. If the port does not receive the IGMP membership report message before the timeout, OLT will delete the port from the IGMP Snooping forwarding table.
Query Response Time	Configure the maximum response time of IGMP General Group Queries.
Last Member Query Interval	Configure the transmit interval of IGMP Specific Group Query packets.
Last Member Query Count	Configure the number of IGMP Specific Group Query packets sent.
Last Member Query Response	Configure the maximum response time of IGMP Specific Group Queries.
General Query Packet	The OLT port will periodically transmit IGMP General Query packets based on the configured General Query Interval after being enabled.
General Query Interval	Configure the interval for the OLT port to transmit IGMP General Group Query packets.
Query Source IP	Configure the source IP address of the IGMP group query packet.

Table 3.9-1 IGMP Configuration Parameter

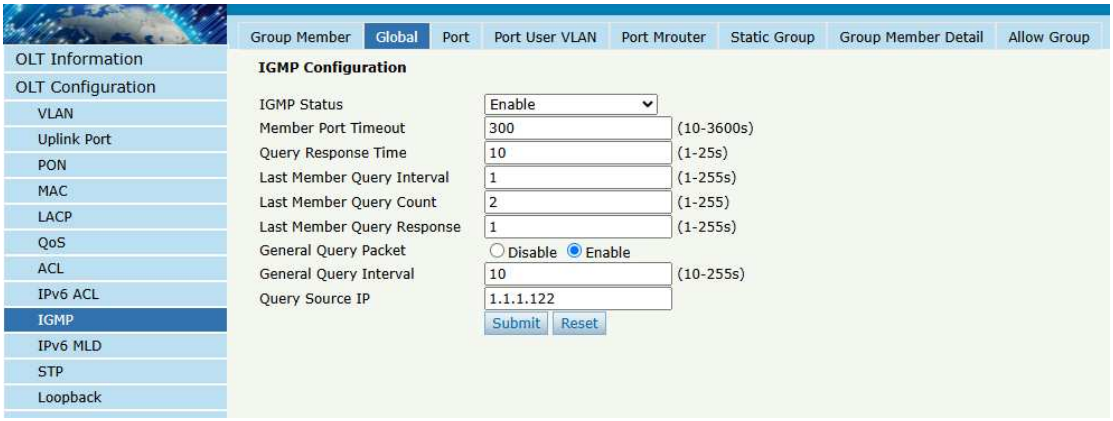


Figure 3.9-2: IGMP Global

3.9.3 Port

OLT Configuration →IGMP→Port

This configuration is used to set the maximum number of multicast groups and fast leave mode. When the port enables fast leave, it will not transmit IGMP Specific Group Query packet after receiving the IGMP group leave packet. OLT will delete the relevant table entries in the IGMP Snooping list.

Figure 3.9-3: IGMP Port

3.9.4 Port User VLAN

OLT Configuration →IGMP→Port User VLAN

Users can configure the OLT ports and VLAN for IGMP listening on this interface. Generally, PON ports should be configured, and user VLAN and group VLAN are the same. If user VLAN and group VLAN are different, multicast VLAN will be translated.

Figure 3.9-4: IGMP Port User VLAN

3.9.5 Port Mrouter

OLT Configuration →IGMP→Port Mrouter

The Multicast router port is used to transmit IGMP protocol packets to the multicast source. Generally, OLT uplink ports should be set as multicast router ports.

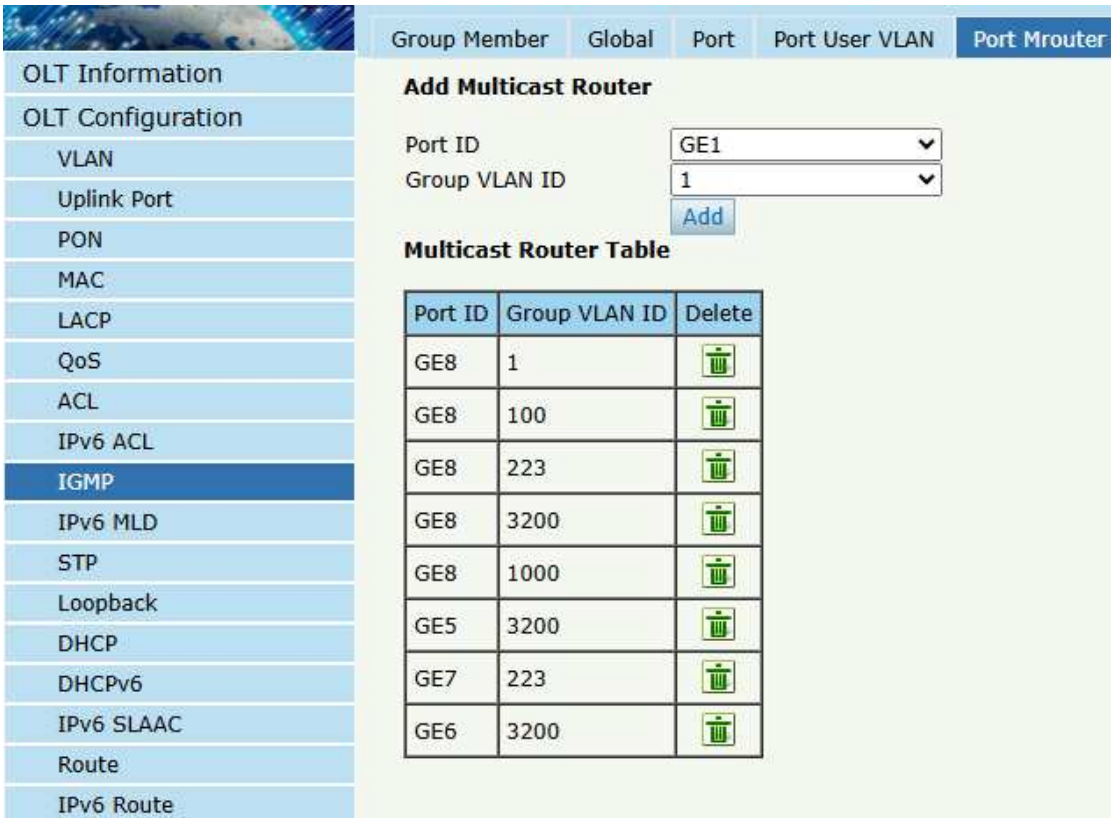


Figure 3.9-5: IGMP Port Mrouter

3.9.6 Static Group

OLT Configuration →IGMP→Static Group

This interface is used to configure static multicast listening table entries. It doesn't age like dynamic entries. If the host connected to the port needs to fixedly receive multicast data sent to a certain multicast group, the port can be configured to statically join the multicast group and become a static member port.

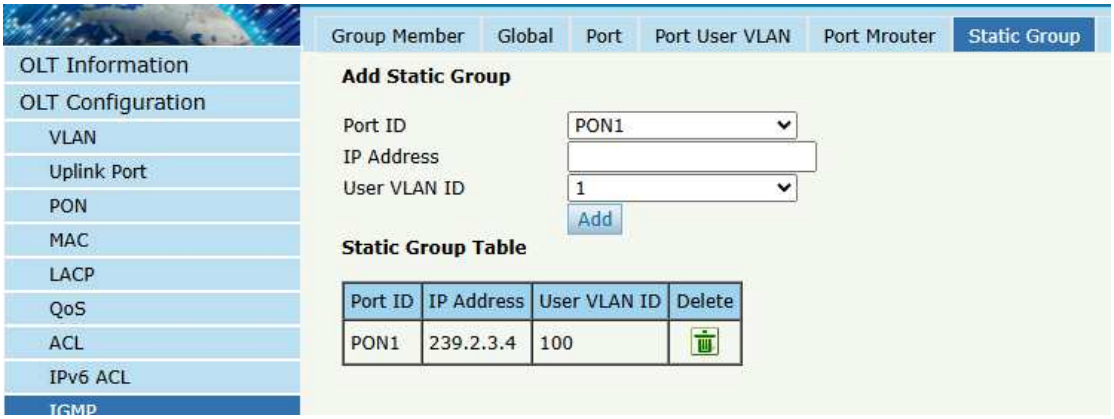


Figure 3.9-6: IGMP Static Group

3.9.8 Group Member Detail

OLT Configuration →IGMP→Group Member Detail

This page is used to view detailed information about current IGMP group members, including PON/ONU ID, Group VLAN ID, IP Address, and Client MAC.

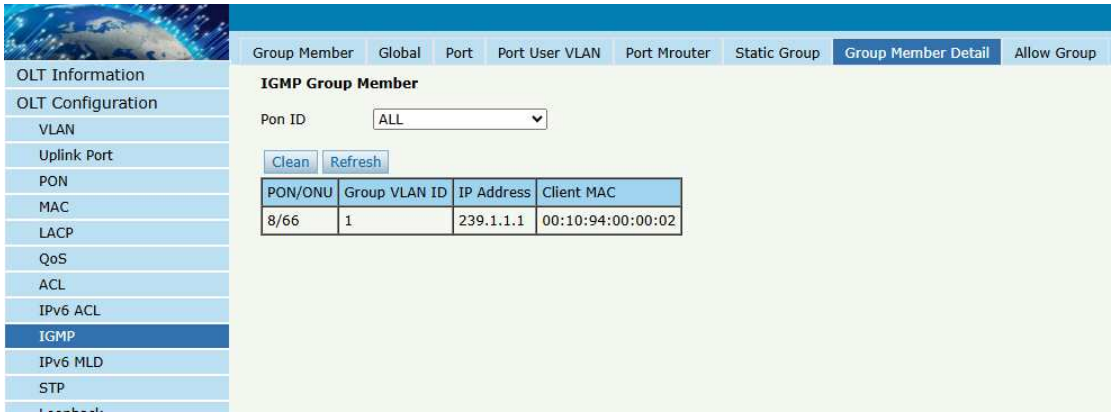


Figure 3.9-7: Group Member Detail

3.9.9 Allow Group

OLT Configuration →IGMP→Allow Group

IGMP Allow Group is a whitelist function for grouping, only groups within the configuration range can work properly, and groups outside the configuration range cannot be grouped.

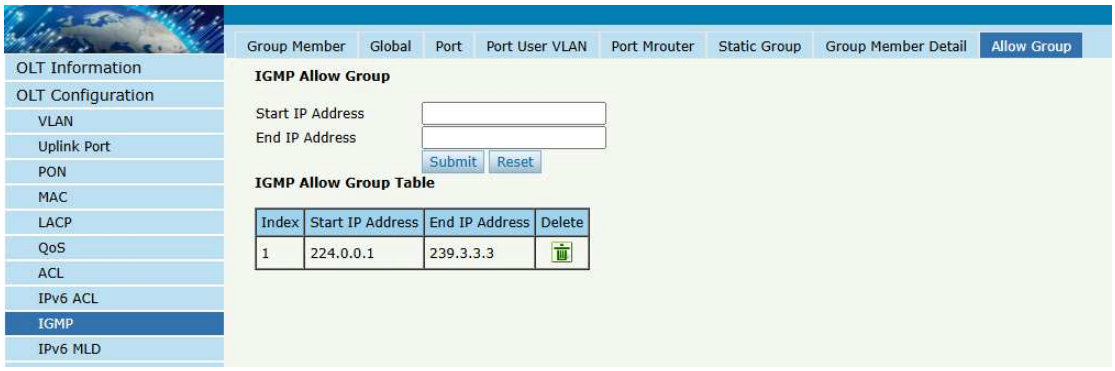


Figure 3.9-8: Allow Group

3.10 IPv6 MLD

3.10.1 Group Member

OLT Configuration → IPv6 MLD → Group Member

After OLT enables MLD Snooping, this interface displays the MLD member group information that OLT listens to.

Figure 3.10-1: IPv6 MLD Group Member

3.10.2 Global

OLT Configuration→IPv6 MLD→Global

This interface is used to enable IPv6 MLD Snooping and set IPv6 MLD related parameters.

Illustrations of each parameter:

Parameters	Illustration
Query Interval	Configure the time interval of the general group query packet in the MLDv2 QQIC field. The Non-Querier router synchronizes its own query timer through the received QQIC value to ensure that all routers in the network use the same query interval.
Query Response Interval	Configure the maximum response time of MLD General Group Queries. Multicast members need to reply to the report packet within this time.
Robustness Variable	This is the field in the MLDv2 query message.It defines the number of re-transmission.
Last Listener Query Count	Configure the number of MLD Specific Group Query packets sent.

Last Listener Query Interval	Configure the transmit interval of MLD Specific Group Queries.
Send General Query Packet	The OLT port will periodically transmit MLD General Query packets based on the configured General Query Interval after being enabled.
MLD Version	OLT supports MLDv1 and MLDv2.
General Query Interval	Configure the interval for the OLT port to transmit MLD General Group Query packets.
Query Source IP	Configure the source IPv6 address of the MLD group query packet.

Table 3.10-1 MLD Configuration Parameter

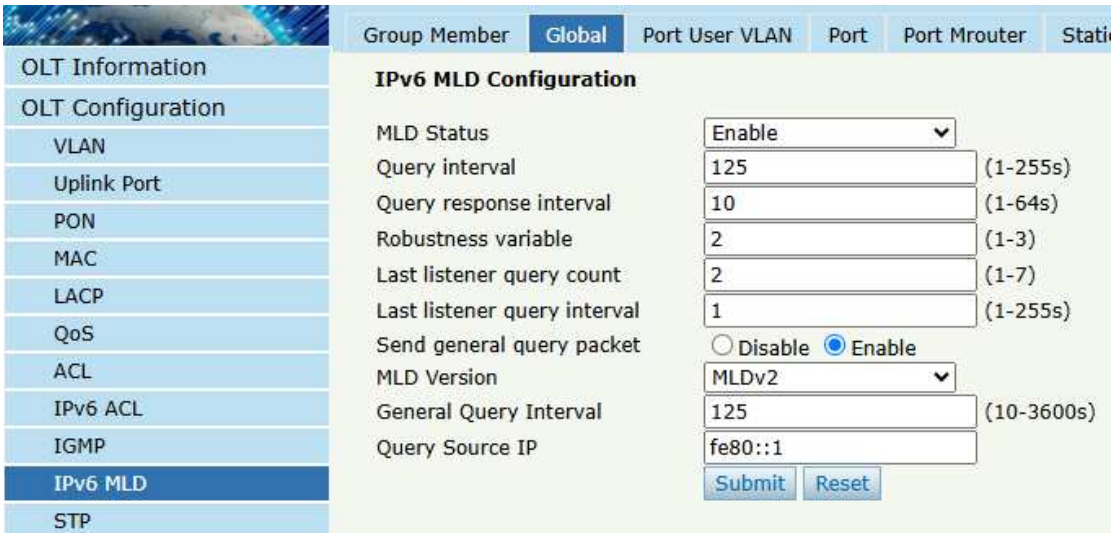


Figure 3.10-2: IPv6 MLD Global

3.10.3 Port User VLAN

OLT Configuration→IPv6 MLD→Port User VLAN

Users can configure the OLT ports and VLAN for MLD listening on this interface.

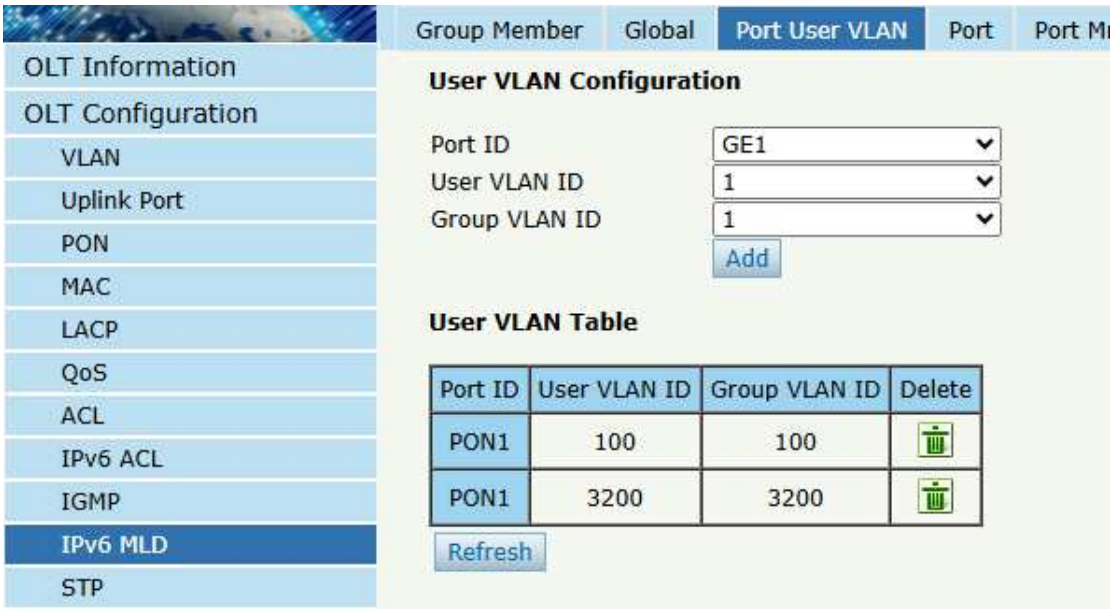


Figure 3.10-3: IPv6 Port User VLAN

3.10.4 Port

OLT Configuration → IPv6 MLD → Port

This configuration is used to set the maximum number of multicast groups and fast leave mode. When the port enables fast leave, it will not transmit MLD Specific Group Query packet after receiving the MLD group leave packet. OLT will delete the relevant table entries in the MLD Snooping list.

Figure 3.10-4: IPv6 MLD Port

3.10.5 Port Mrouter

OLT Configuration → IPv6 MLD → Port Mrouter

The Multicast router port is used to transmit MLD protocol packets (ICMPv6) to the multicast source. Generally, OLT uplink ports should be set as multicast router ports.

Figure 3.10-5: IPv6 MLD Port Mrouter

3.10.6 Static Group

OLT Configuration →IPv6 MLD → Static Group

This configuration is used to bind MLD IPv6 address and VLAN ID.

Notice: Before configuring Static Group, you must set MLD port user VLAN first.

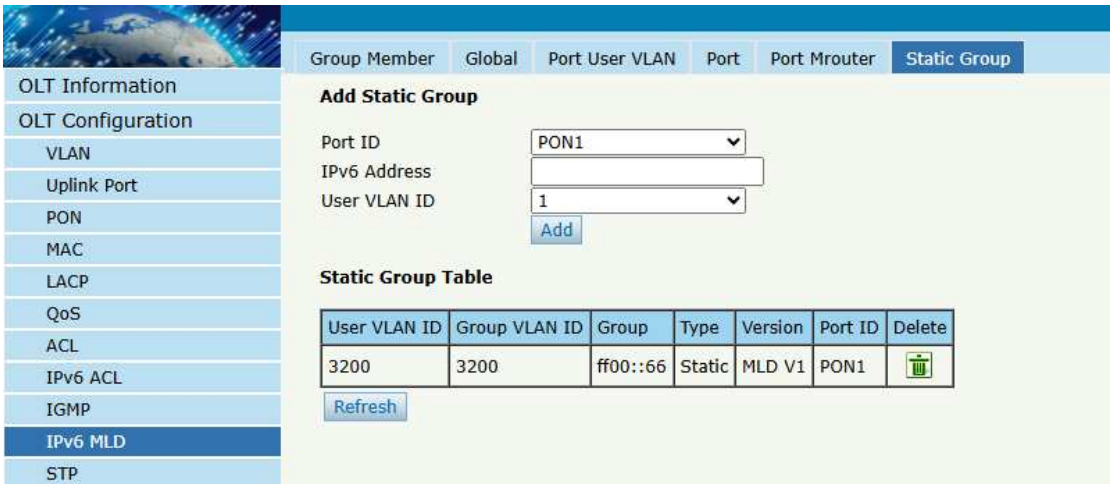


Figure 3.10-6: IPv6 MLD Static Group

3.11 STP

Spanning Tree Protocol is layer 2 protocol, which is used to eliminate network loop by blocking network redundant links selectively. It has the feature of link backup as well. Its protocol packet is called BPDU.

3.11.1 RSTP

3.11.1.1 Information

OLT Configuration→RSTP→Information

After OLT enables RSTP, you can view the root bridge device information and the RSTP port status information in this interface. For the protocol details and specific parameters of STP, please refer to IEEE 802.1D.

Illustrations of each parameter:

Parameters	Illustration
Cost	The path cost from this OLT to the root bridge device. It is actually the sum of the port cost along the path to the root bridge. If this OLT is the root bridge, the cost is 0.
Port	The port with the least path cost to the root bridge. If this OLT is the root bridge, the port is displayed as CPU. If this device is not a root bridge device, this port displays the current root port ID. The root port refers to the port with the lowest path cost to the root bridge.
Priority	Display the priority of the root bridge device and OLT. The device with the lowest bridge priority will be selected as the root bridge.
MAC Address	Display the MAC addresses of the root bridge and OLT. When the bridge priorities of the devices are equal, the device with the smallest MAC address will be selected as the root bridge.
Hello Time	The time interval for devices running the STP protocol to send BPDU is used for devices to detect whether there is a fault in the link.
Max Age	The aging time of the BPDU packet on the device port.
Forward Delay	The delay time of device port state transition.

Table 3.11-1 RSTP Information Table

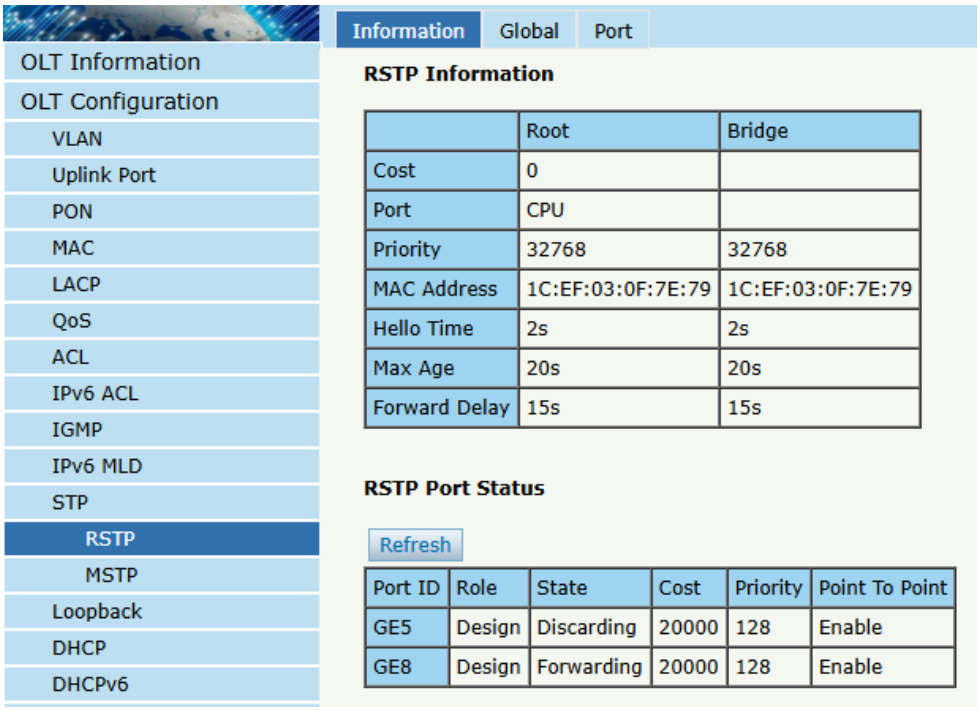


Figure 3.11-1: RSTP Information

3.11.1.2 Global

OLT Configuration→RSTP→Global

This configuration is used to set RSTP parameters of the device, which contains RSTP switch, priority, hello time, max age and forward delay. When the device uses Port-based mode, the transmitted BPDUs do not carry VLAN tags. If VLAN-based mode is used, the device will send BPDUs carry VLAN tag s according to the VLAN that the port has joined.

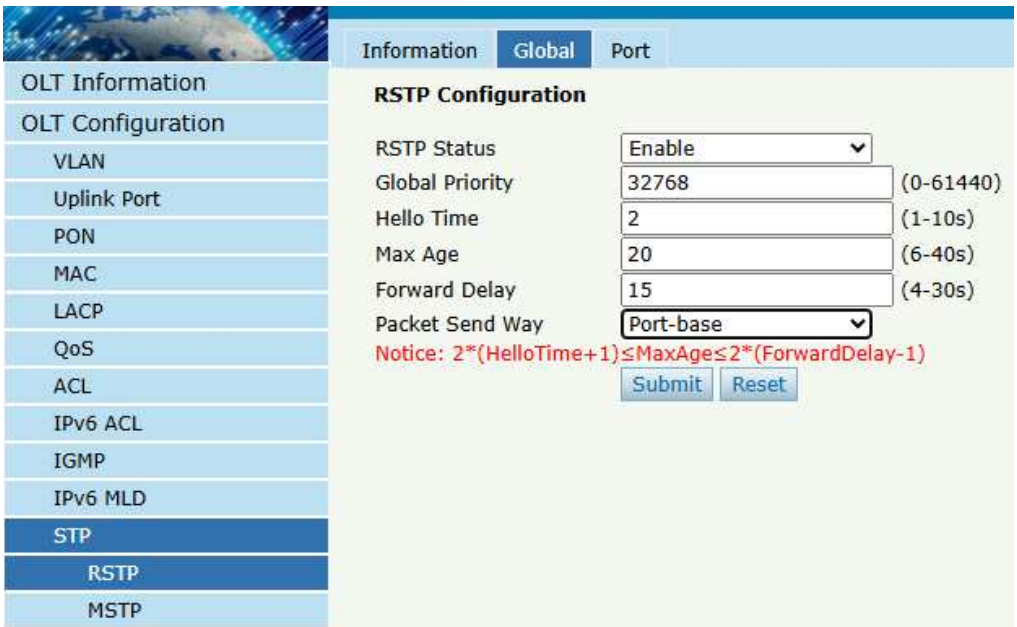


Figure 3.11-2: RSTP Global Configuration

3.11.1.3 Port

OLT Configuration→RSTP→Port

This user interface is used to set port RSTP parameters which contain port RSTP switch, port priority, port path cost, edge port and p2p port.

Illustrations of each parameter:

Parameters	Illustration
Status	The RSTP switch of the port.
Priority	The main function of Port Priority is to assist in determining port roles, such as the root port and the specified port, when the path cost is the same.
Cost	The main function of Port Path Cost is to determine the optimal path to the root bridge in the network topology.
admin Edge	Edge ports do not engage in RSTP operations and can transition directly to the Forwarding state without experiencing any delay. However, if an edge port receives a configured BPDU, it will lose its edge port characteristic, revert to a standard STP port, and re-initiate the spanning tree calculation process. If the port is directly connected to the terminal device, it can be configured as an edge port.
Point To Point	The two ports of the P2P link negotiate quickly through the Proposal/Agreement mechanism, directly switching the ports from the blocked state to the forwarding state without waiting for forwarding delay, which is used to switch the full-duplex link between devices.

Table 3.11-2 RSTP Port Parameter

Figure 3.11-3: RSTP Port Configuration

3.11.2 MSTP

The Multiple Spanning Tree Protocol (MSTP) is defined by the 802.1s standard developed by IEEE. It can converge quickly and forward traffic from different VLAN along their respective paths, providing a better load sharing mechanism for redundant links.

Notice: Within one OLT, both Fast Spanning Tree Protocol and Multi Spanning Tree Protocol cannot be enabled simultaneously.

3.11.2.1 Information

OLT Configuration→STP→MSTP→Information

MSTP information mainly displays the root bridge information of all spanning trees, VLAN mapping range, and roles and forwarding status of participating interfaces.

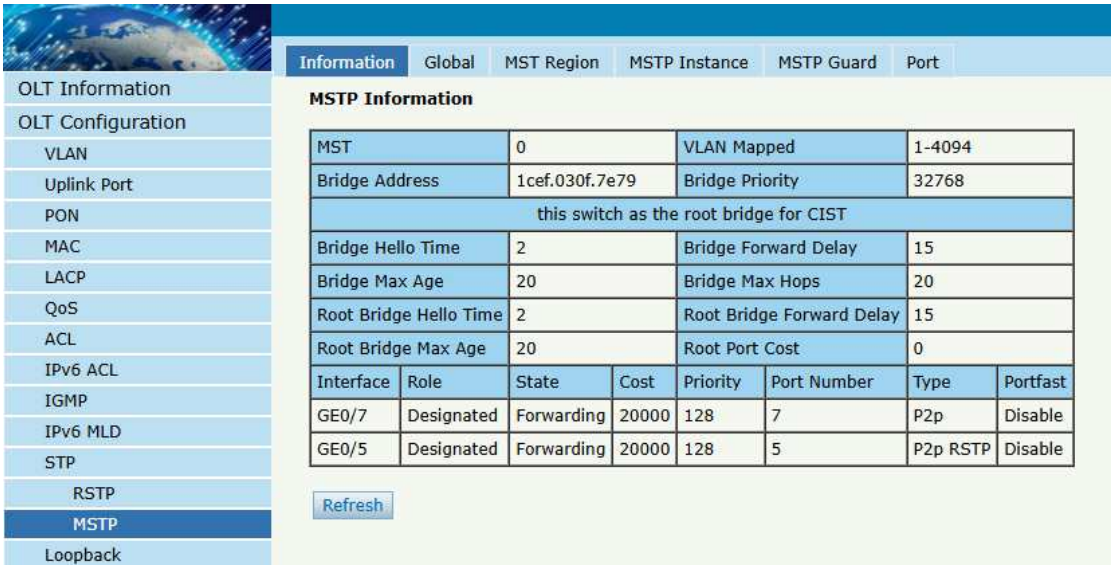


Figure 3.11-4: MSTP Information

3.11.2.2 Global

OLT Configuration→STP→MSTP→Global

This page is used to set the parameters of the device's spanning tree protocol, including spanning tree protocol switch, Hello Time, Forward Delay, Max Age and Bridge Max Hops.

Notice:2*(Hello Time+1)≤Max Age≤2*(ForwardDelay-1)

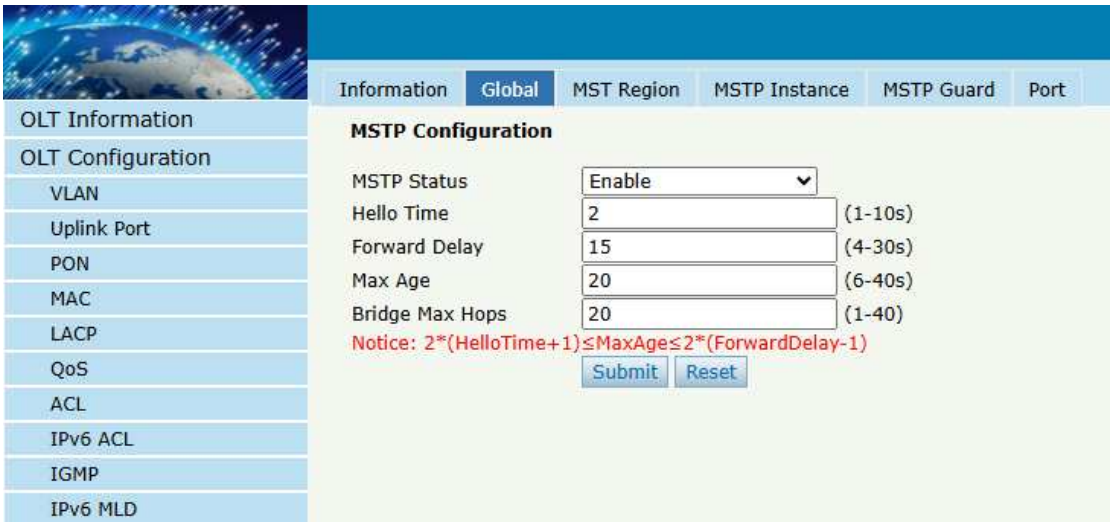


Figure 3.11-5: MSTP Global

3.11.2.3 MST Region

OLT Configuration→STP→MSTP→MST Region

This interface is used to configure MSTP region name. The configuration of the mapping relationship between VLAN and MST instances in the switching network is the same, the MSTP region name and revision level are the same, and devices connected by physical links will be divided into the same MST region.

Figure 3.11-6: MSTP Region

3.11.2.4 MSTP Instance

Multiple spanning trees can be generated within an MST region through MSTP, and

each spanning tree is independent of each other and corresponds to its corresponding VLAN. Each spanning tree is called an MST instance.

OLT Configuration→STP→MSTP→MST Instance

This page is used to configure the mapping relationship between VLAN and MST instances. MSTP implements load sharing based on the VLAN mapping table. By default, instance 0 maps all VLAN.

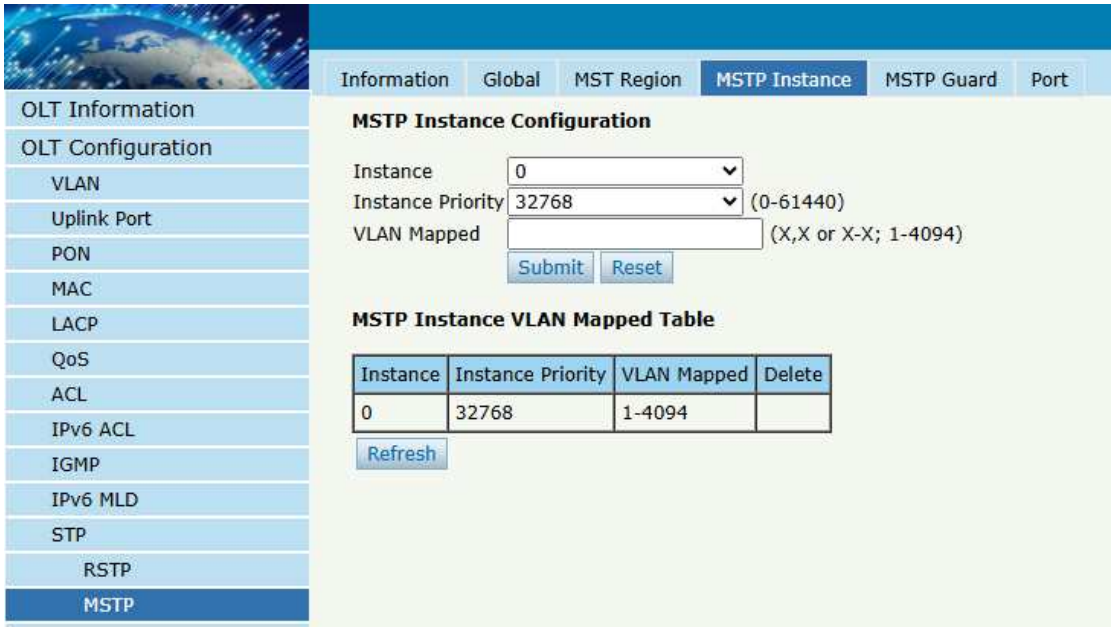


Figure 3.11-7: MSTP Instance

3.11.2.5 MSTP Guard

OLT Configuration→STP→MSTP→MST Guard

This interface provides BPDU Filter, BPDU Filter Recovery, BPDU Guard and Loop Guard functions to achieve stable network operation.

After enabling Loop Guard, when a loop port appears in the switching network, relevant information is displayed in the inconsistent loop port table of the spanning tree.

Figure 3.11-8: MSTP Guard

3.11.2.6 Port

OLT Configuration→STP→MSTP→Port

This page is used to configure the Status, Priority (0-240), Cost (1-200000000), Portfast, Point To Point, BPDU Filter, BPDU Guard and Guard. Please select the instance that needs to be configured.

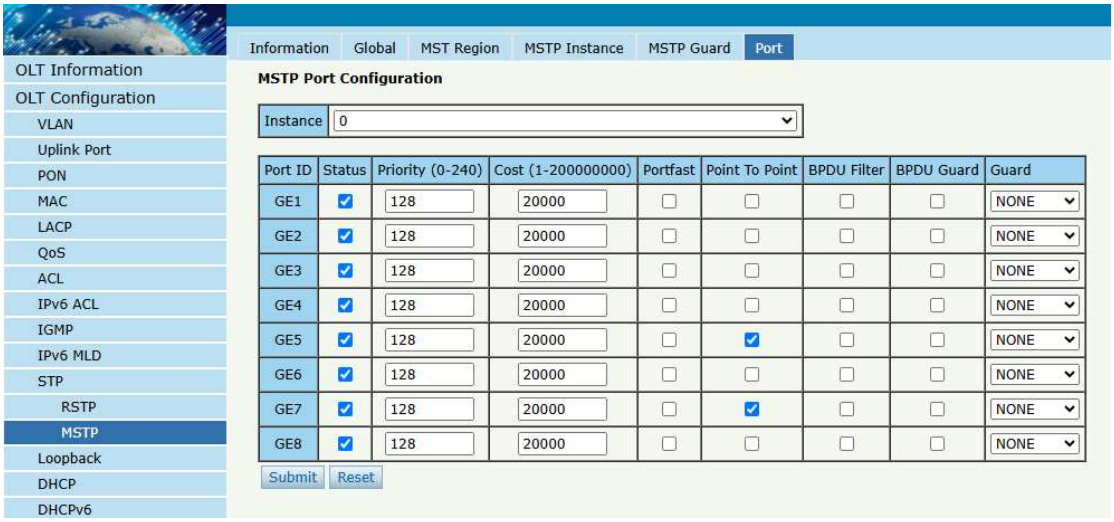


Figure 3.11-9: MSTP Port

3.12 Loopback

Loopback in the network can cause devices to repeatedly send broadcast, multicast and unknown unicast messages, resulting in waste of network resources or even network paralysis. Loopback detection periodically sends detection packets from the

interface to check if the packets are returned to the device, thereby determining whether there are loops in the interface, the network where the device is located, or the network to which the device is connected, and thus alerting the network administrator to take measures to eliminate the loops.

3.12.1 Information

OLT Configuration→Loopback→Information

After the device detects the Loopback, it will display the Loopback information on this interface.

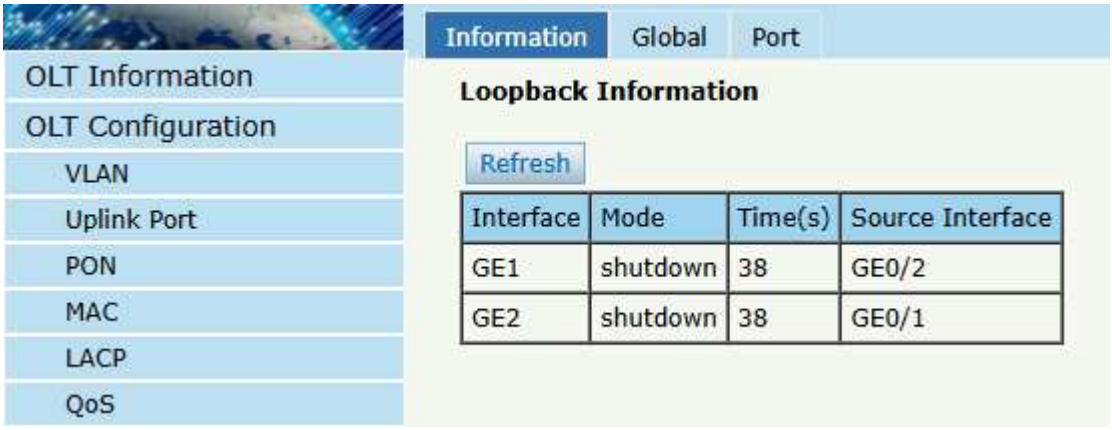


Figure 3.12-1: Loopback Information

3.12.2 Global

OLT Configuration→Loopback→Global

This interface is used to enable or disable Loopback detect and configure Loopback detection mode, age time.

Illustrations of each parameter:

Parameters	Illustration
Status	Loopback detection switch.
Range	Loopback detection port range, with All, PON and Uplink options available.
Mode	The way the device handles the Loopback port. **Only-alarm:** The device only displays loop alarm information. **Auto-recovery:** The device will automatically shutdown the loop port and re-enable it after the loop ages. **Manual-recovery:** The device will automatically shutdown the loop port. When the loop ages, it will not automatically resume operation. Users need to manually enable the port.

Age Time	Aging time of loop state.
Packet Send Way	When the device uses Port-based mode, the transmitted detection packets do not carry VLAN tags. If VLAN-based mode is used, the device will send detection packets carry VLAN tag s according to the VLAN that the port has joined.
Packet Send Time	The sending interval of Loopback detection packets.

Table 3.12-1 Loopback Configuration Parameter

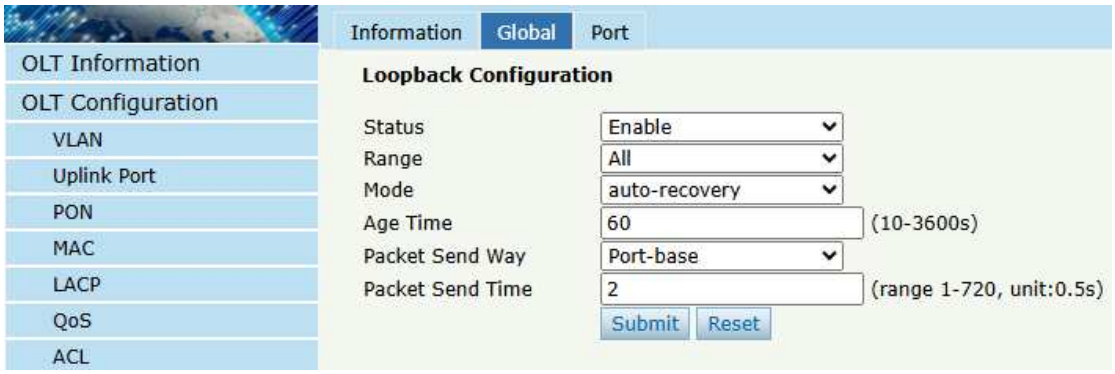


Figure 3.12-2: Loopback Global Configuration

3.12.3 Port

OLT Configuration→Loopback→Port

Loopback port configuration is used to specify the port range of Loopback function. Loopback detection will take effect on the port when it is checked.

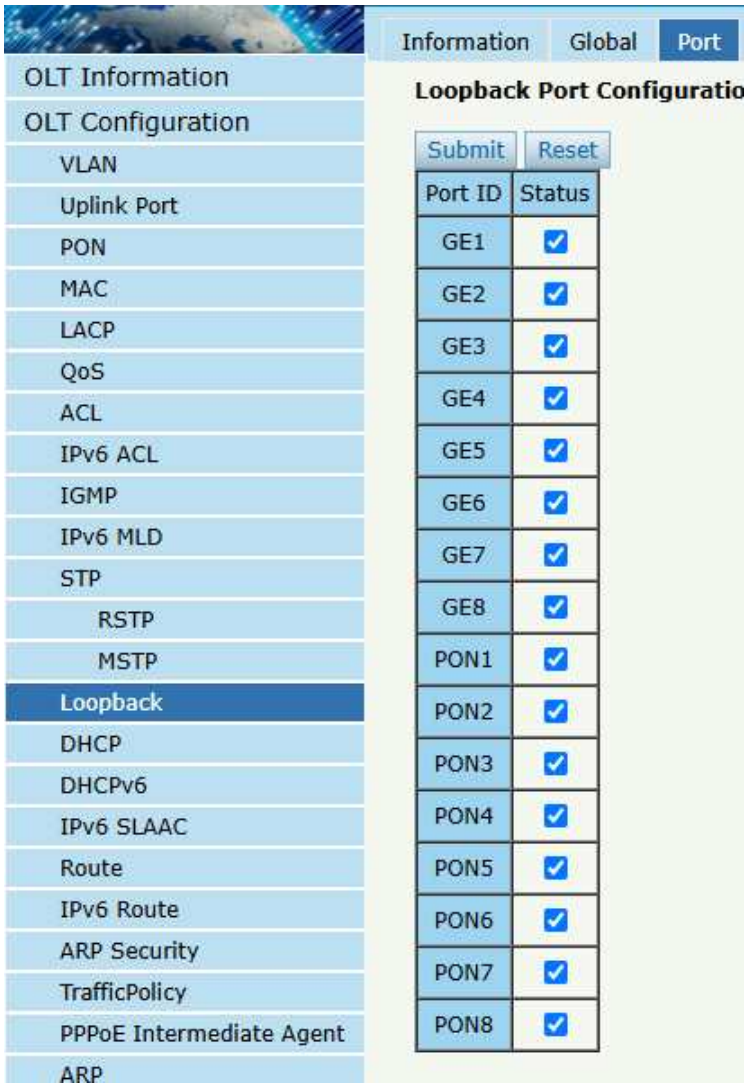


Figure 3.12-3: Loopback Port

3.13 DHCP

OLT can support the following DHCP functions.

- DHCP Server
- DHCP Relay
- DHCP Snooping

3.13.1 DHCP Server

3.13.1.1 DHCP Lease

OLT Configuration→DHCP→DHCP Server→Lease

This table displays the MAC addresses, host name and IP addresses, lease time assigned to them by OLT.

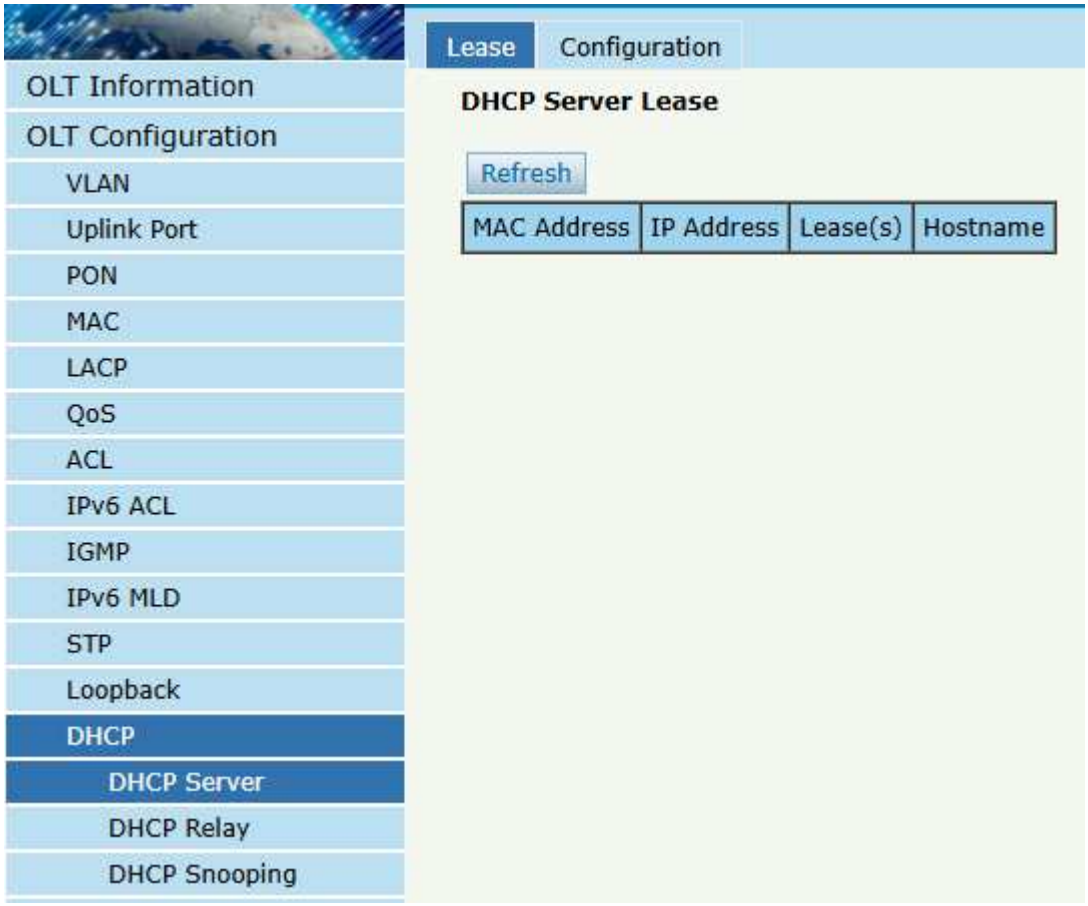


Figure 3.13-1: DHCP Lease

3.13.1.2 DHCP Configuration

OLT Configuration→DHCP→DHCP Server→Configuration

You can configure the OLT as the DHCP Server to allocate IP addresses in this interface. Before enabling DHCP server, you must configure IP address for the VLAN.

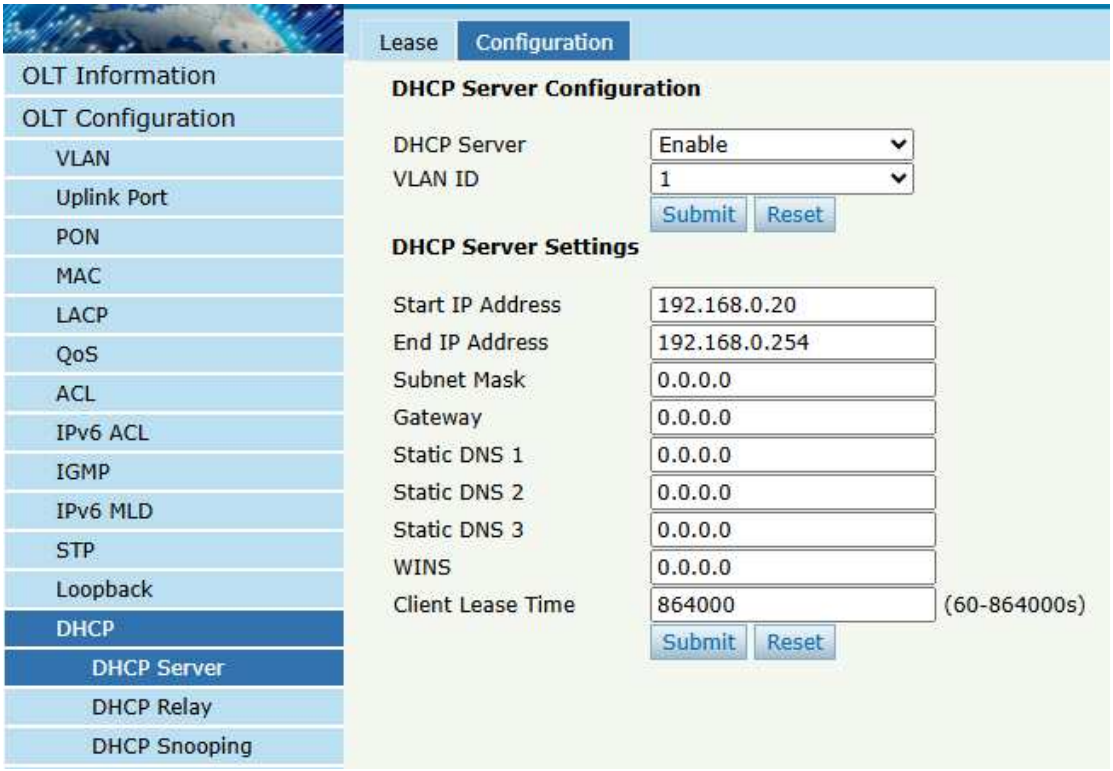


Figure 3.13-2: DHCP Configuration

3.13.2 DHCP Relay

3.13.2.1 DHCP Relay

OLT Configuration→DHCP→DHCP Relay

Because the DHCP service exists in one broadcast domain, the server and the client are usually in the same network segment. DHCP relay can solve the issue that DHCP server and client do not exist in the same network segment. You can configure the destination DHCP server IP and the VLAN to be relayed in this interface.

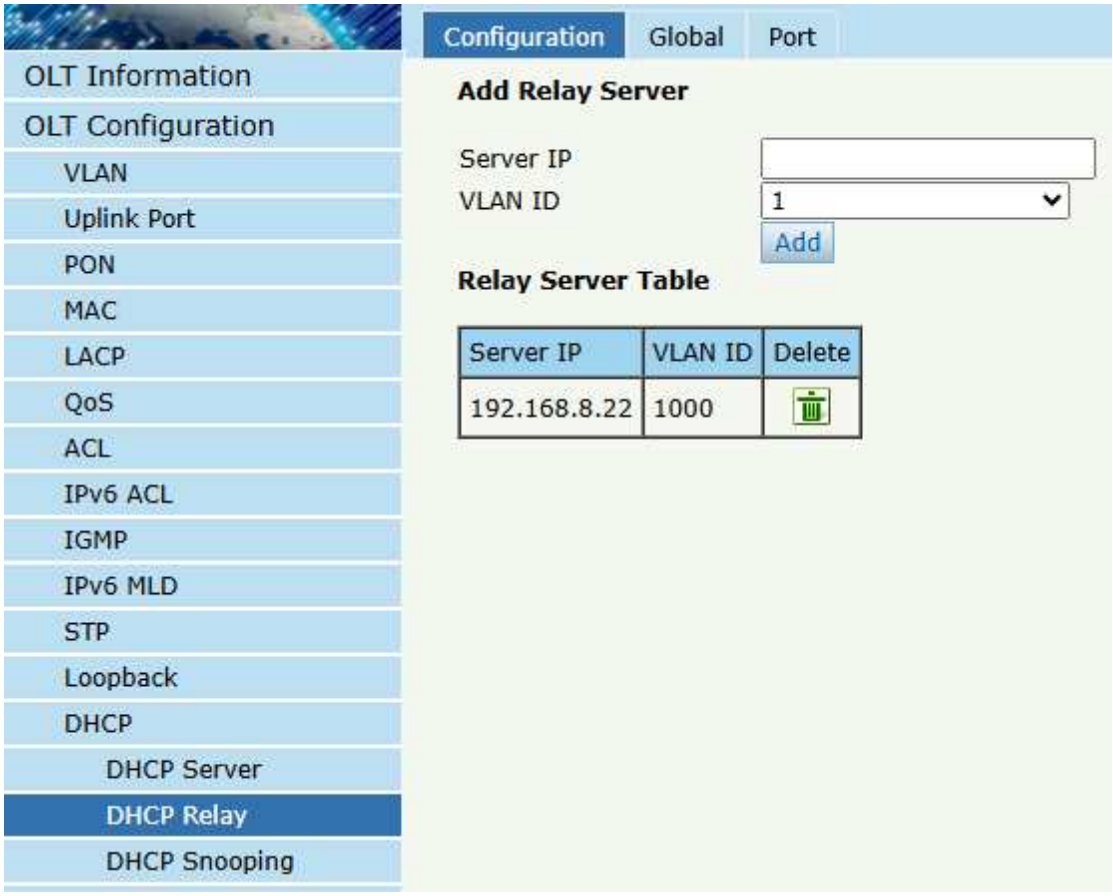


Figure 3.13-3: DHCP Relay Configuration

3.13.2.2 Global

OLT Configuration→DHCP→DHCP Relay→Global

This page is used to configure the Option 82 function of DHCP relay. After receiving the DHCP request message, the DHCP relay will process the message according to whether it contains Option 82 and the processing strategy and padding mode configured by the user, and forward the processed message to the DHCP server.

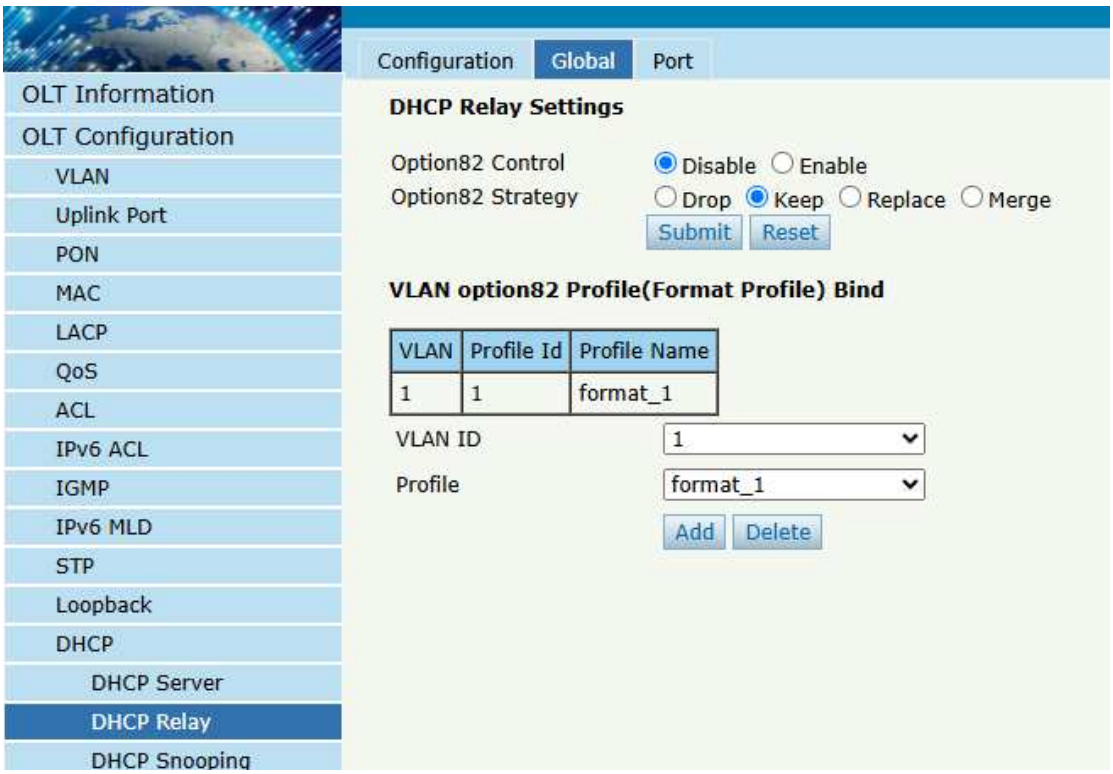


Figure 3.13-4: DHCP Relay Global

3.13.2.3 Port

OLT Configuration→DHCP→DHCP Relay→Port

This page is used to configure the Option 82 Circuit ID and Remote ID of the port.

Figure 3.13-5: DHCP Relay Port

3.13.3 DHCP Snooping

DHCP Snooping is a network security mechanism designed to ensure that DHCP clients obtain IP addresses from legitimate DHCP servers. It maintains mappings between DHCP clients' IP addresses and their MAC addresses, along with other parameters, to prevent DHCP related attacks on the network.

3.13.3.1 Bind List

OLT Configuration→DHCP→DHCP Snooping→Bind List

After OLT enables DHCP Snooping, it will listen to the DHCP interaction process, record information such as the MAC address of the DHCP client, the assigned IP address, lease time, VLAN and port number, and form a dynamic binding table. The DHCP Snooping binding table ages according to the DHCP lease period or automatically deletes the corresponding table entry based on the DHCP Release

packet sent when the user releases the IP address. Since the DHCP Snooping binding table records the mappings between DHCP clients' IP addresses, MAC addresses, and other parameters, verifying DHCP packets against this table can effectively prevent IP Spoofing and ARP Spoofing attacks. It should be noted that after OLT enables DHCP Snooping, the trusted port also needs to be specified. For details, please refer to Section 3.13.3.3.

This interface shows the DHCP Snooping binding list.

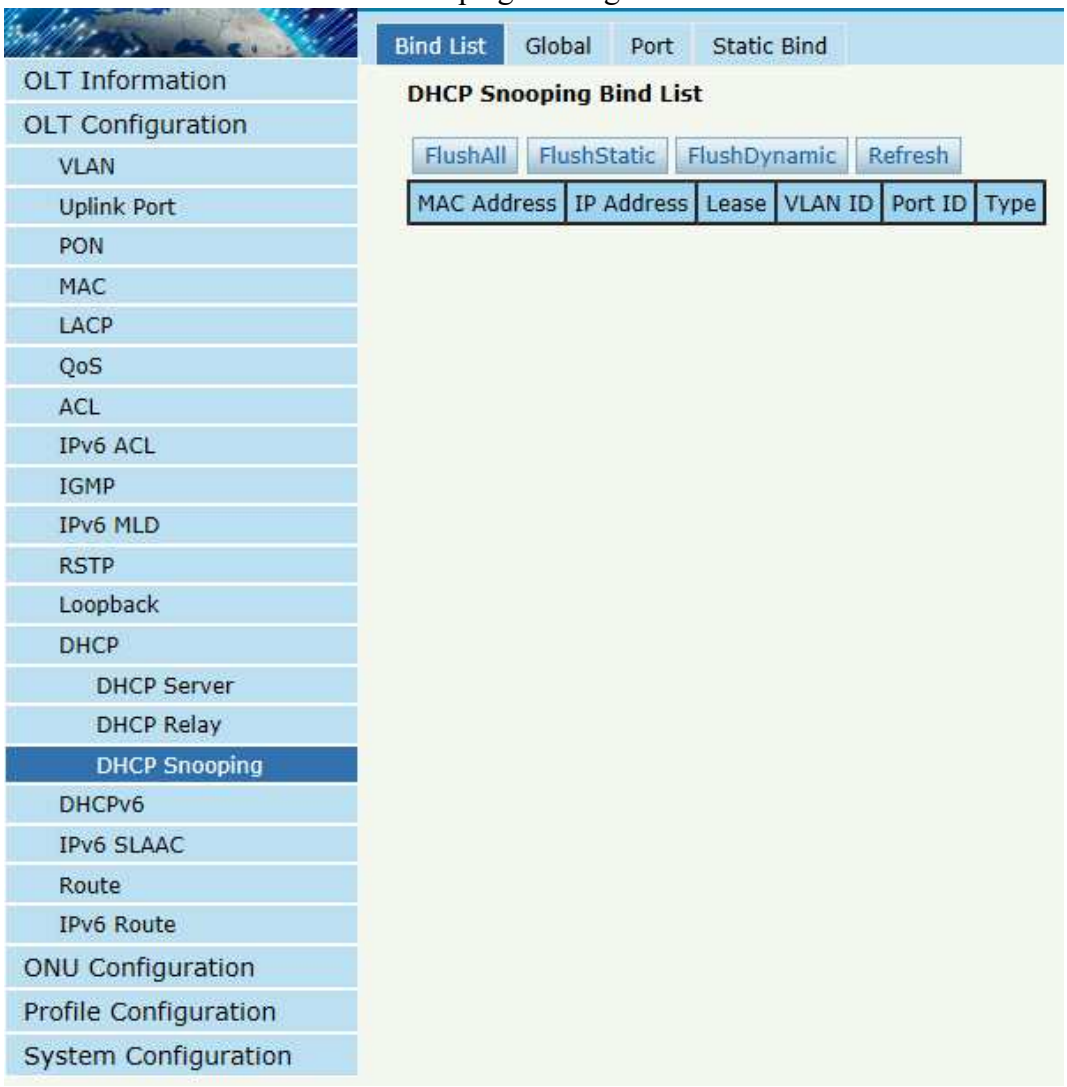


Figure 3.13-6: DHCP Snooping Bind List

3.13.3.2 Global

OLT Configuration→DHCP→DHCP Snooping→Global

DHCP snooping global configuration mainly contains DHCP Snooping switch, option 82 settings, DHCP traffic rate limit. After enabling DHCP Snooping, it is necessary to specify the target VLAN for listening; otherwise, the OLT will not forward the relevant packets.

When OLT enables the Option 82 function, please refer to the following table for the

specific effects of each processing strategy:

Strategy	The Processing of Packets by DHCP Snooping
Drop	If the packet carries the Option 82 option, discard the packet. If the packet does not carry the Option 82 option, no processing will be done and it will be forwarded directly.
Keep	If the packet carries the Option 82 option, Keep Option 82 in the packet unchanged and forward it. If the packet does not carry the Option 82 option, just forward.
Replace	If the packet carries the Option 82 option, OLT will populate Option 82 based on the filling mode, content, format, etc. configured on DHCP Snooping, replace the original Option 82 in the packet and forward it. If the packet does not carry the Option 82 option, OLT will add the option 82 defined by the device in the packet and then forward it.
Merge	If the packet carries the Option 82 option, OLT will replace and fill the option 82 field according to the content defined by the format profile and then forward it. If the packet does not carry the Option 82 option, no processing will be done and it will be forwarded directly.

Table 3.13-1 DHCP Snooping Option 82 Strategy

To prevent illegal users from sending a large number of DHCP packets and causing attacks on the network, DHCP Snooping supports a packet speed limit function, which restricts the rate at which the interface receives DHCP packets. When the rate of the DHCP packets received by the port exceeds the maximum rate limit, the OLT will automatically shutdown this port. After waiting for the over speed recovery interval, the port will be enabled again. Each port supports DHCP packet receiving rate limit. For specific configuration please refer to Section 3.13.3.3.

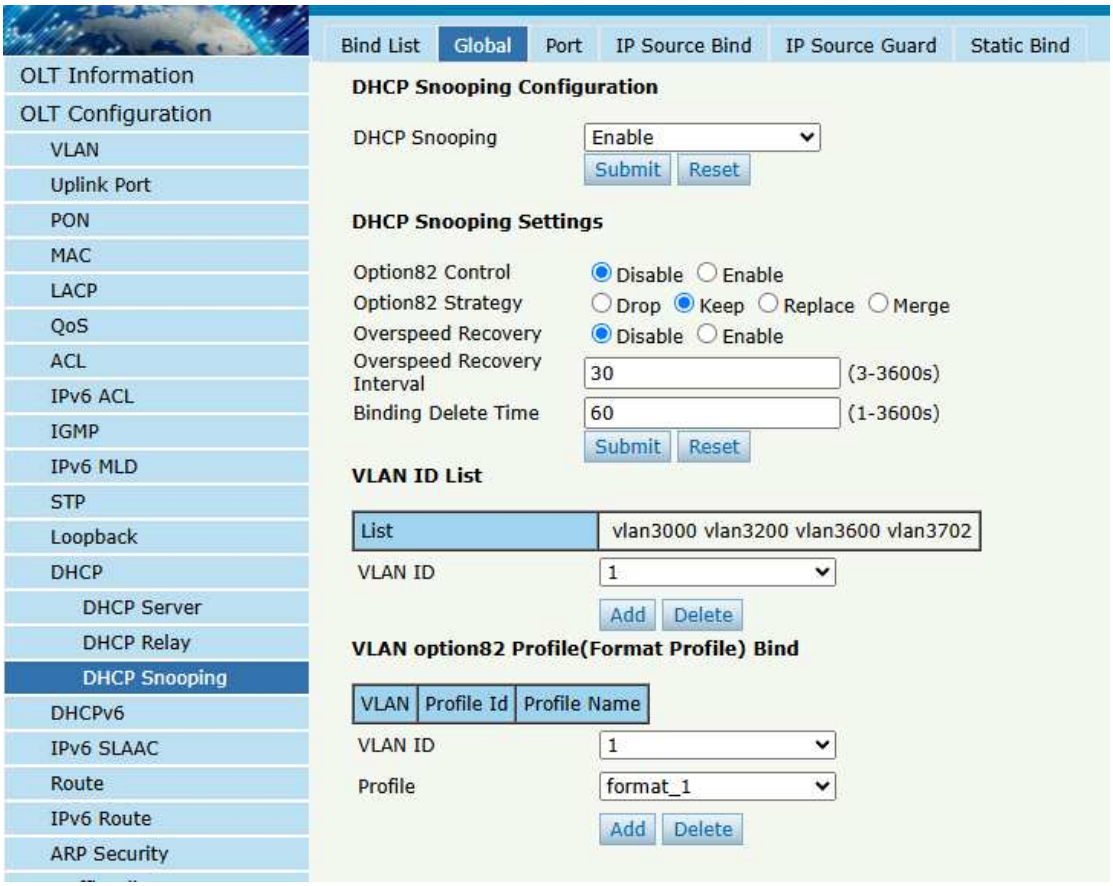


Figure 3.13-7: DHCP Snooping Global

3.13.3.3 Port

OLT Configuration→DHCP→DHCP Snooping→Port

This user interface is used to configure DHCP snooping parameters of ports which contain port type, option 82 parameters and rate limit.

You need to configure the port connected to the DHCP server as a trusted port in order to forward DHCP packets normally. Option82 parameters, “Option 82 Circuit ID” and “Option 82 Remote ID”, are effective for untrust ports.

“Limit Rate” is the ports’ max speed of receiving DHCP packets.

Figure 3.13-8: DHCP Snooping Port Configuration

3.13.3.4 Static Bind

OLT Configuration→DHCP→DHCP Snooping→Static Bind

The DHCP Snooping binding table is divided into dynamic binding tables and static binding tables. Dynamic binding tables are generated through DHCP packets, while static binding tables are manually configured by users. Since servers, printers and other devices usually use static IP addresses, static IP devices are not in the dynamic binding table. Adding them to the static binding table can prevent them from being misjudged as illegal devices and at the same time stop the behavior of IP misuse.

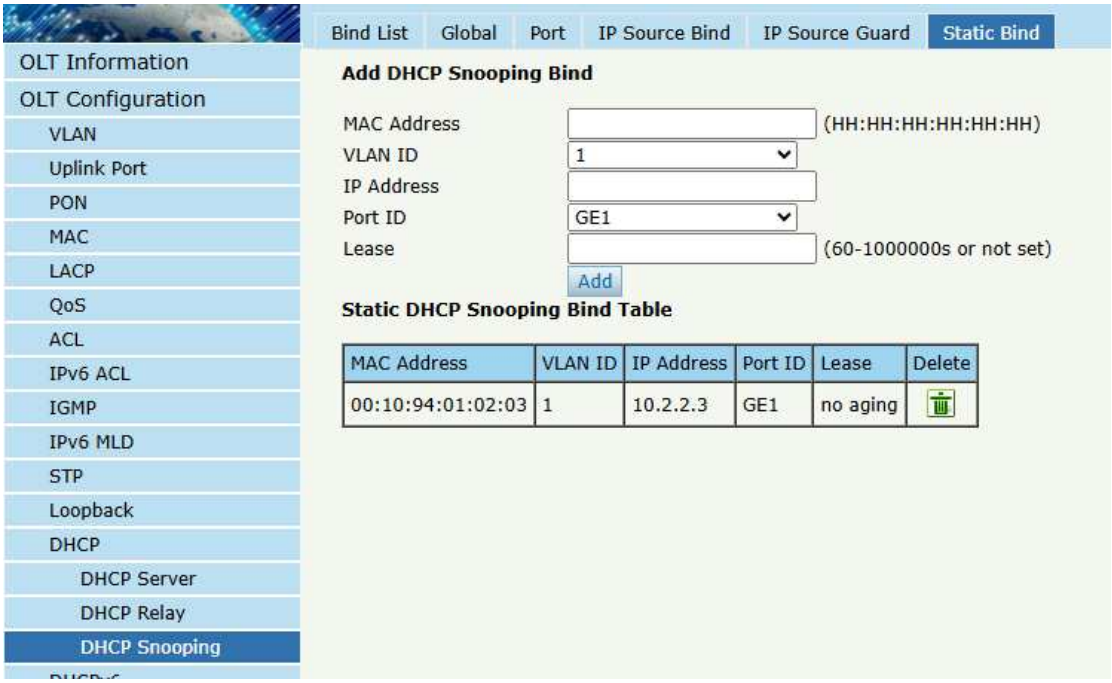


Figure 3.13-9: DHCP Snooping Static Bind

3.13.3.5 IP Source Guard

OLT Configuration→DHCP→DHCP Snooping→IP Source Guard

This function is actually based on the DHCP Snooping Bind List to restrict access to the external network .That means that an issue outside the list cannot access the external network. For example, in Filter-type, if IP-Address is selected, those devices whose IP addresses are the IP in the table have the permission to access the external network. If IP-MAC-Address is selected, only those devices that match both addresses simultaneously have the permission to access the external network.

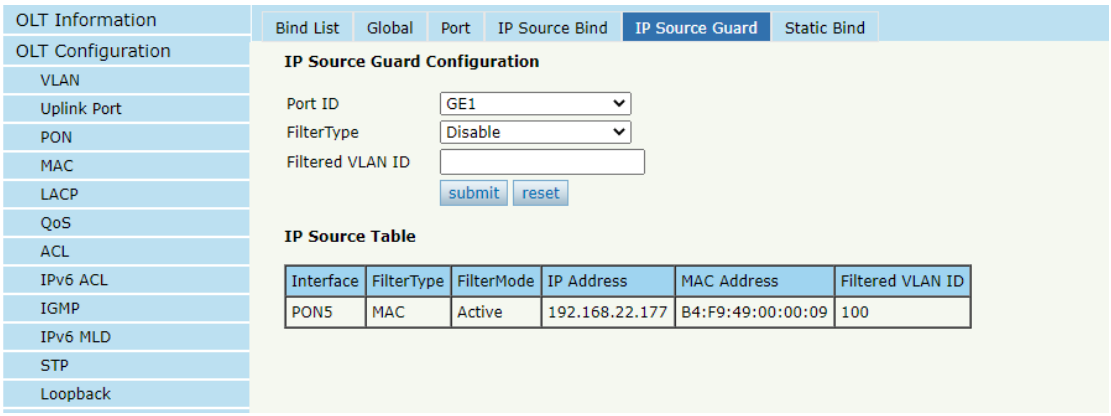


Figure 3.13-10: DHCP Snooping IP Source Guard

3.13.3.6 IP Source Bind

OLT Configuration→DHCP→DHCP Snooping→IP Source Bind

If you configure a rule in IP Source Guard, a dynamic rule is displayed in IP Source Bind Table.You can add a static rule manually on this interface.It works as described in the previous section.

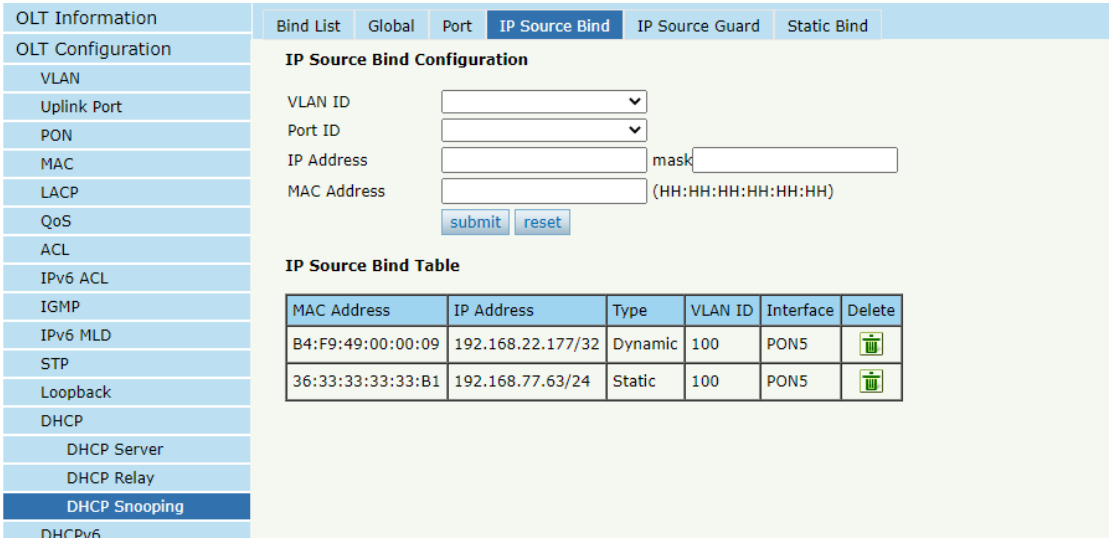


Figure 3.13-11: DHCP Snooping IP Source Bind

3.14 DHCPv6

3.14.1 DHCPv6 Server

DHCPv6 is a network protocol that used to configure IPv6 address, IPv6 prefix, DNS, domain and other network parameters for a host which operating on an IPv6 network.

3.14.1.1 DHCPv6 Bind Information

OLT Configuration →DHCPv6 →DHCPv6 Server → DHCPv6 Bind Information

DHCPv6 bind information displays IPv6 addresses which have been assigned to hosts by OLT.

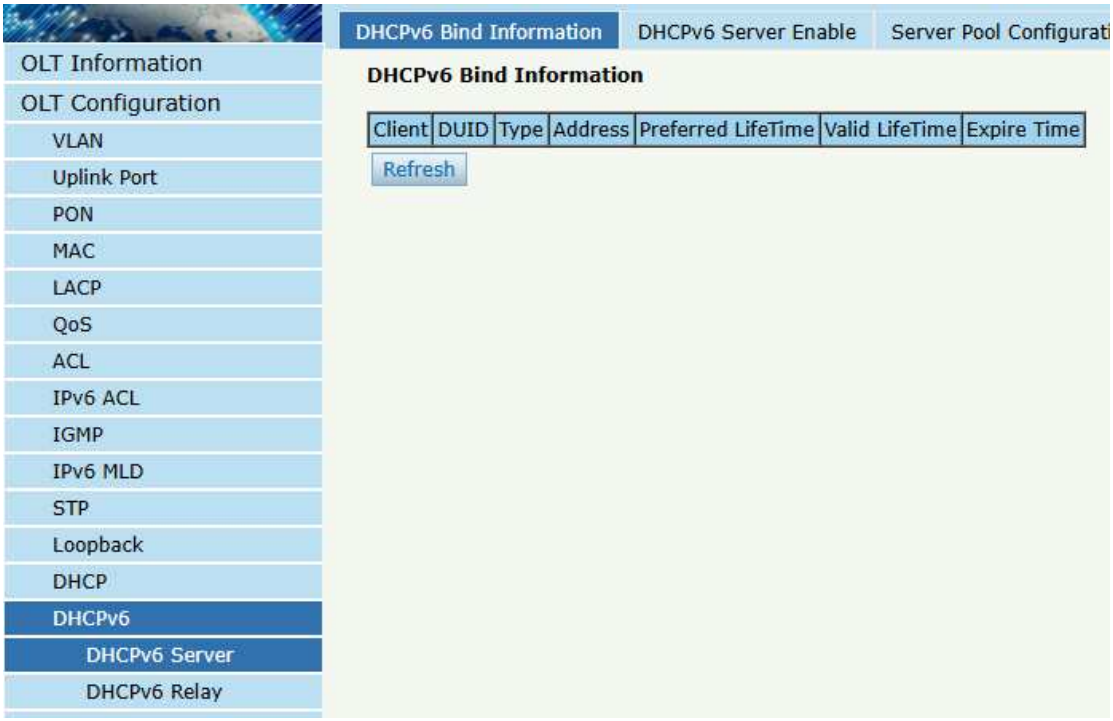


Figure 3.14-1: DHCPv6 Bind Information

3.14.1.2 DHCPv6 Server Enable

OLT Configuration → DHCPv6 → DHCPv6 Server → DHCPv6 Server Enable
Select VLAN and fill in DHCPv6 pool name, enable DHCPv6 server, then the VLAN will be added into the table. Before enabled DHCPv6 server, VLAN IPv6 address and server pool are required.

When there are multiple DHCPv6 servers in the network, the client compares the Preference value in the DHCPv6 Advertise packets of each server and gives priority to the server with the highest preference value.

The "Rapid Commit" option is used for quickly allocating IPv6 addresses. If OLT enables rapid allocation, a Reply packet is directly returned to assign IPv6 addresses/prefixes and other network configuration parameters to the client.

DUID stands for the unique identifier of DHCPv6 devices. Each server or client has exactly one unique identifier. Servers use DUID to identify different clients, while clients use DUID to identify servers.

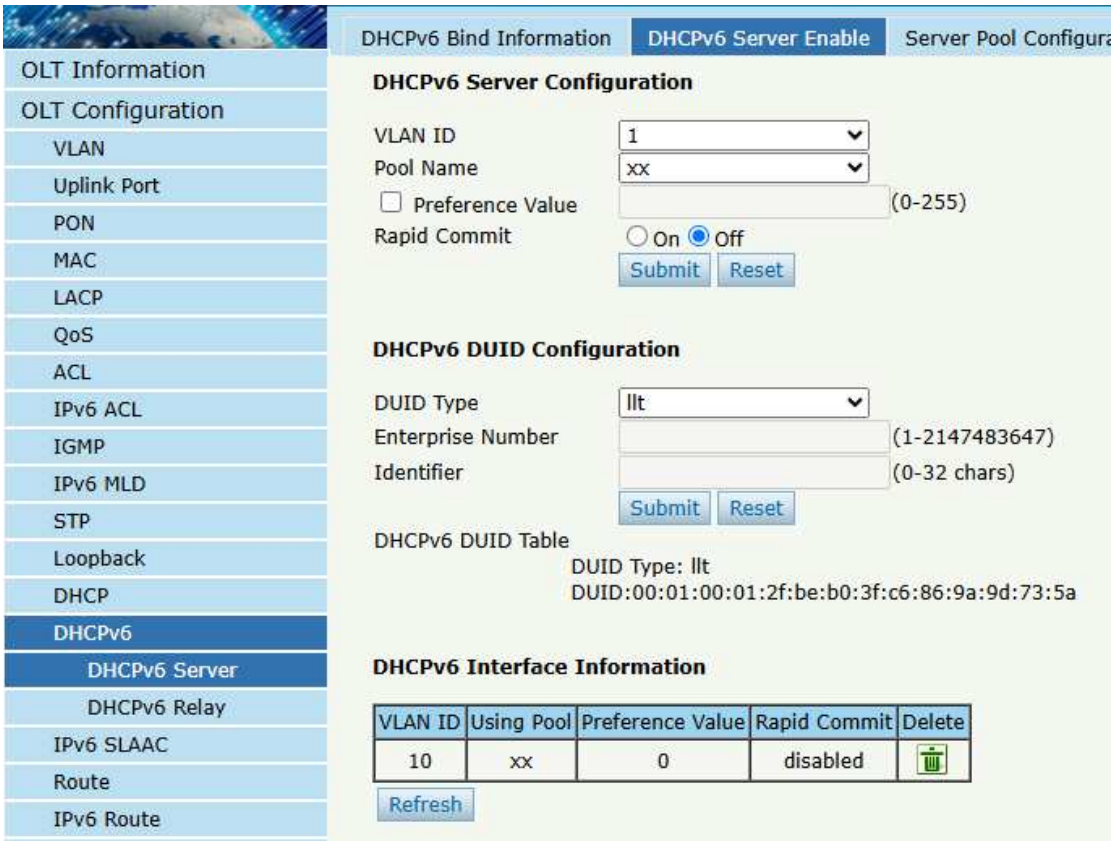


Figure 3.14-2: DHCPv6 Server

3.14.1.3 Server Pool Configuration

OLT Configuration →DHCPv6 → DHCPv6 Server → Server Pool Configuration
DHCPv6 pool specifies the range of assigned IPv6 address. Life time, DNS and domain also can be specified here for DHCPv6 client.

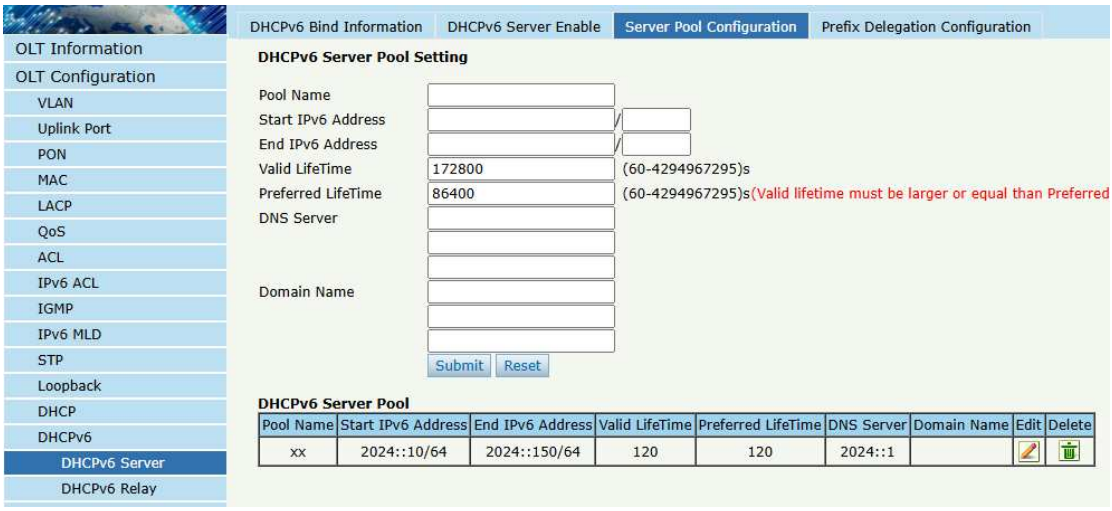


Figure 3.14-3: DHCPv6 Pool Configuration

3.14.1.4 Prefix Delegation Configuration

OLT Configuration → DHCPv6 → DHCPv6 Server → Prefix Delegation Configuration

This page supports configuring DHCPv6 prefix delegation, which can configure the prefix information, PD ValidLifeTime, and PD PreferLifeTime allocated by the DHCPv6 service.

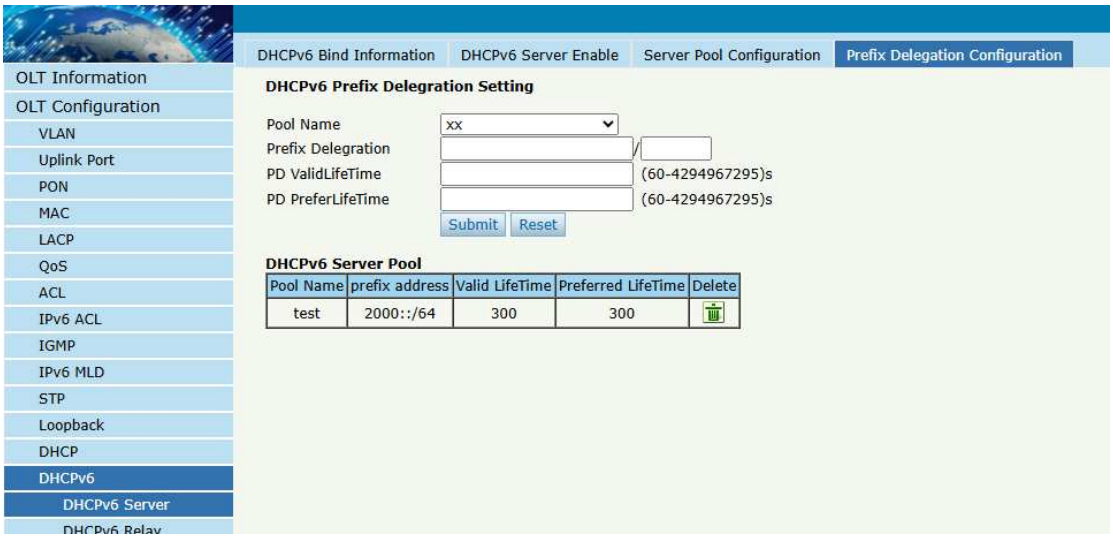


Figure 3.14-4: DHCPv6 Prefix Delegation Configuration

3.14.2 DHCPv6 Relay

OLT Configuration → DHCPv6 → DHCPv6 Relay → Configuration

Option 37 is called the Remote ID Option. After the DHCPv6 Relay device receives the request message sent by the DHCPv6 client to the DHCPv6 server, it adds Option 37 to the message and forwards it to the DHCPv6 server. The server can locate the DHCPv6 client based on the information in Option37 and provide support for allocating IPv6 addresses.

Option 38 is used to carry the physical or logical location information of the client accessing the network. Its function is similar to the Subscriber-ID field of Option 82 in DHCPv4, which is used to identify user or device and supports authentication, billing or policy control.

'VLAN ID' fills in the VLAN you want to relay, 'Server IPv6' fills in the destination DHCPv6 server, and 'Remote id' and 'Subscriber id' fill in the information to be carried in the option 37 field and option 38 field respectively.

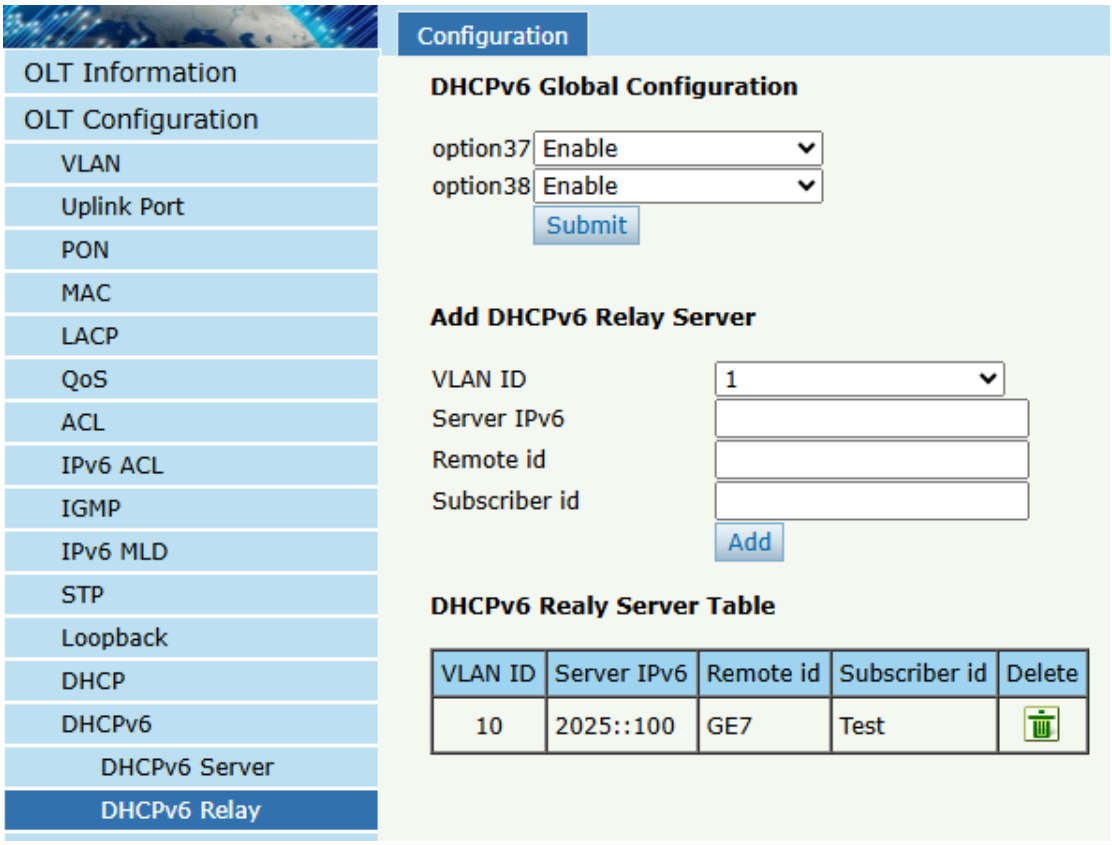


Figure 3.14-5: DHCPv6 Relay

3.15 IPv6 SLAAC

IPv6 network uses the ICMPv6 route discovery protocol. When an IPv6 host connects to the network for the first time, it automatically configures it according to the information got by route discovery/prefix discovery. Route discovery/prefix discovery is that when a host is connected to IPv6 network, it can discover local router and obtain neighbor information, prefix of current network and other configuration parameters from route advertisement (RA) packets.

3.15.1 IPv6 SLAAC

OLT Configuration → IPv6 SLAAC → IPv6 SLAAC

When IPv6 host use SLAAC (Stateless Address Auto Configuration), OLT will send a route advertisement (RA) packet to it. This interface is used to configure parameters of the route advertisement packet.

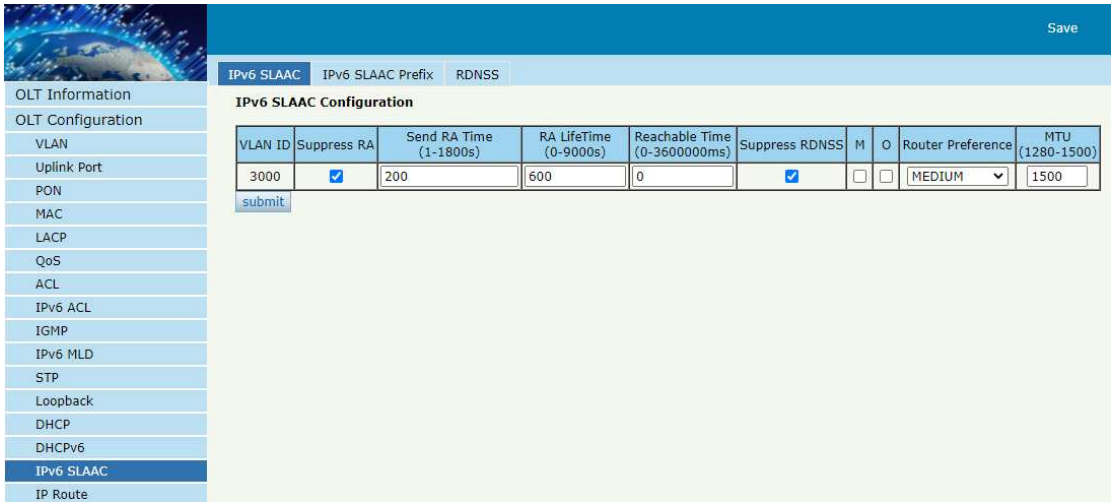


Figure 3.15-1: IPv6 SLAAC

3.15.2 IPv6 SLAAC Prefix

OLT Configuration → IPv6 SLAAC → IPv6 SLAAC Prefix

When IPv6 host uses stateless address auto configuration, OLT can provide IPv6 prefix. The host will generate an IPv6 address with the prefix.

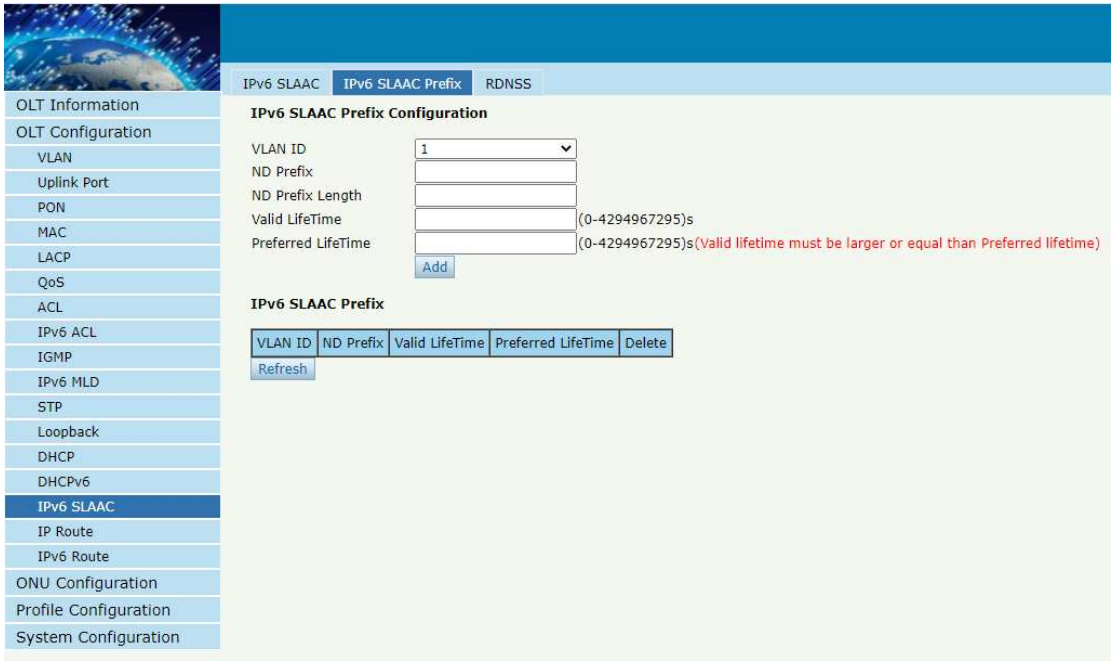


Figure 3.15-2: IPv6 SLAAC Prefix

3.15.3 RDNSS

OLT Configuration → IPv6 SLAAC → RDNSS

OLT will send the route advertisement packet with the DNS parameters you configured.

Figure 3.15-3: RDNSS

3.16 Route

3.16.1 IP

3.16.1.1 VLAN IP

OLT Configuration→Route→IP→VLAN IP

This configuration is used to configure IP address for VLAN. When the VLAN is added to a port, you can access OLT by the IP address from the port. This is in-band management.

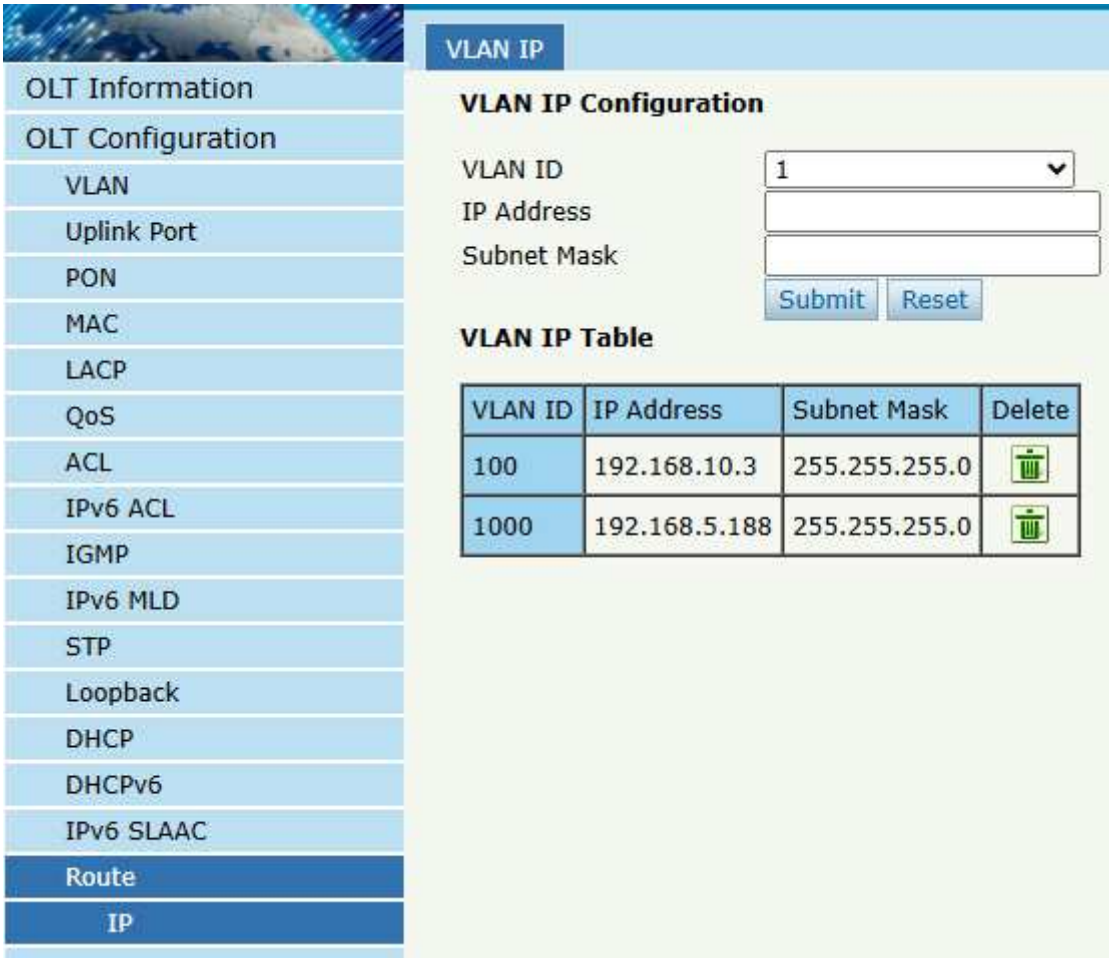


Figure 3.16-1: VLAN IP

3.16.2 Static Route

Static route is a form of routing that a router uses a manually-configured routing entry. In many cases, static routes are manually configured by a network administrator. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured.

OLT Configuration→Route→Static Route

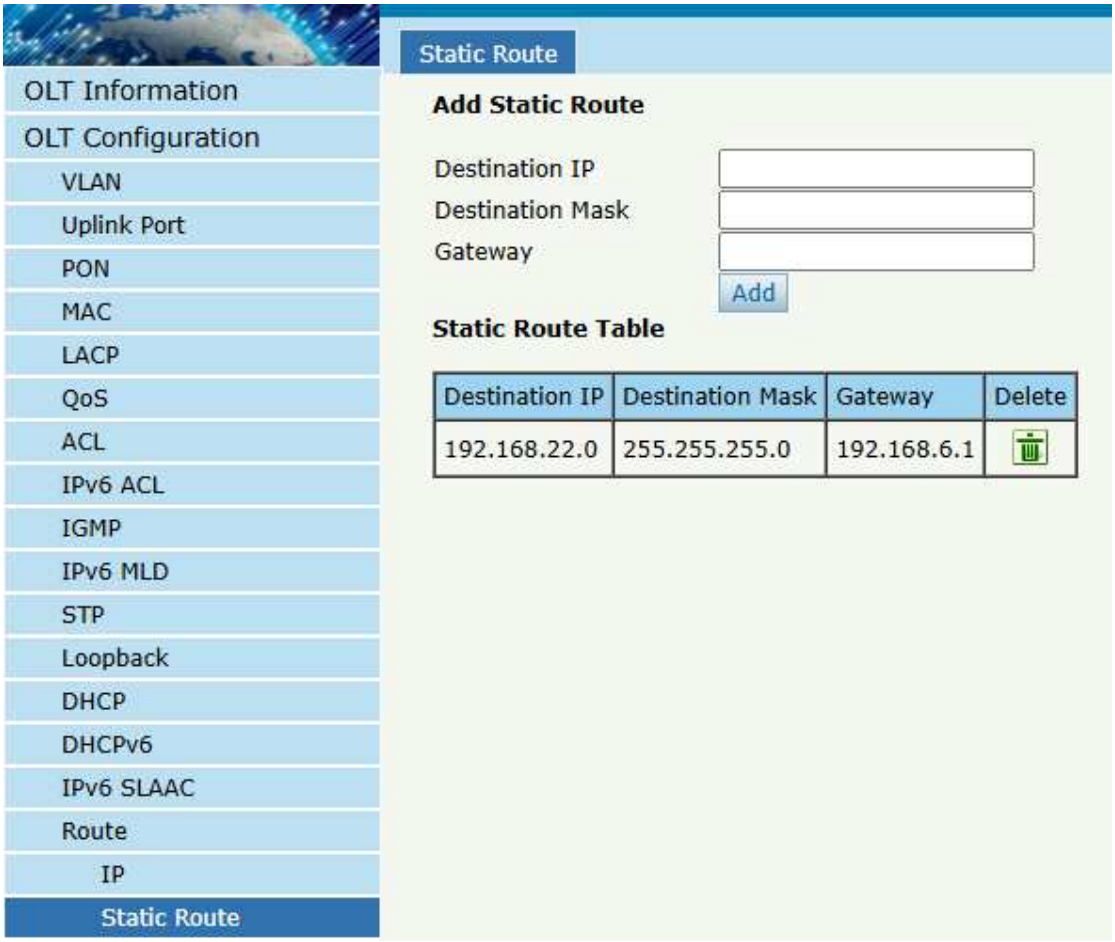


Figure 3.16-2: Static Route

3.16.3 RIP

RIP (Routing Information Protocol) is a simple internal gateway protocol, which is based on the D-V algorithm and uses hop count to represent metric. The hop count is the number of routers that a data-gram must pass through. RIP only support maximum 15 hops; hence it is fit for a small network.

3.16.3.1 RIP Information

OLT Configuration → Route → RIP → RIP Information

This interface displays RIP route table and neighbor routing information.

Illustrations of part parameter:

Parameters	Illustration
Route Type	Display the way to obtain the routing table entries.
Network	Network segment information.
Next Hop	The next-hop address of the target network.

Metric	The metric value (hop count) of the route, with a value range from 1 to 16: 1: Direct connection to the network. 16: Unreachable (The maximum hop count of RIP is 15)
From	The source device of Advertising routing table entry.
Tag	Used to distinguish internal routes from external routes (such as routes redistributed from other protocols).
Time	Routing table entry timeout time.

Table 3.16-1 RIP Route Table

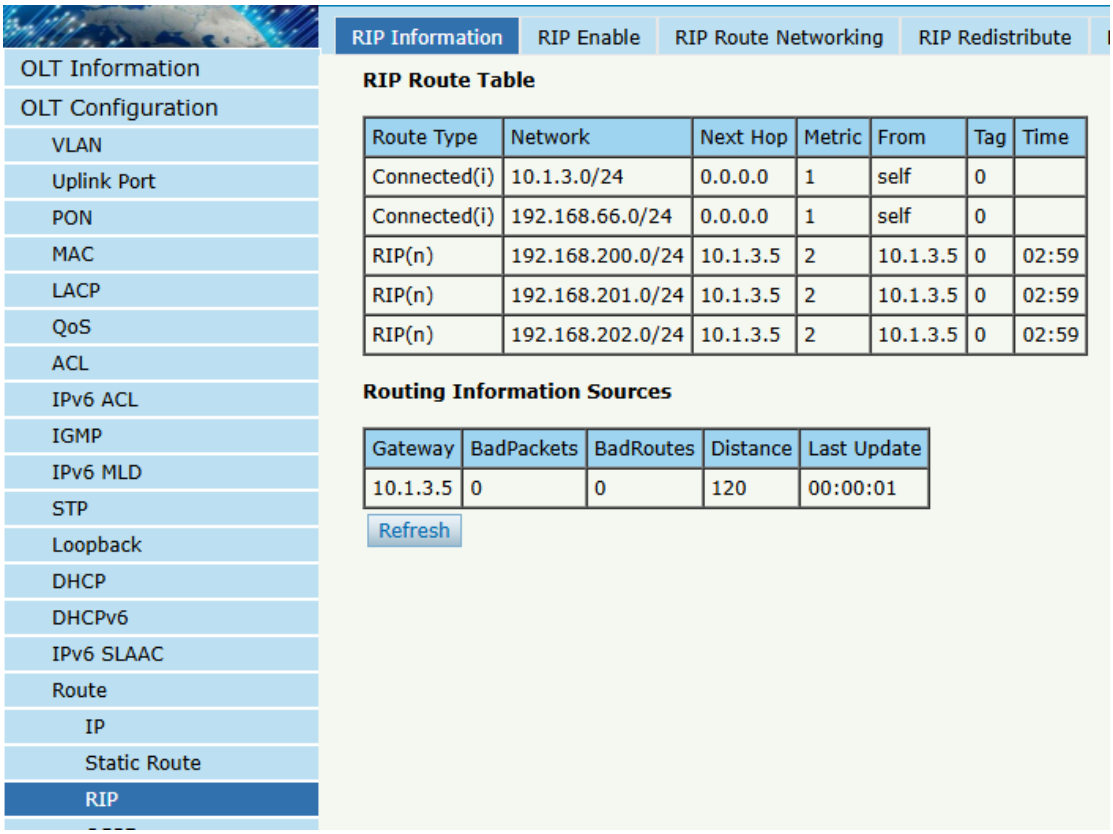


Figure 3.16-3: RIP Information

3.16.3.2 RIP Enable

OLT Configuration → Route → RIP → RIP Enable

Enable RIP protocol and configure RIP parameters.

Illustrations of part parameter:

Parameters	Illustration
RIP Version	RIP has two versions: RIP-1 and RIP-2. RIP-1 is the Classful Routing Protocol, which only supports the publication of protocol messages in a broadcast manner. The protocol message of RIP-1 cannot carry mask information. It

	can only identify the routes of natural network segments such as Class A, B, and C. Therefore, RIP-1 does not support Discontiguous Subnet. RIPv2 supports features such as subnet masks, authentication, and multicast, and is compatible with CIDR.
Update Time	The time interval for sending route updates.If no update message about a certain route is received during the aging time, the metric value of this route in the routing table will be set to 16.
Timeout Time	Routing table entry timeout time.
Garbage Time	The time elapsed from when the metric value of the route changes to 16 to when it is deleted from the routing table. During garbage time, RIP sends the update information of this route with a metric value of 16. If the route is still not updated after the garbage time, it will be completely deleted from the routing table.
Default Metric	Metric is the core parameter for measuring the "cost" of a route in the RIP protocol, measured in terms of Hops. The default metric of the direct connection network is 1, and the maximum effective hop count is 15. Routes with more than 15 hops are marked as unreachable.
Distance	It is the priority identifier of the routing protocol and is used to resolve conflicts among multiple routing protocols. The smaller the management distance value is, the higher the priority of the routing source is. When the OLT learns the routes of the same destination network from multiple routing protocols, it gives priority to the routes with a smaller management distance.

Table 3.16-2 RIP Parameters

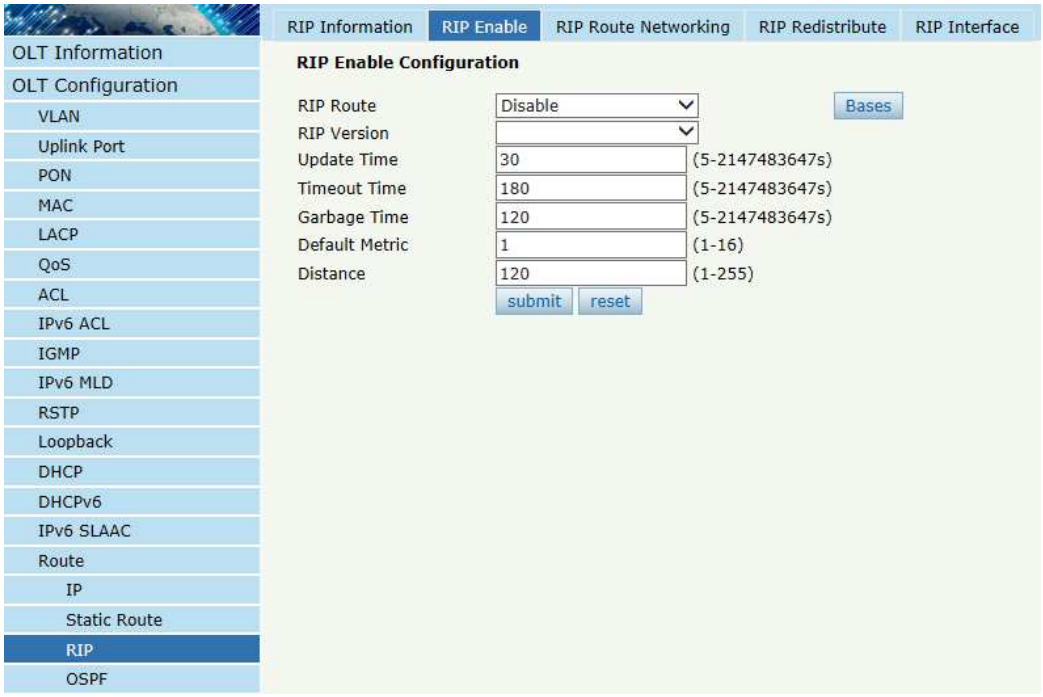


Figure 3.16-4: RIP Enable

3.16.3.3 RIP Route Networking

OLT Configuration → Route → RIP → RIP Route Networking

This interface is used to advertise RIP route networking. VLAN IP address must be set before advertising the VLAN to RIP route networking table.

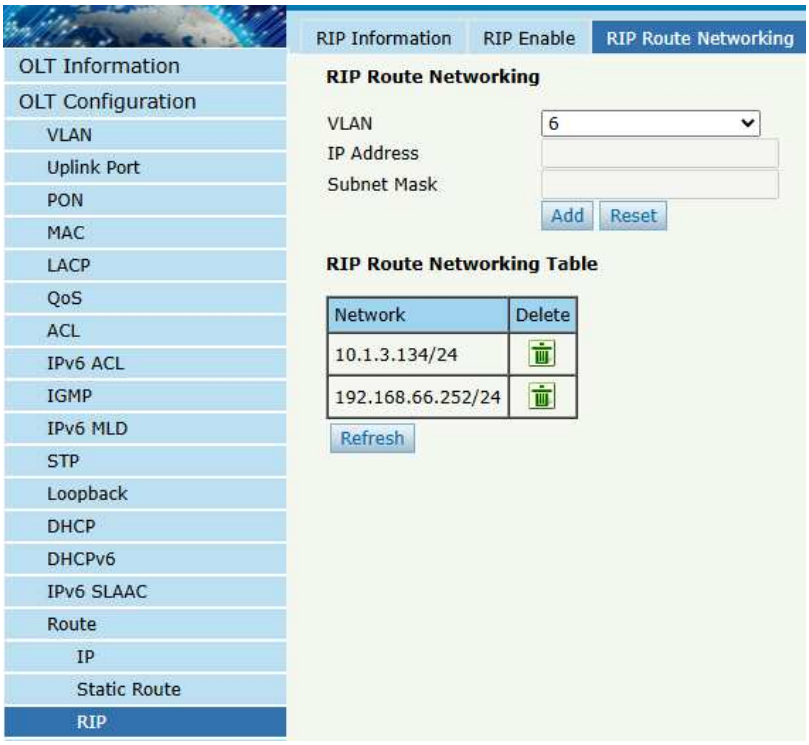


Figure 3.16-5: RIP Route Networking

3.16.3.4 RIP Redistribute

OLT Configuration → Route → RIP → RIP Redistribute.

This page is used to enable or disable route redistribute and choose redistribute mode.

Figure 3.16-6: RIP Redistribute

3.16.3.5 RIP Interface

OLT Configuration → Route → RIP → RIP Interface

This page is used to configure RIP interface and its authentication type. VLAN IP address must be set before configuring RIP interface. And auth chain should be set on page **Key Chain**, refer to section 3.16.5.

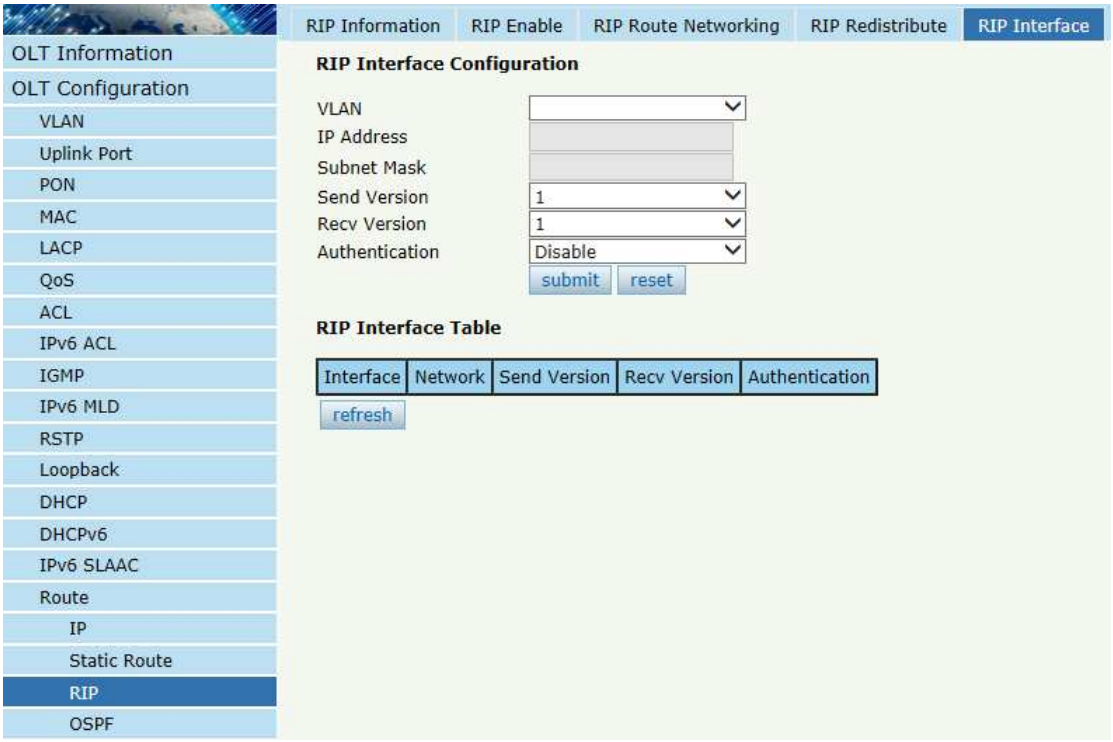


Figure 3.16-7: RIP Interface

3.16.4 OSPF

OSPF (Open Shortest Path First) is an internal gateway protocol based on link state routing protocol. This protocol uses the Dijkstra algorithm to calculate the shortest path to each network, and performs the algorithm to quickly converge to the new loop-free topology when detecting changes in the link (such as link failure).

3.16.4.1 OSPF Information

OLT Configuration → Route → OSPF → OSPF Information

This page displays OSPF information, including neighbor information and OSPF routing information.

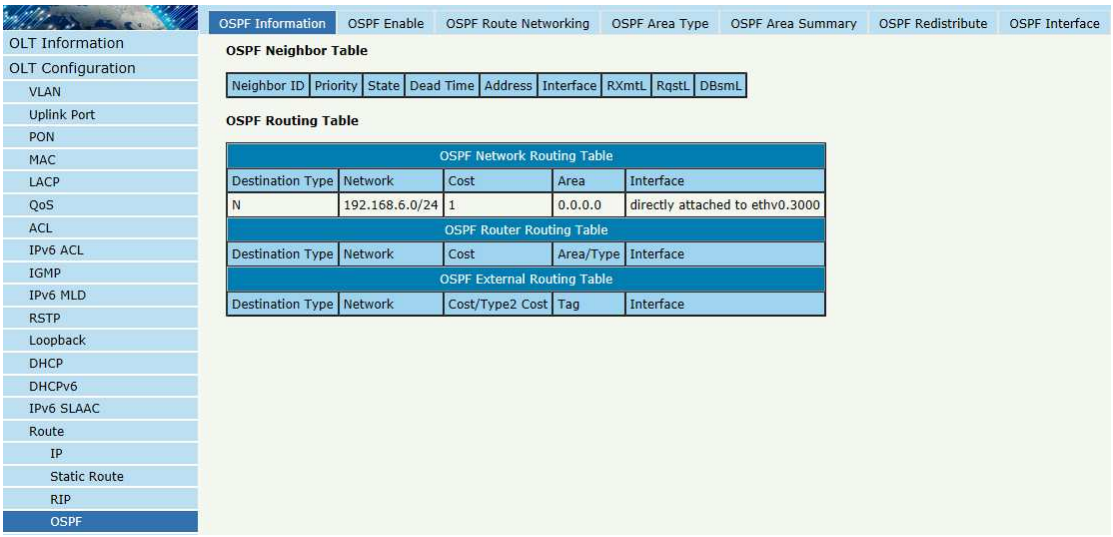


Figure3.16-8: OSPF Information

3.16.4.2 OSPF Enable

OLT Configuration → Route → OSPF → OSPF Enable

This page is used to enable OSPF. Fill in route ID and let it blank, enable OSPF. OLT will use the biggest IP address as route ID if it's blank.

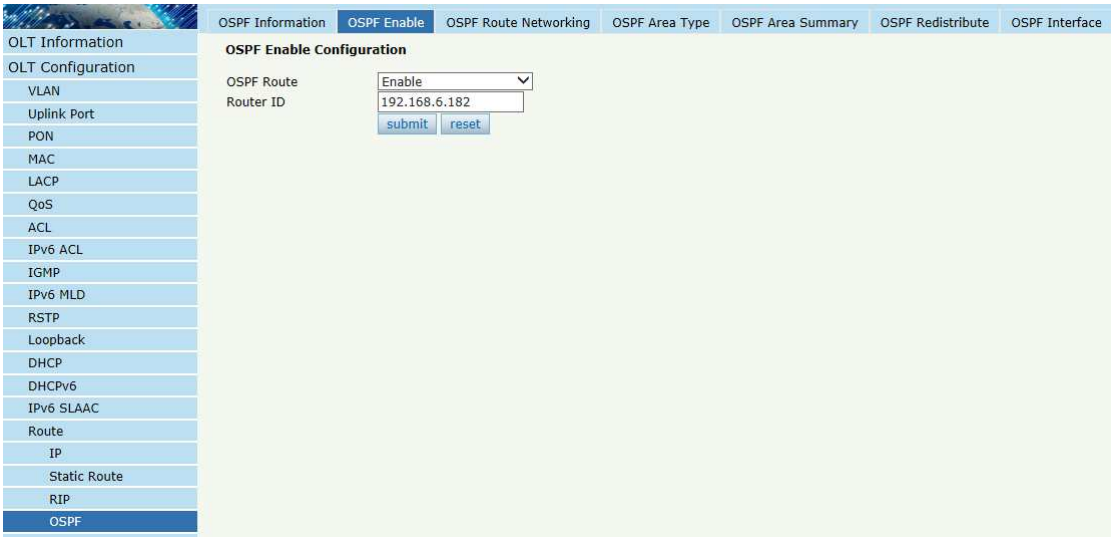


Figure 3.16-9: OSPF Enable

3.16.4.3 OSPF Route Networking

OLT Configuration → Route → OSPF → OSPF Route Networking

This page is used to configure area number for VLAN where OSPF protocol is operating.

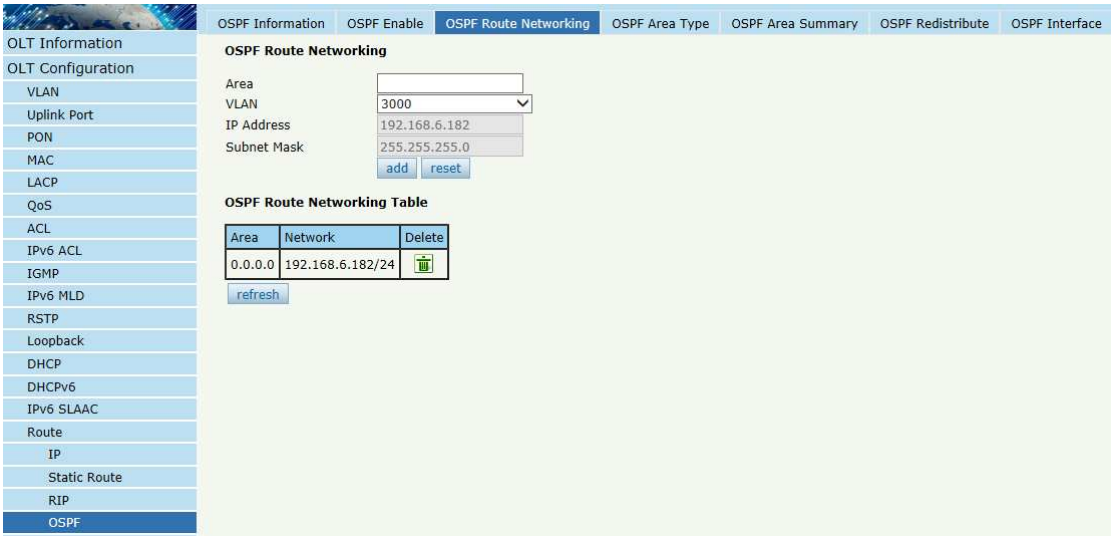


Figure 3.16-10: OSPF Route Networking

3.16.4.4 OSPF Area Type

OLT Configuration → Route → OSPF → OSPF Area Type

This page is used to configure area type. Backbone area will not display on this page.

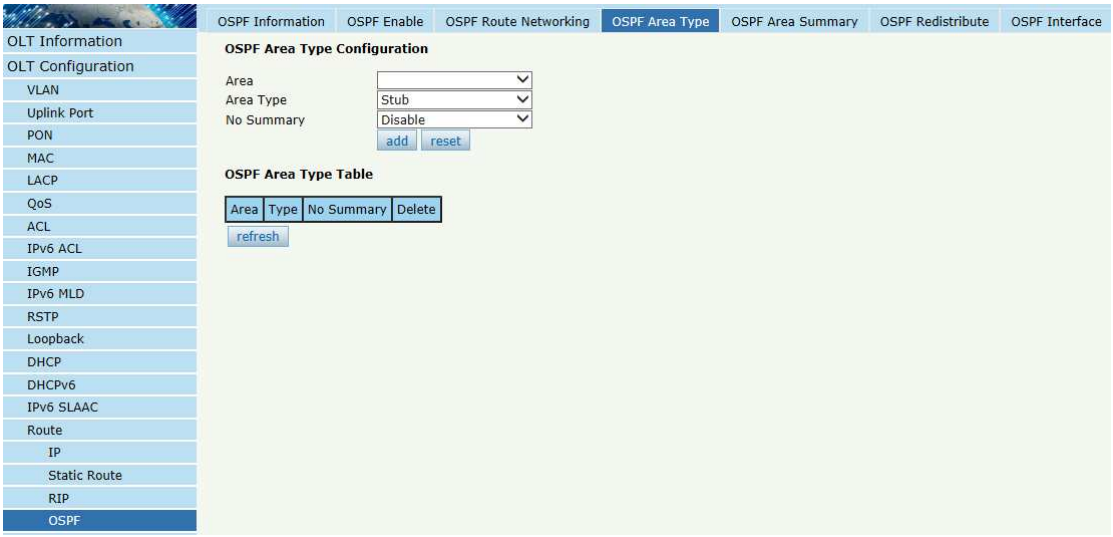


Figure 3.16-11: OSPF Area Type

3.16.4.5 OSPF Area Summary

OLT Configuration → Route → OSPF → OSPF Area Summary

This page is used to configure area IP address summary.

Figure 3.16-12: OSPF Area Summary

3.16.4.6 OSPF Redistribute

The router can use route redistribution to broadcast the OSPF routing it learns through another routing protocol so that several routing protocols can cooperate with each other in a network.

OLT Configuration → Route → OSPF → OSPF Redistribute

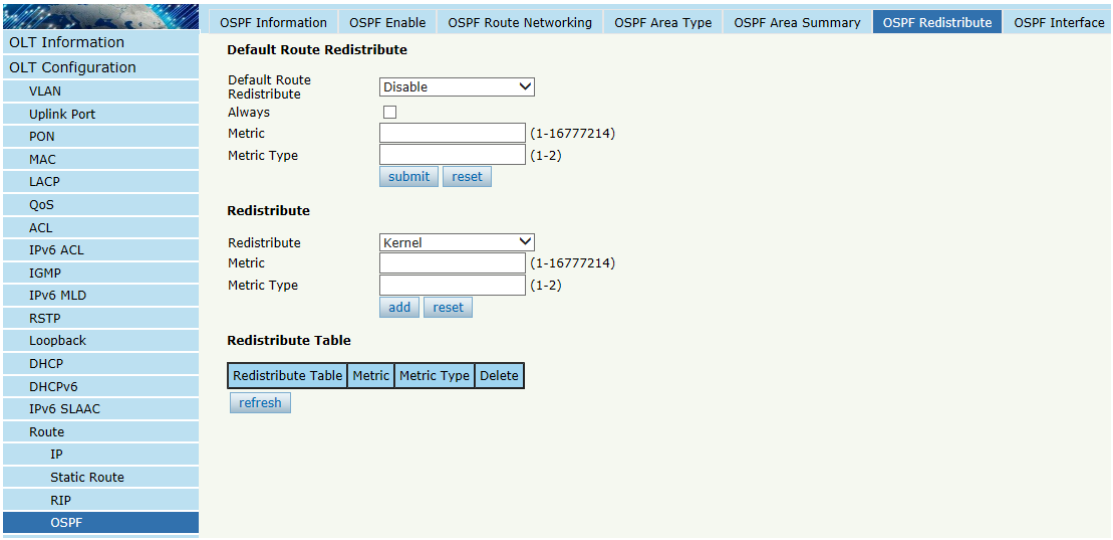


Figure 3.16-13: OSPF Redistribute

3.16.4.7 OSPF Interface

OLT Configuration → Route → OSPF → OSPF Interface

This page is used to OSPF interface parameters such as cost, time, priority, authentication, and so on.

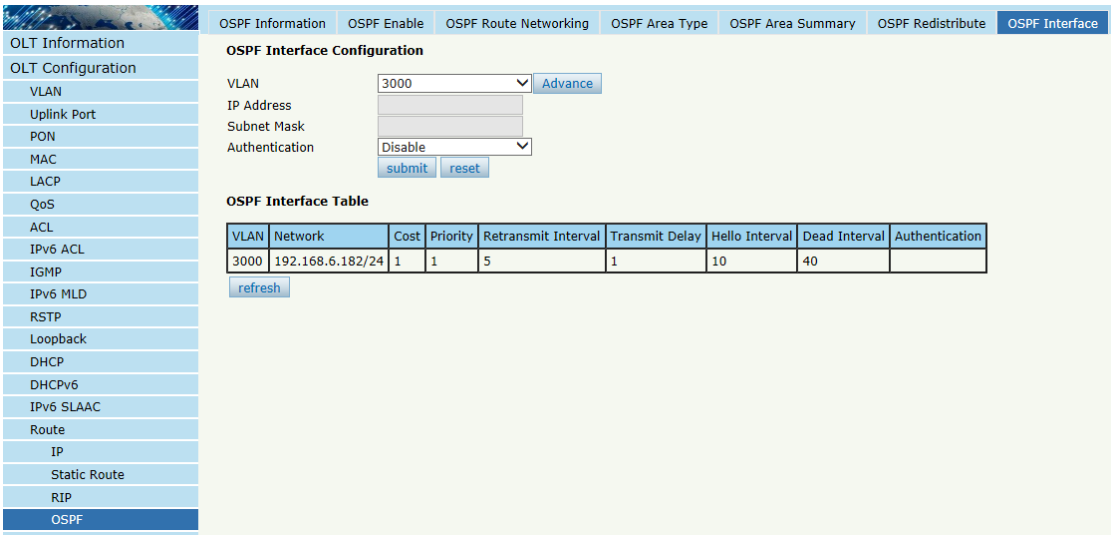


Figure 3.16-14: OSPF Interface

3.16.5 Key Chain

Key management is a method of controlling the authentication key used by routing protocols. The authentication key is available for EIGRP and RIP version 2. To manage the authentication key needs a key chain. Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

OLT Configuration → Route → Key Chain

Figure 3.16-15: Key Chain

3.16.6 Route Table

OLT Configuration → Route → Route Table

This page displays routing items of OLT.

Figure 3.16-16: Route Table

3.17 IPv6 Route

3.17.1 IPv6

OLT Configuration → IPv6 Route → IPv6 → VLAN IPv6
Configure IPv6 address for VLAN that has been created.

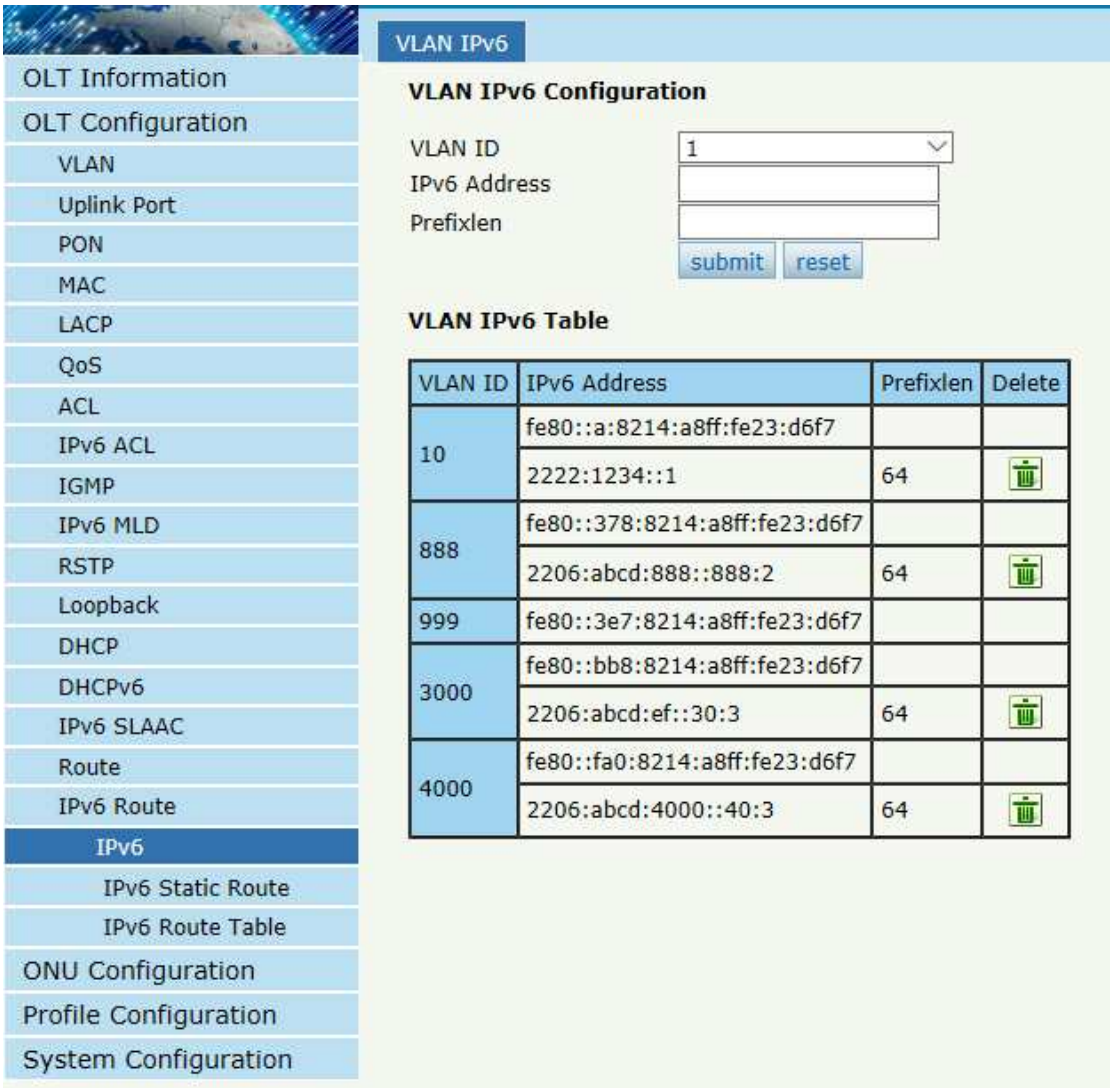


Figure 3.17-1: VLAN IPv6

3.17.2 IPv6 Static Route

Static route is added manually. It will not change even the situation and network topology has been changed.

OLT Configuration → IPv6 Route → IPv6 Static Route

Add IPv6 static route item one by one.

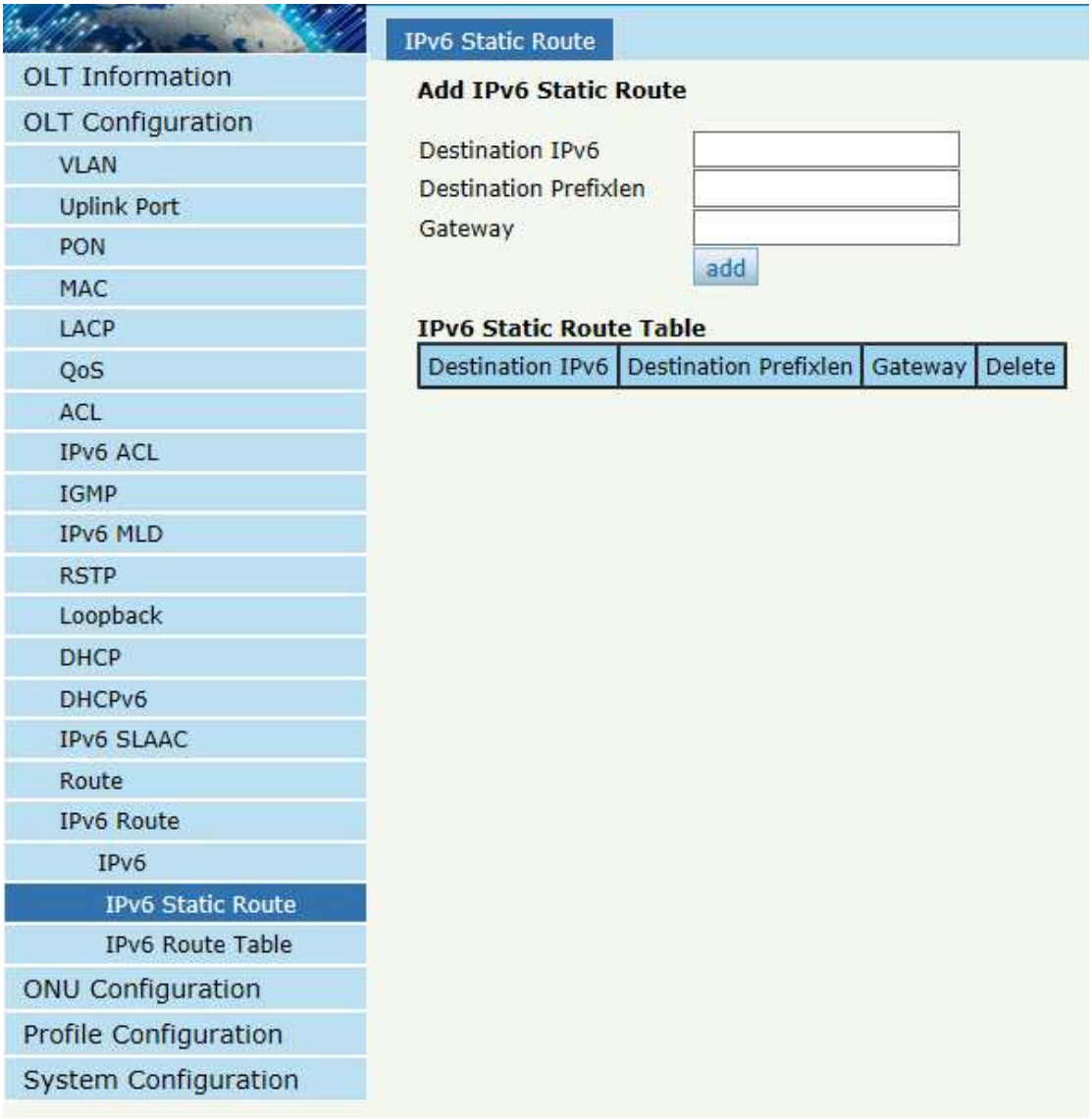


Figure 3.17-2: IPv6 Static Route

3.17.3 RIPng

RIPng (RIP next generation) is an extension of the RIPv2 protocol in the original IPv4 network. Most RIP concepts can be applied to RIPng.

3.17.3.1 RIPng Information

OLT Configuration → IPv6 Route → RIPng →RIPng Information

This page will display RIPng routing table information, including Route Type Network, Next Hop, Via, Metric, Tag, Time and so on.

Figure 3.17-3: RIPng Information

3.17.3.2 RIPng Enable

OLT Configuration → IPv6 Route → RIPng →RIPng Enable

This page is used to switch RIPng routing and modify some related parameters, including Update Time, Timeout Time, Garbage Time, and Default Metric.

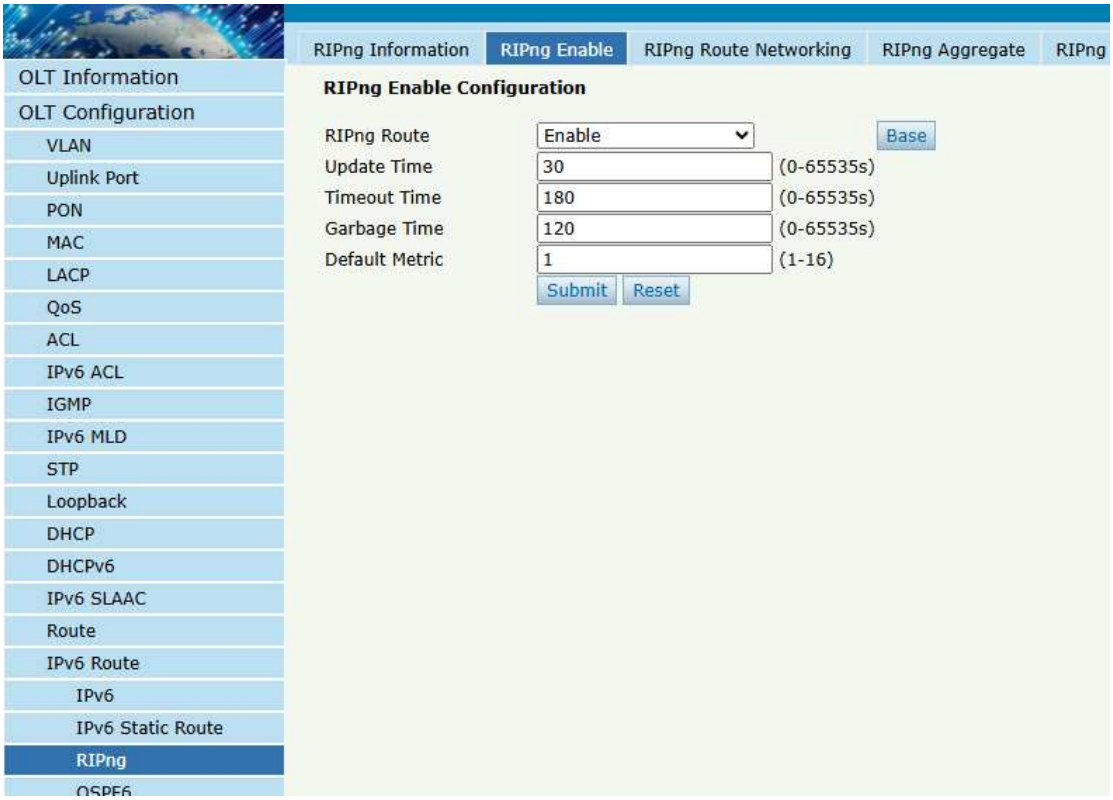


Figure 3.17-4: RIPng Enable

3.17.3.3 RIPng Route Networking

OLT Configuration → IPv6 Route → RIPng →RIPng Route Networking

This page is used to add RIPng routing network. Before adding a VLAN to the RIPng routing network table, the VLAN IPv6 address must be set first.

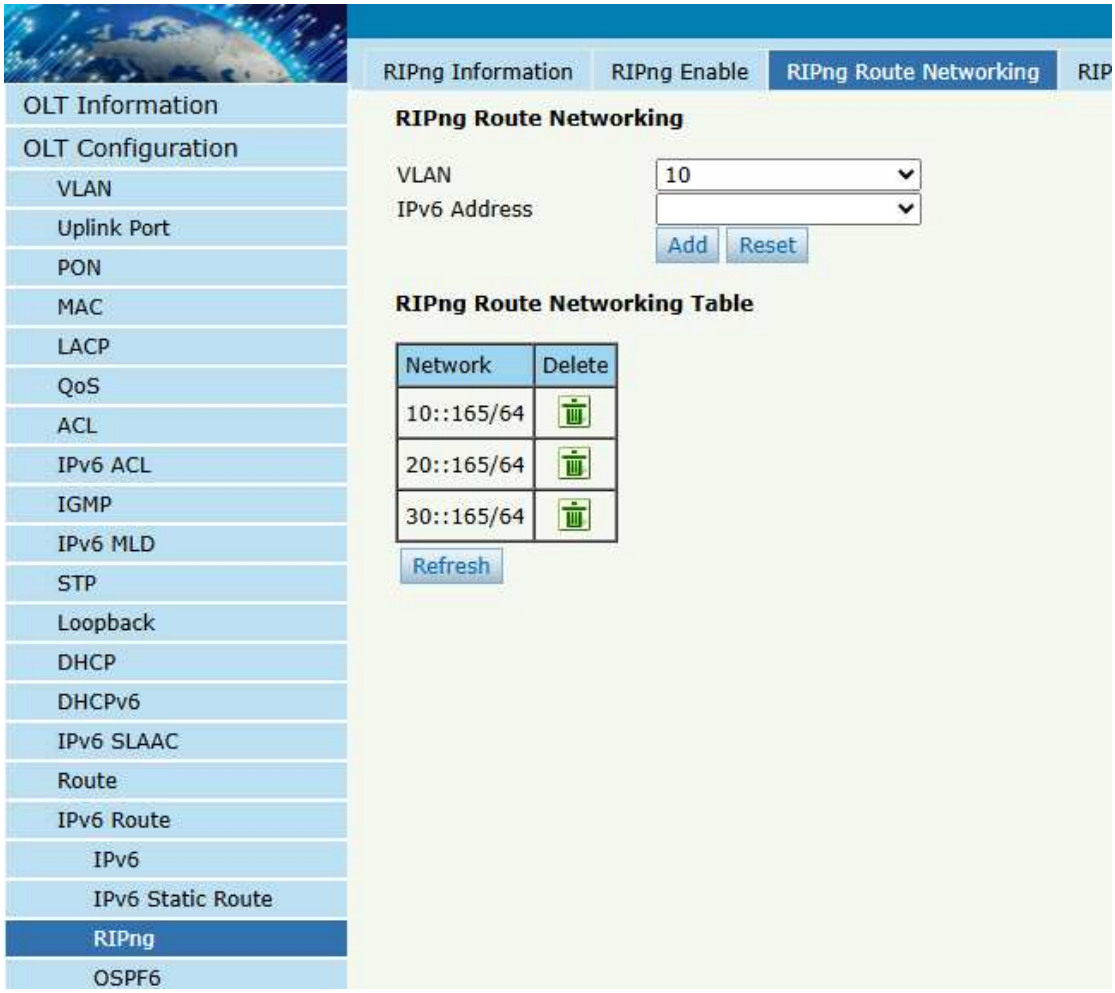


Figure 3.17-5: RIPng Route Networking

3.17.3.4 RIPng Aggregate

OLT Configuration → IPv6 Route → RIPng →RIPng Aggregate

This page supports configuring route aggregation on the interface, which can aggregate the routes that RIPng wants to publish on this interface according to the longest matching principle and publish them. It can improving the scalability and efficiency of the network and reducing the routing table.

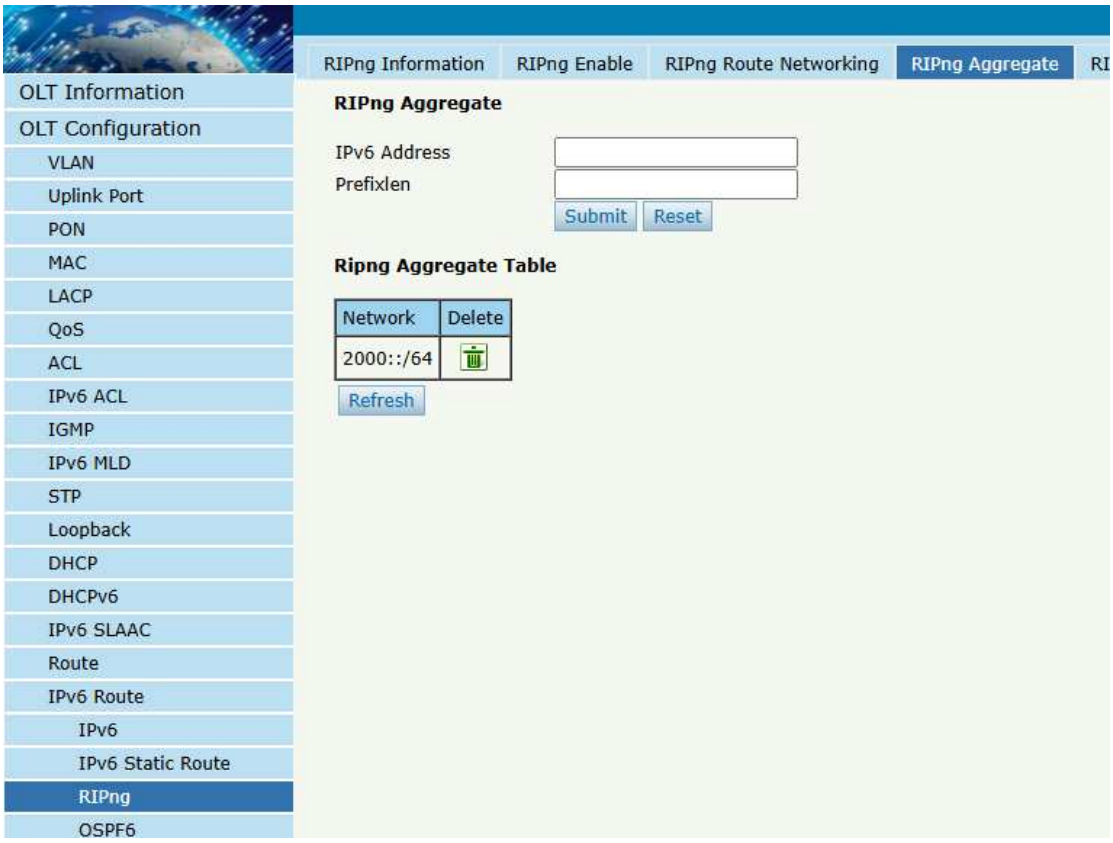


Figure 3.17-6: RIPng Aggregate

3.17.3.5 RIPng Redistribute

OLT Configuration → IPv6 Route → RIPng →RIPng Redistribute

This page is used to enable or disable default route redistribute and select redistribute modes, including Kernel, Connect, Static, OSPF6, the Metric ranging from 0-16.

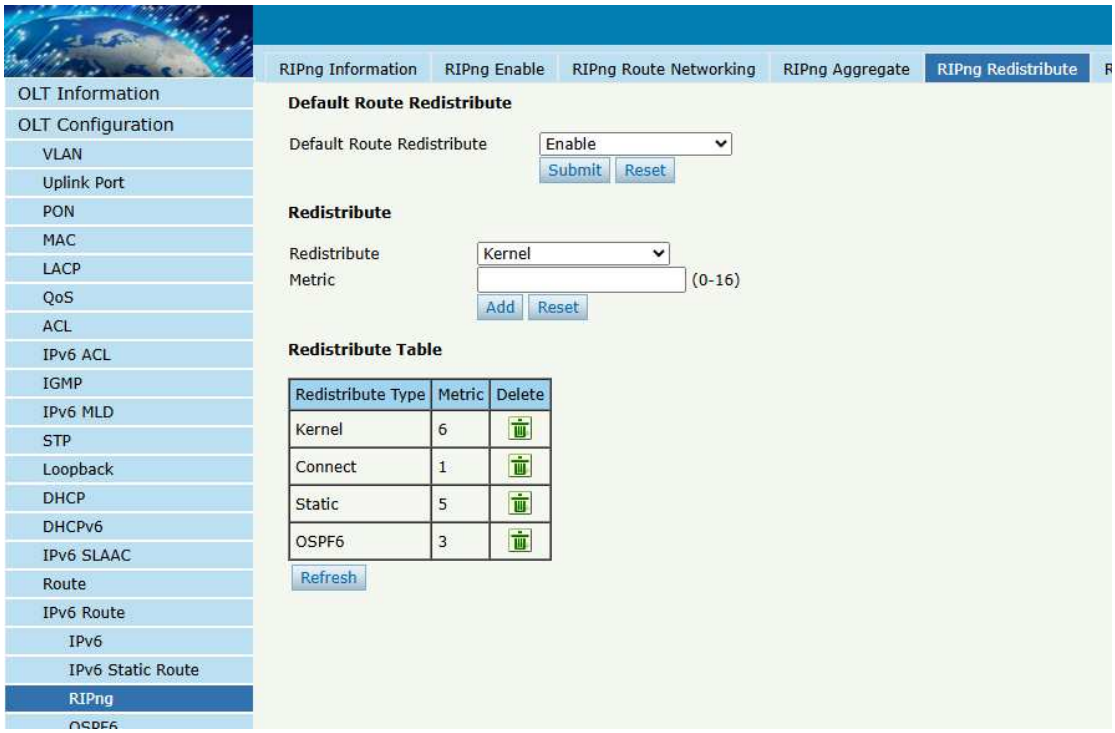


Figure 3.17-7: RIPng Redistribute

3.17.3.6 RIPng Interface

OLT Configuration → IPv6 Route → RIPng →RIPng Interface

This page supports configuring RIPng interface to enable split-horizon and poisoned-reverse.

split-horizon: The routing update information received by the router from a certain interface will not be transmitted back to the source neighbor device through the same interface. For example, after R1 sends routing information to R2 through interface A, R2 will not transmit the same routing information back to R1 through interface A.

poisoned-reverse: When a router receives routing update information from an interface, it will set the hop count (Metric) of the corresponding route to 16 (unreachable) and send it back to the neighboring device via the original interface. For example, after R2 receives the routing information from R1, it will send the update of this route with Metric=16 to R1.

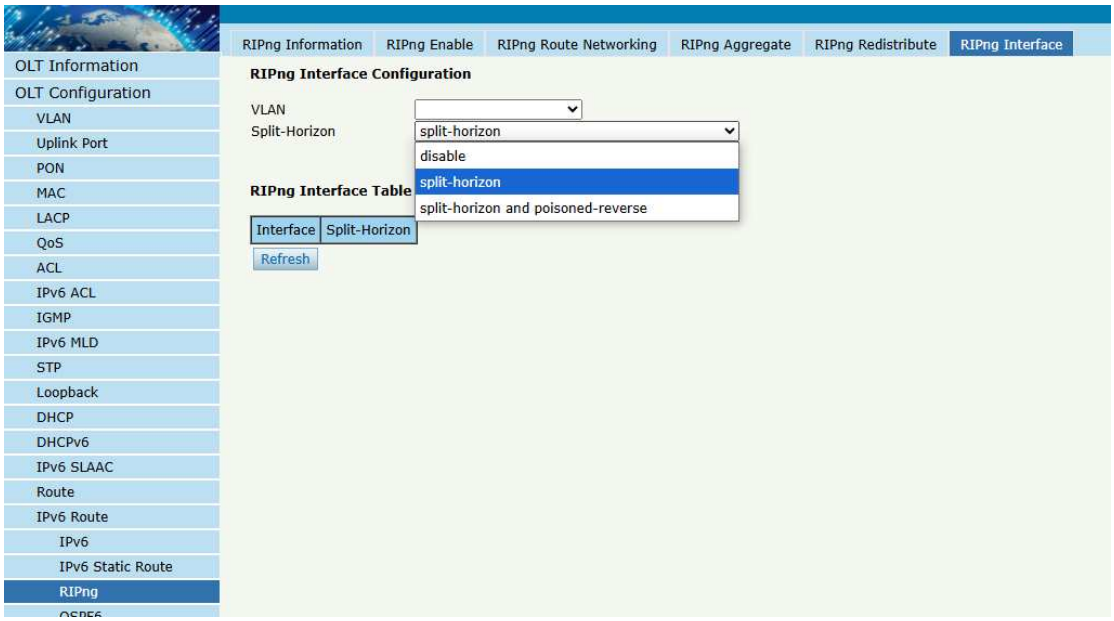


Figure 3.17-8: RIPng Interface

3.17.4 OSPF6

3.17.4.1 OSPF6 Information

OLT Configuration → IPv6 Route →OSPF6→OSPF6 Information

This interface is used to display the neighbor table and routing table discovered by OLT through OSPFv3.

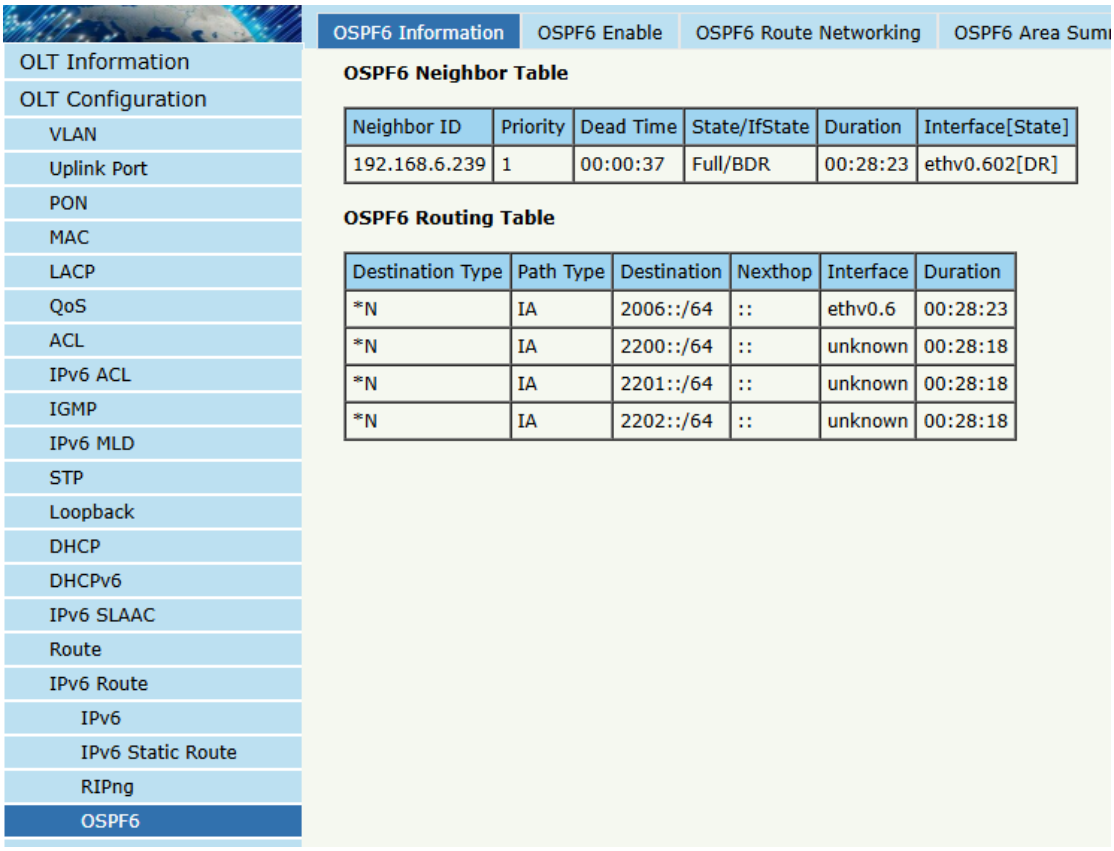


Figure 3.17-9: OSPF6 Routing Table

3.17.4.2 OSPF6 Enable

OLT Configuration → IPv6 Route →OSPF6→OSPF6 Enable

This interface is used to configure the OSPFv3 function switch and Router ID. The Router ID is a 32-bit unsigned integer in the form of IPv4 address and is the unique identifier of a switch in an autonomous system. The Router ID of OSPFv3 must be configured manually. If the ID number is not configured, OSPFv3 cannot operate normally.

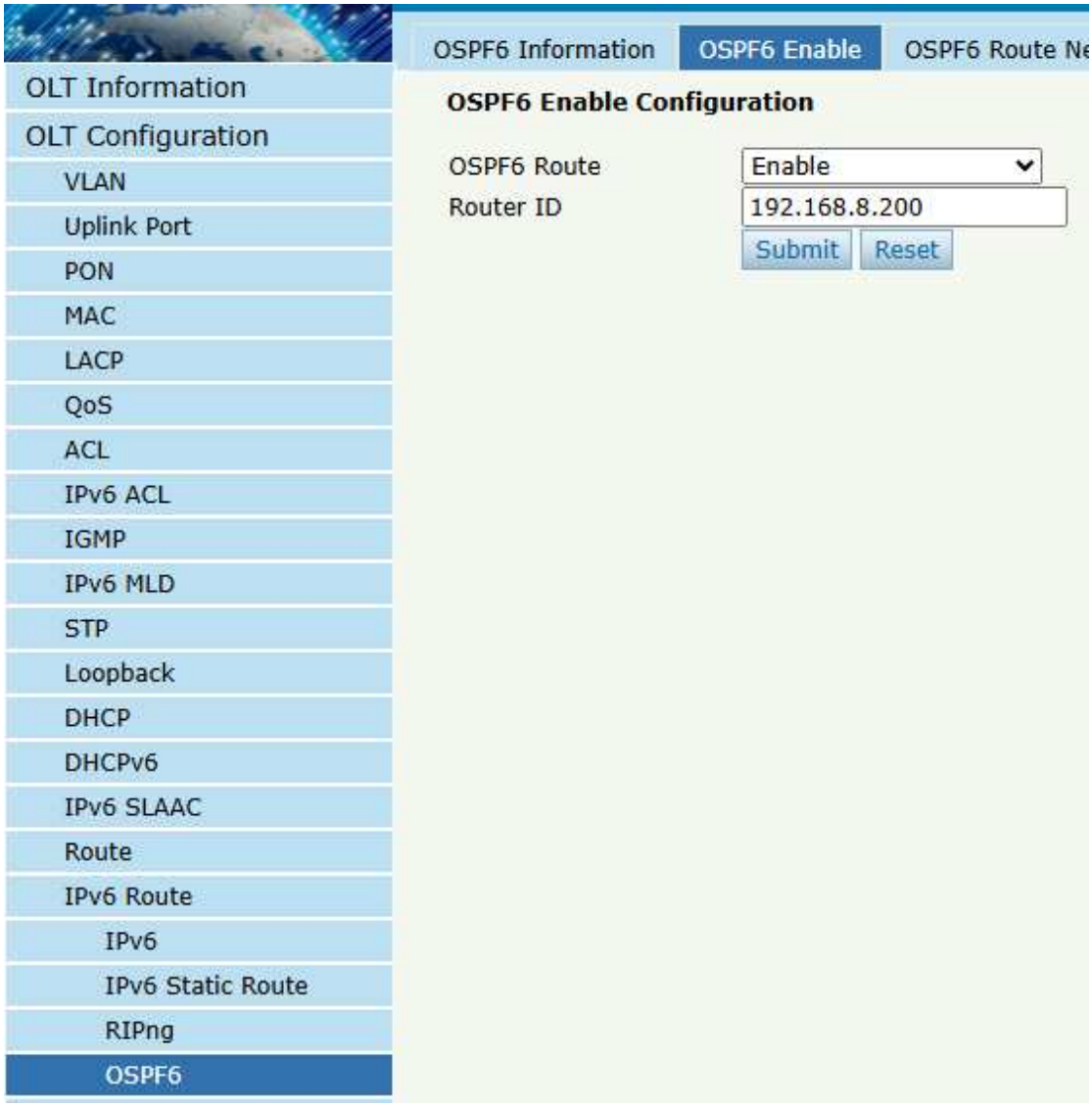


Figure 3.17-10: OSPF6 Enable Configuration

3.17.4.3 OSPF6 Route Networking

OLT Configuration → IPv6 Route →OSPF6→OSPF6 Route Networking
This interface is used to advertise the network directly connected to this OLT.
The prerequisite is that the VLAN IP needs to be configured for the declared VLAN.

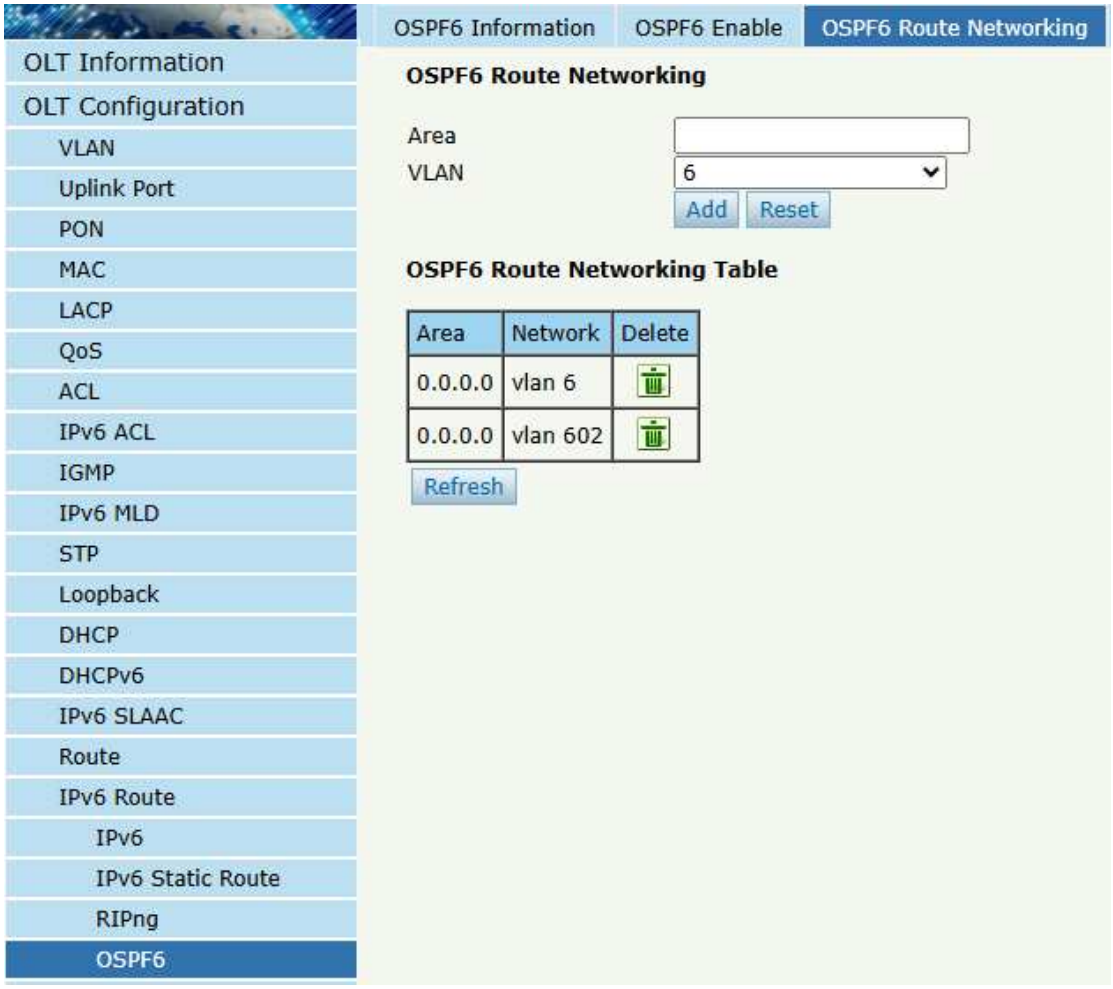


Figure 3.17-11: OSPF6 Route Networking

3.17.4.4 OSPF6 Area Summary

OLT Configuration → IPv6 Route →OSPF6→OSPF6 Area Summary

This interface is used to configure OSPFv3 route summary. If there are multiple consecutive network segments in an area, a routing summary can be configured on the Area Border Router (ABR) to summarize them into one network segment. The ABR will then only send a single summarized LSA. All LSA that fall within the range of the summarized network segment specified by this rule will no longer be sent separately, which can reduce the size of the LSDB in other areas.

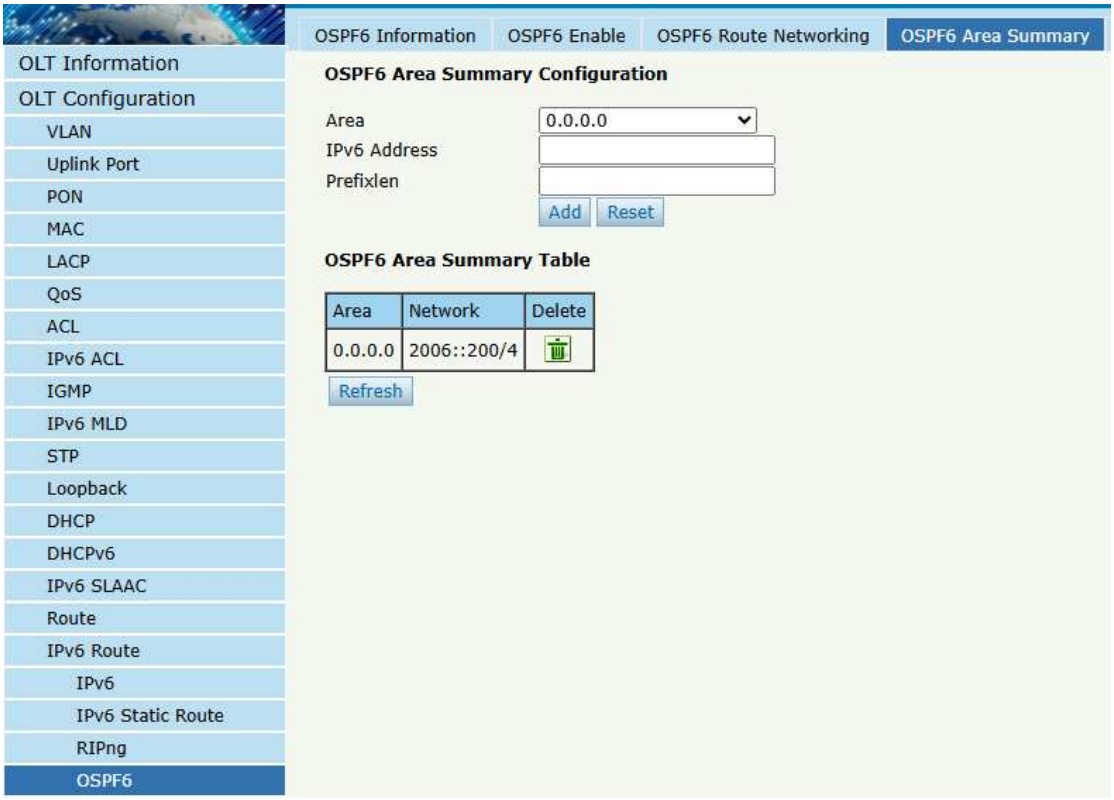


Figure 3.17-12: OSPF6 Area Summary

3.17.4.5 OSPF6 Redistribute

OLT Configuration → IPv6 Route →OSPF6→OSPF6 Redistribute

OLT supports the routing redistribution feature, which can introduce the routing information learned by other routing protocols into the OSPFv3 area, allowing the exchange of information between different routing protocols and achieving network intercommunication.

Figure 3.17-13: OSPF6 Redistribute

3.17.4.6 OSPF6 Interface

OLT Configuration → IPv6 Route →OSPF6→OSPF6 Interface

The interface function configures the OSPFv3 protocol parameters, which take effect on different networks according to different VLAN.

Illustrations of part parameter:

Parameters	Illustration
Retransmit Interval	Configure the interval for adjacent routers to Retransmit LSA.
Transmit Delay	Configure the LSA transmission delay of the interface.
Hello Interval	Configure the interval for the interface to send OSPFv3 Hello packets to discover neighbors and maintain relationships.
Dead Interval	Configure the aging time of the router neighbor table.
Priority	Configure the DR Priority of the interface. The DR Priority of the Router interface will affect the eligibility of the interface when electing DR(Designated Router). Routers with a priority of 0 will not be elected as DR or BDR(Backup Designated Router).

Table 3.17-1 OSPFv3 Parameters

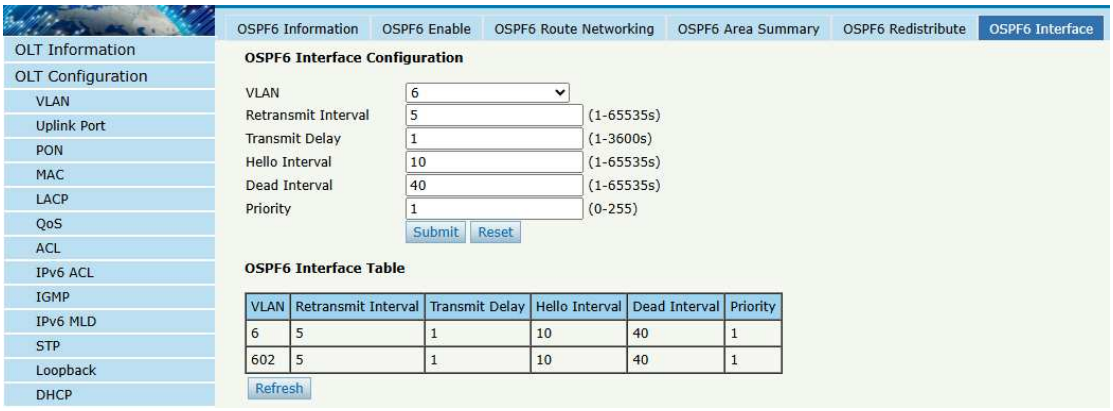


Figure 3.17-14: OSPF6 Interface

3.17.5 IPv6 Route Table

OLT Configuration → IPv6 Route → IPv6 Route Table

This table displays all IPv6 route items of the device, including static route and dynamic route.

Figure 3.17-15: IPv6 Route Table

3.18 ARP Security

3.18.1 Dynamic ARP Inspection

OLT Configuration → ARP Security → Dynamic ARP Inspection

Dynamic ARP Inspection, used to monitor ARP packets under VLAN and prevent ARP attack behavior. After enabling this function, only trust ports can forward ARP packets corresponding to VLAN.

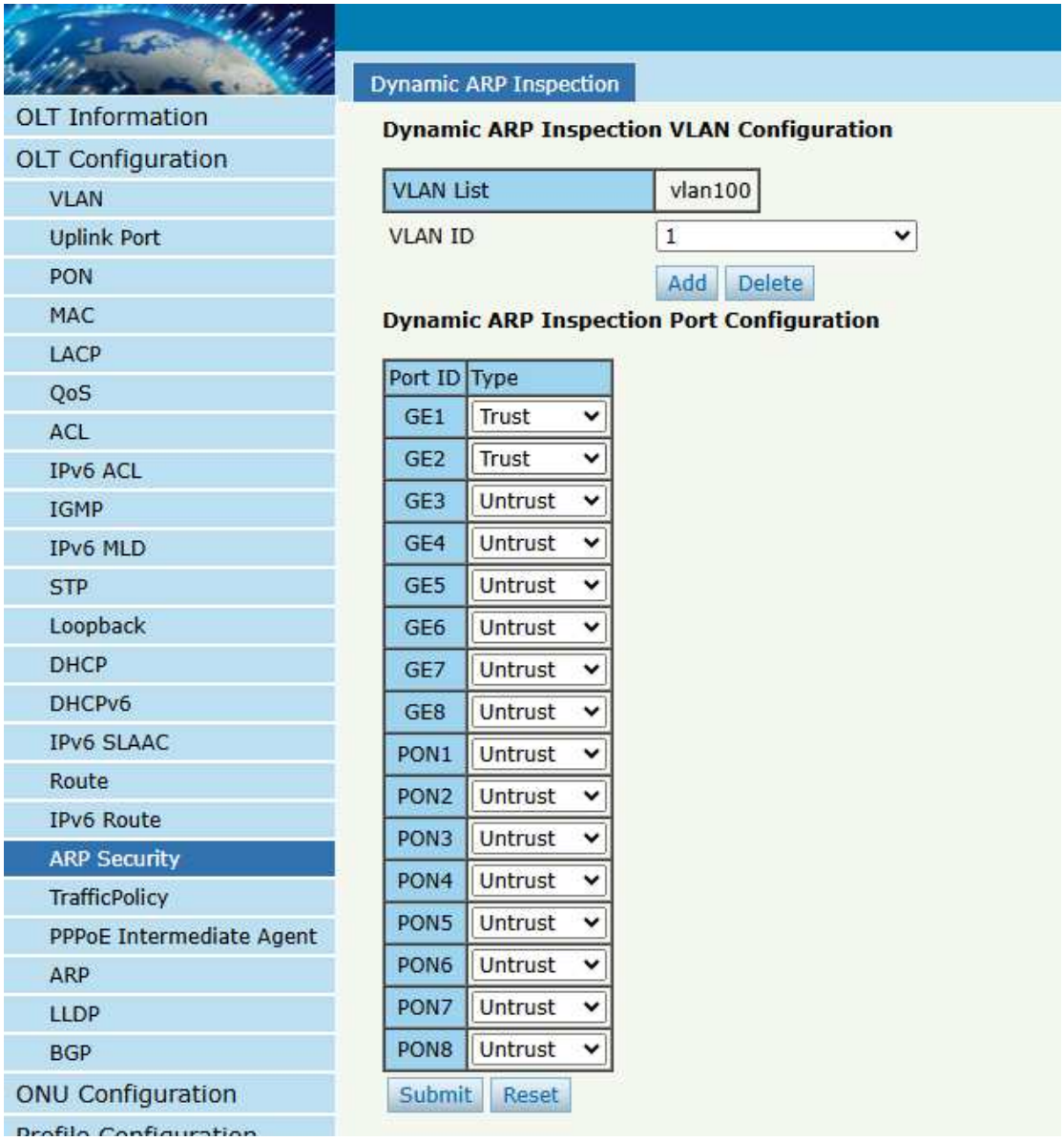


Figure 3.18-1: Dynamic ARP Inspection

3.19 TrafficPolicy

3.19.1 Policy

OLT Configuration → TrafficPolicy→ Policy

A Policy is created by binding classifier and behavior together, which can achieve the effect of matching a classifier with a certain behavior in the traffic entering a certain port. This process is called a Policy.

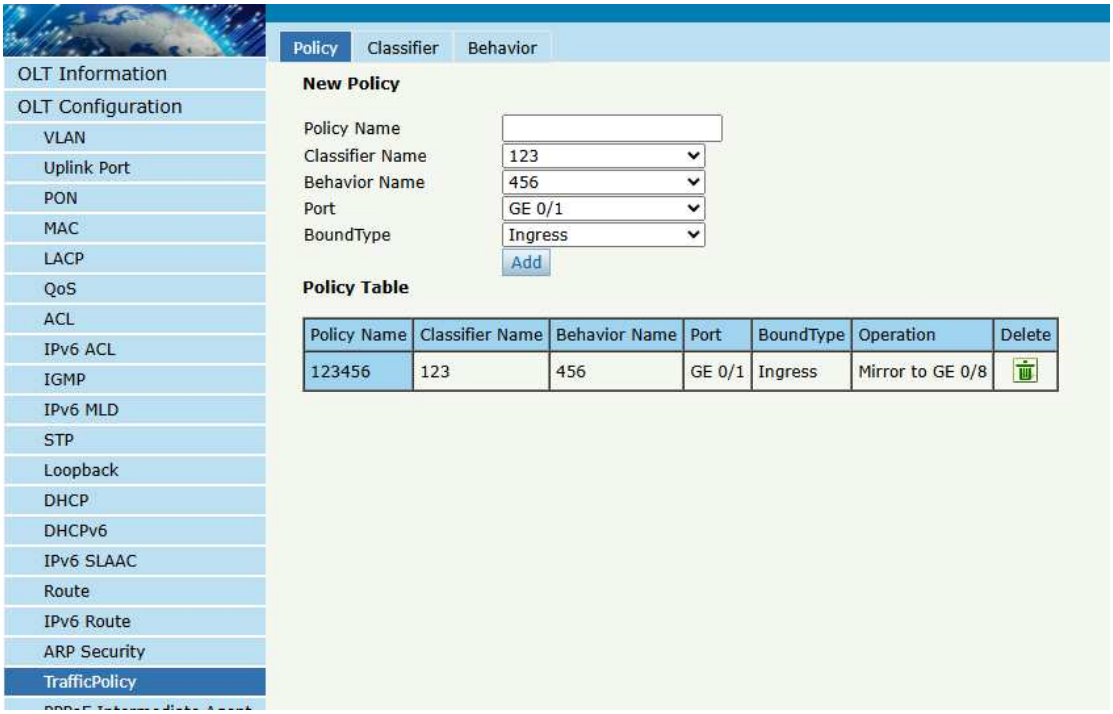


Figure 3.19-1: Policy

3.19.2 Classifier

OLT Configuration → TrafficPolicy→ Classifier

Classifier is created through ACL rules, which can specify the matching information you want, such as IP address and MAC address.

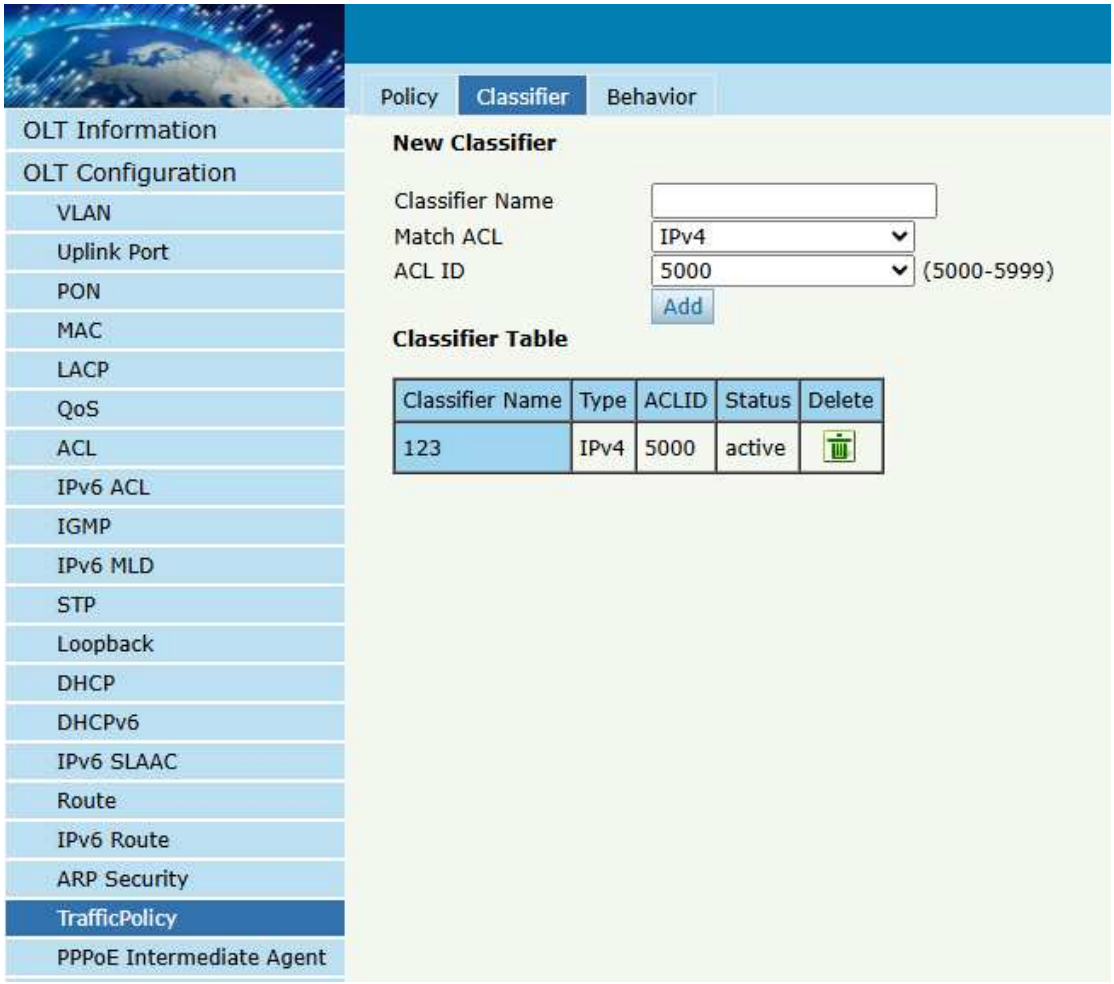


Figure 3.19-2: Classifier

3.19.3 Behavior

OLT Configuration → TrafficPolicy→ Behavior

Behavior can perform many operations, such as mirroring, speed limiting, remark DSCP, and remark 802.1p, etc. Choose according to actual needs.

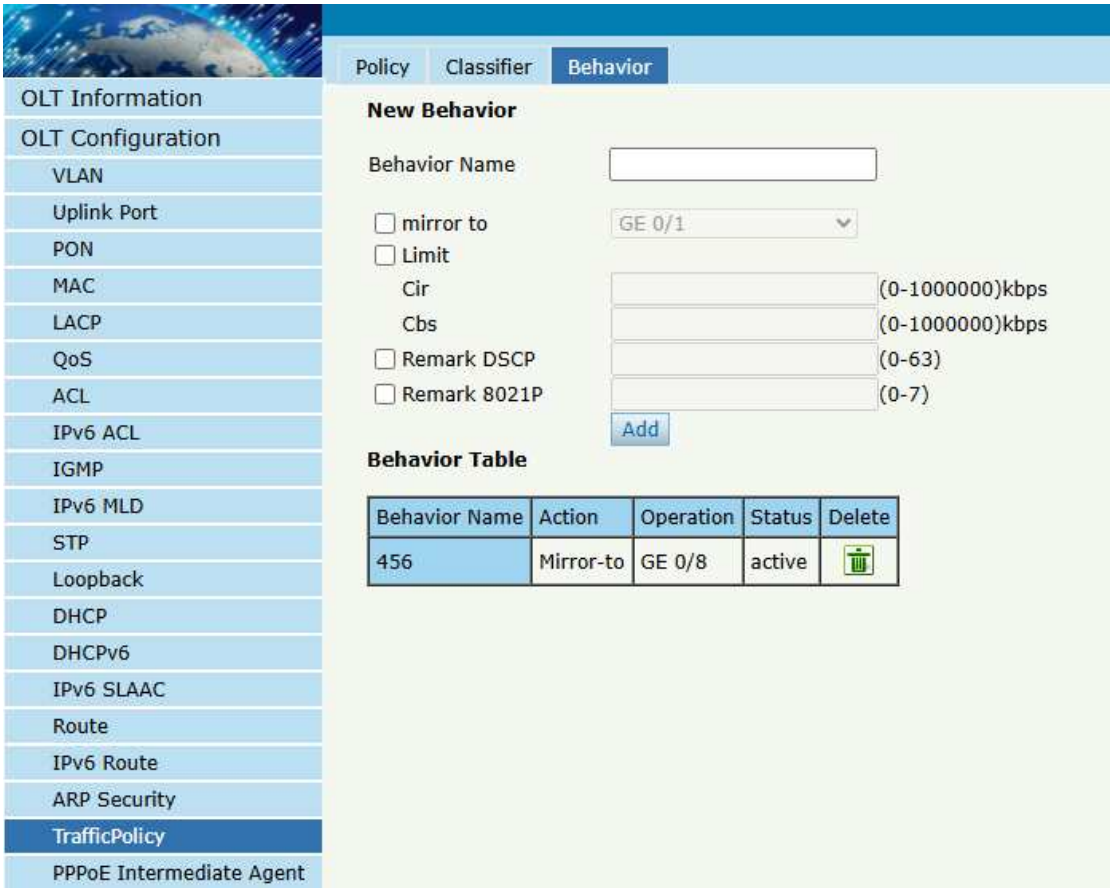


Figure 3.19-3: Behavior

3.20 PPPoE Intermediate Agent

PPPoE Intermediate Agent, also referred to as PPPoE+, plays a critical role in the network architecture of the PPPoE protocol. It is primarily utilized to modify the information of PPPoE packets on the user side, relay and forward these packets, thereby enabling functionalities such as user identity recognition, policy enforcement, and cross-network segment communication. The core functionality of PPPoE+ closely resembles that of a DHCP relay agent.

3.20.1 PPPoE Intermediate Agent Configuration

OLT Configuration →PPPoE Intermediate Agent→PPPoE Intermediate Agent
This interface is used to configure PPPoE+ switches and parameters. After enabling PPPoE+, users also need to add the target VLAN of the agent.
Illustrations of each parameter:

Parameters	Illustration
Vendor ID	It is used to identify the manufacturer. By default, the device adds a value of 3561 in the PPPoE packet.

Encapsulation	The tag filled in the PPPoE packet by the OLT can be selected.
Policy	OLT' processing strategy for the received PPPoE packets. **DROP:** If the PPPoE packets received by the OLT carries a tag, the OLT will strip the tag then forwarding. If the PPPoE packets received by OLT do not have tags, OLT will transmit them transparently. **KEEP:** Whether the received packet carries Tag or not, the OLT will transmit them transparently. **REPLACE:** If the PPPoE packets received by the OLT carries a tag, OLT will replace the original PPPoE Tag according to the configuration. If the PPPoE packets received by OLT do not have tags, OLT will transmit them transparently.
Ignore Reply	It determines whether the OLT processes the PPPoE packets replied by the server. By default, it is enabled, and the OLT directly transmits the packets received from the server.

Table 3.20-1 PPPoE+ Parameters

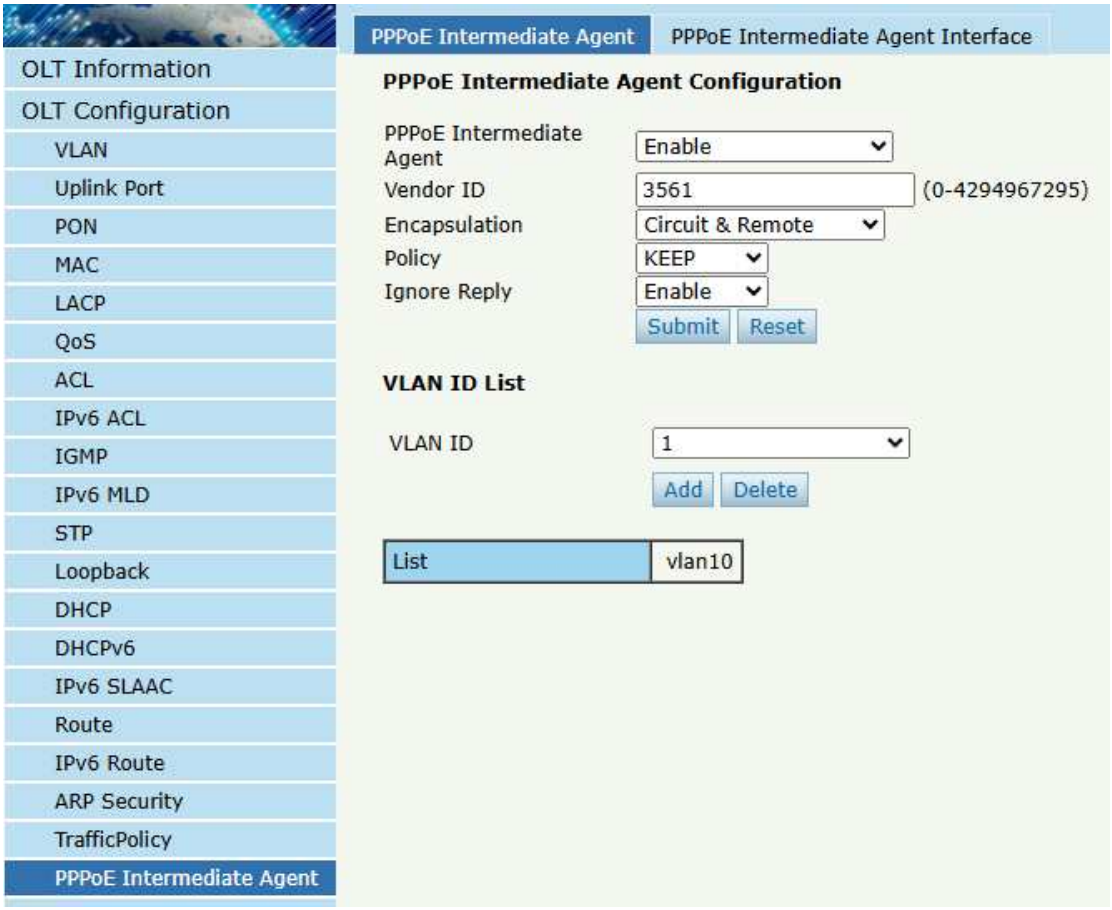


Figure 3.20-1: PPPoE+ Configuration

3.20.2 PPPoE Intermediate Agent Interface

OLT Configuration →PPPoE Intermediate Agent→PPPoE Intermediate Agent Interface

This interface is used to configure PPPoE+ trusted ports and specify the formats of Circuit ID and Remote ID.

The interface connecting the OLT to the PPPoE Server must be a trust interface in order to prevent the PPPoE Server from being deceived and to prevent PPPoE packets from being forwarded to non-pppoe service ports and obtained by illegal users. After configuring the trust interface, PPPoE packets from the PPPoE Client to the PPPoE Server direction will only be forwarded by the trust interface, and only PPPoE packets received from the trust interface will be forwarded to the PPPoE Client. The trust interface only controls the protocol packets in the PPPoE Discovery stage and does not control the service messages in the PPPoE Session stage.

Circuit/Remote ID can be configured in three field formats:

COMMON is the standard fill format:
Circuit ID format: *Slot number/sub-card number/port number: SVLAN.CVLAN Host name* 0/0/0/0/0, ASCII encapsulation.
Remote ID format: *Device MAC*(6 bytes), ASCII encapsulation.

EXTEND is an extended fill format:
Circuit ID format:
Circuit id type(1)+length(4)+SVLAN(2byte)+slot(5bit)+sub-slot(3bit +port(1byte), HEX encapsulation.
Remote ID format: remote-id type(2)+length(6)+mac(6 bytes), HEX encapsulation.

USER-DEFINED is a format defined by users.

Figure 3.20-2: PPPoE+ Interface Configuration

3.21 ARP

3.21.1 ARP Table

OLT Configuration →ARP→ARP Table

You can view the ARP table of OLT in this interface and also manually add or delete ARP entries. For some key devices such as servers, it can prevent ARP spoofing attacks to configure static table entries.

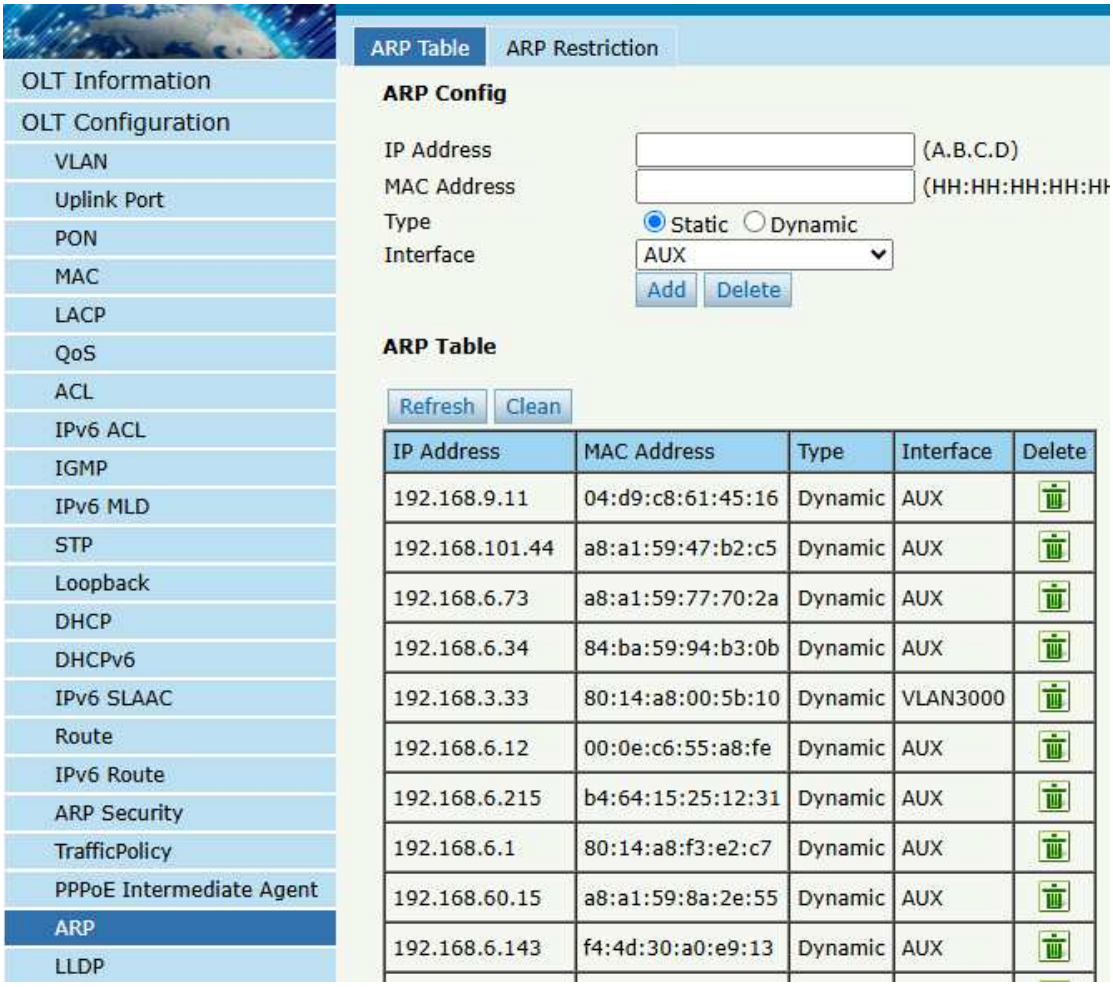


Figure 3.21-1 ARP Table

3.21.2 ARP Restriction

OLT Configuration →ARP→ARP Restriction

This interface can be used to configure ARP Restriction Rules. It is like a blacklist, and the OLT will not learn the ARP table entries that match the rules. OLT also supports limiting the forwarding rate of ARP packets.

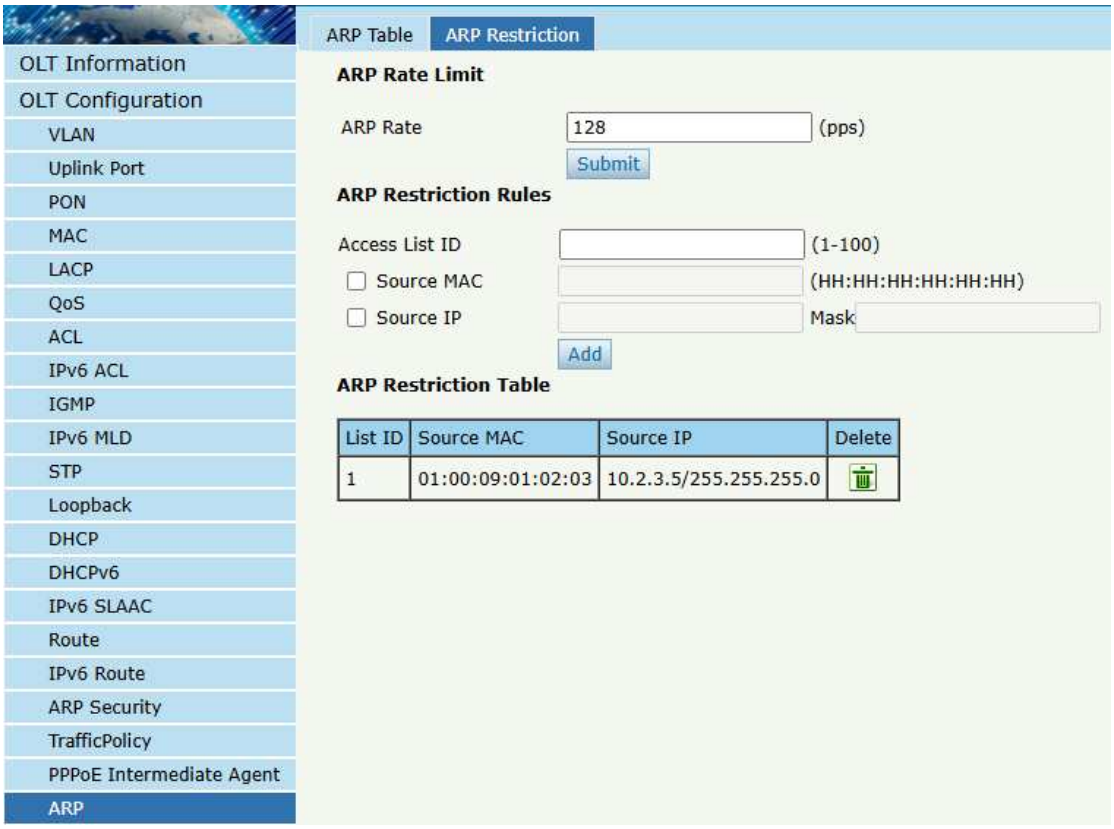


Figure 3.21-2 ARP Restriction

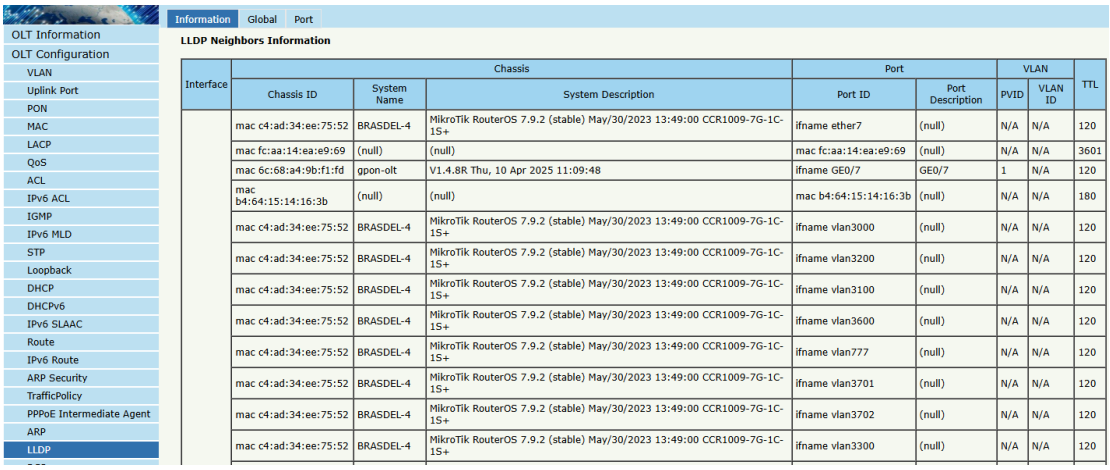
3.22 LLDP

LLDP is the link layer discovery protocol defined in IEEE 802.1ab. It can organize the management addresses, device identifiers, interface identifiers and other information of the local devices and publish them to its neighboring devices. After receiving this information, the neighboring devices save it in the form of a standard management information base MIB for the network management system to query and determine the communication status of the link.

3.22.1 Information

OLT Configuration →LLDP→Information

This interface displays the chassis and port information of neighboring devices discovered through LLDP.



Interface	Chassis			Port		VLAN		TTL
	Chassis ID	System Name	System Description	Port ID	Port Description	PVID	VLAN ID	
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname ether7	(null)	N/A	N/A	120
	mac fc:aa:14:ea:e9:69	(null)	(null)	mac fc:aa:14:ea:e9:69	(null)	N/A	N/A	3601
	mac 6c:68:a4:9b:f1:fd	gpon-olt	V1.4.8R Thu, 10 Apr 2025 11:09:48	ifname GE0/7	GE0/7	1	N/A	120
	mac b4:64:15:14:16:3b	(null)	(null)	mac b4:64:15:14:16:3b	(null)	N/A	N/A	180
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3000	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3200	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3100	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3600	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan777	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3701	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3702	(null)	N/A	N/A	120
	mac c4:ad:34:ee:75:52	BRASDEL-4	MikroTik RouterOS 7.9.2 (stable) May/30/2023 13:49:00 CCR1009-7G-1C-1S+	ifname vlan3300	(null)	N/A	N/A	120

Figure 3.22-1 LLDP Neighbors Information

3.22.2 Global

OLT Configuration →LLDP→Global

This interface is used to enable LLDP and configure other parameters.

Illustrations of each parameter:

Parameters	Illustration
LLDP Global VLAN	Configure and specify a global LLDP VLAN. All ports that join this VLAN will advertise the VLAN ID and VLAN IP externally. If the specified VLAN does not have an IP, the AUX IP will be advertised.
Tx Interval	LLDP packet transmission interval.
Tx Hold	TTL multiplier. The value of TTL in the Time To Live TLV carried by the LLDP packet is used to set the aging time of the neighbor information on the local device. Since TTL = Min (65535, (TTL multiplier×sending interval of the LLDP packet +1)), That is, take the minimum value between 65535 and (TTL multiplier×LLDP packet transmission interval +1). Therefore, by adjusting the TTL multiplier, the aging time of the information of this device on neighboring devices can be controlled.

Table 3.22-1 LLDP Parameters

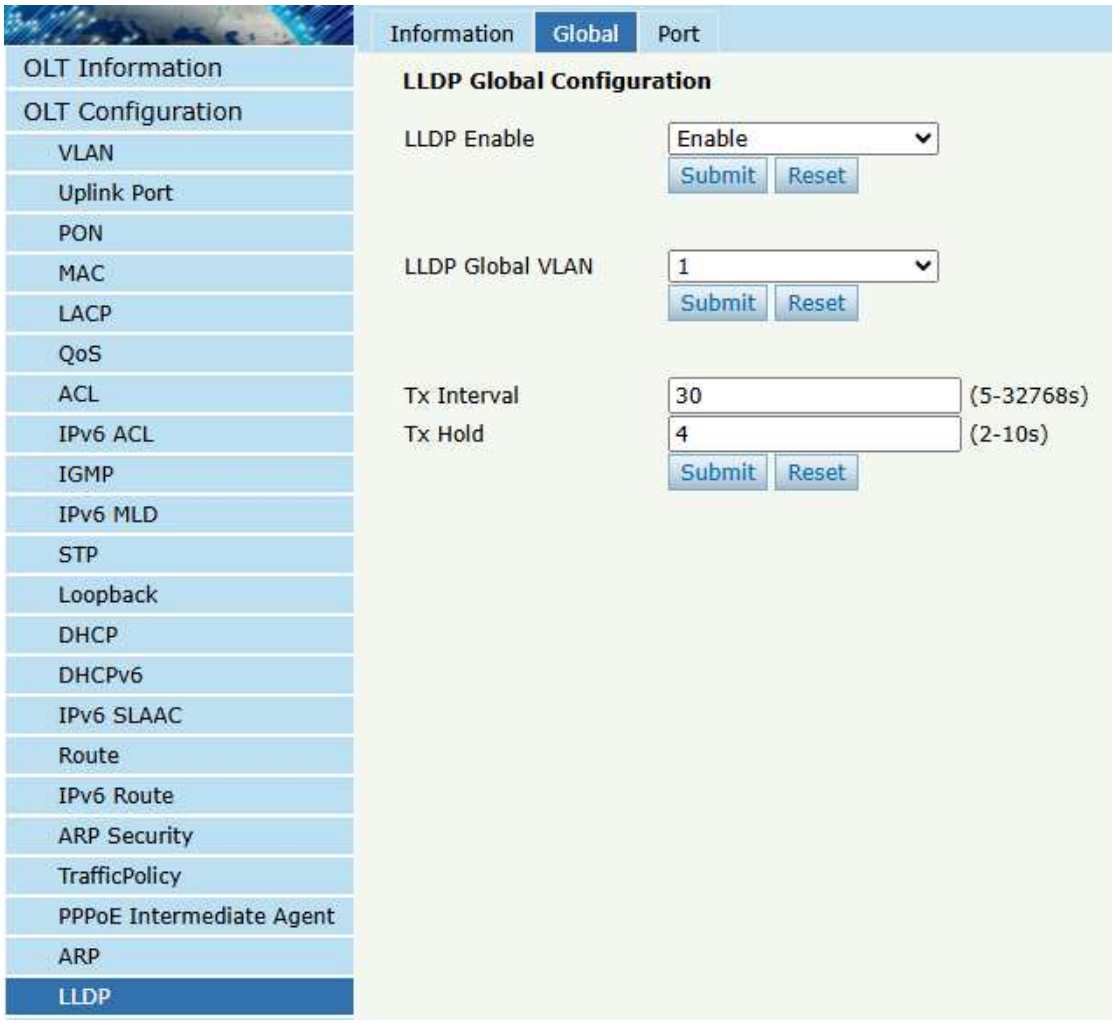


Figure 3.22-2 LLDP Global Configuration

3.22.3 Port

OLT Configuration →LLDP→Port

This interface is used to configure the working mode of the LLDP on the OLT port.

Illustrations of each item:

Item	Illustration
rx-and-tx	The port sends and receives LLDP packets.
rx-only	The port only receives and does not send LLDP packets.
tx-only	The port only sends and does not receive LLDP packets.
disabled	The port neither sends nor receives LLDP packets.

Table 3.22-2 Port LLDP Status

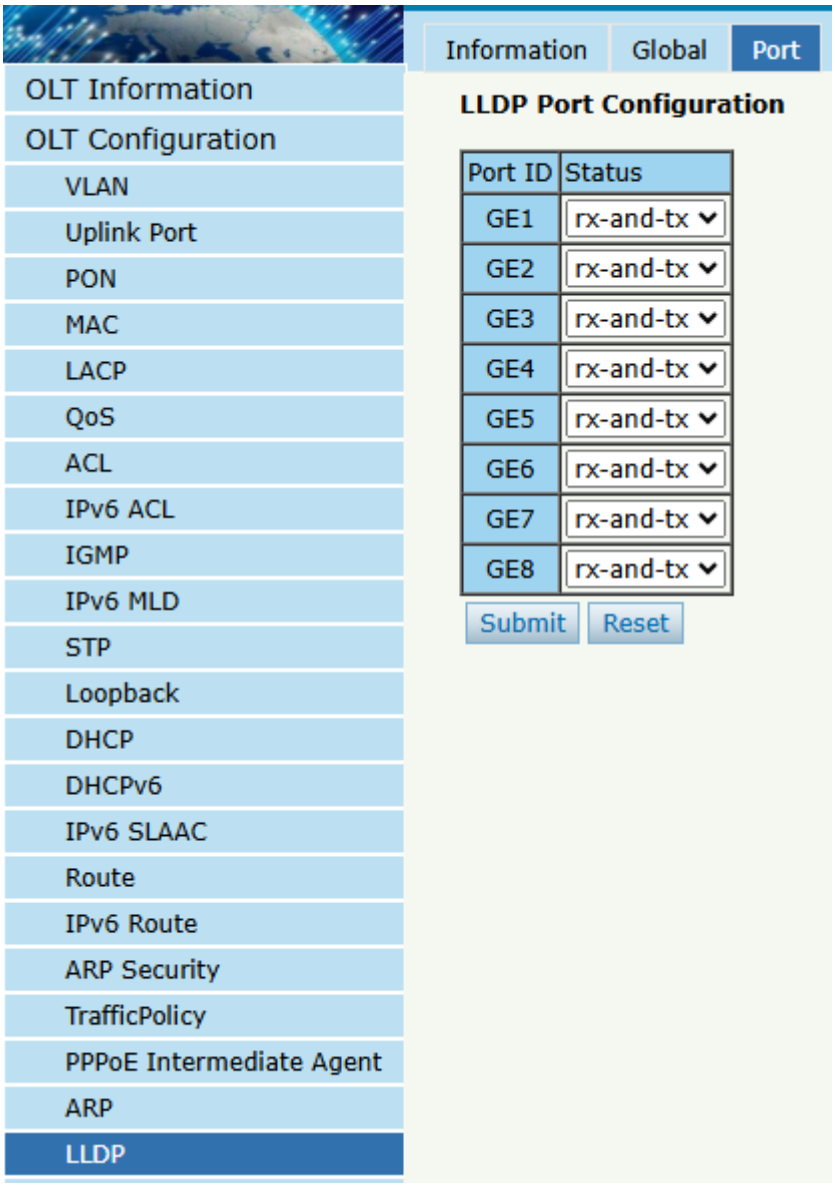


Figure 3.22-3 LLDP Port Configuration

3.23 BGP

BGP (Border Gateway Protocol) is a dynamic routing protocol that can be used both between different AS (Autonomous Systems) and within the same AS. When BGP runs within the same AS, it is called IBGP (Internal BGP). When BGP runs between different AS, it is called EBGP (External BGP). AS is a group of routers that share the same routing strategy and belong to the same technical management department. BGP uses TCP as its transport layer protocol (port number 179), which enhances the reliability of the protocol.

3.23.1 BGP Information

OLT Configuration →BGP→BGP Information

This interface is used to display the BGP Peer Table, which is actually a router neighbor table. After OLT enables the BGP function, it is still necessary to manually configure the IP address of the BGP Peer to generate the BGP Peer Table, which is introduced in Section 3.23.4.
Routers that implement the BGP protocol are referred to as BGP speakers. These BGP speakers are responsible for receiving or generating routing information and subsequently disseminating this information to other BGP speakers. When BGP speakers establish TCP connections with each other and exchange routing information, they are considered BGP Peers.

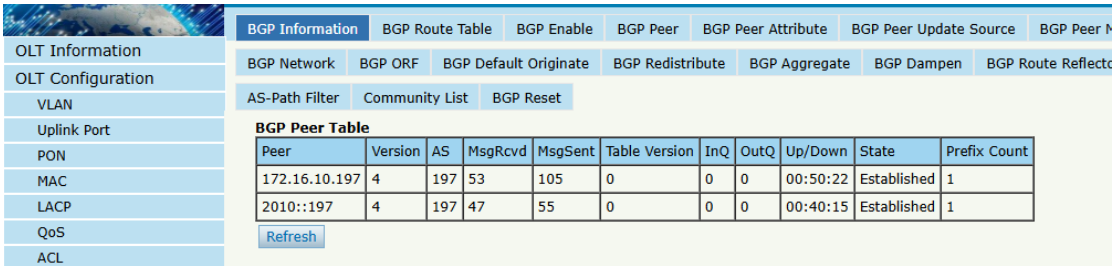


Figure 3.23-1: BGP Peer Table

Illustrations of each parameter:

Parameter	Illustration
Peer	It shows the IPv4/IPv6 address of the peer.
Version	The currently used version of BGP is BGP-4.
AS	Autonomous system number, which is unique in the BGP network, is used to distinguish different AS.
MsgRcvd	The number of BGP packets received from this peer.
MsgSent	The number of BGP packets sent to this peer.
Table Version	The version number of the BGP routing table. When the local version number is higher than the version recorded by the neighbor, an incremental routing update is triggered.
InQ	The number of messages waiting to be processed from this peer.
OutQ	The number of messages to be sent to this peer.
Up/Down	The duration of the current state.
State	The state machine of the peer. During the process of establishing BGP peers, the three commonly visible states are: Idle, Active, and Established. If the peer remains in a

	non-ESTABLISHED state for a long time, it is necessary to check the network connectivity or configuration (such as AS number, authentication, etc.)
Prefix Count	The number of updated routing table entries of the peer.

Table 3.23-1 The Parameters of BGP Peer Table

3.23.2 BGP Route Table

OLT Configuration →BGP→BGP Route Table

You can view the routing tables of BGP IPv4 and IPv6 on this interface.

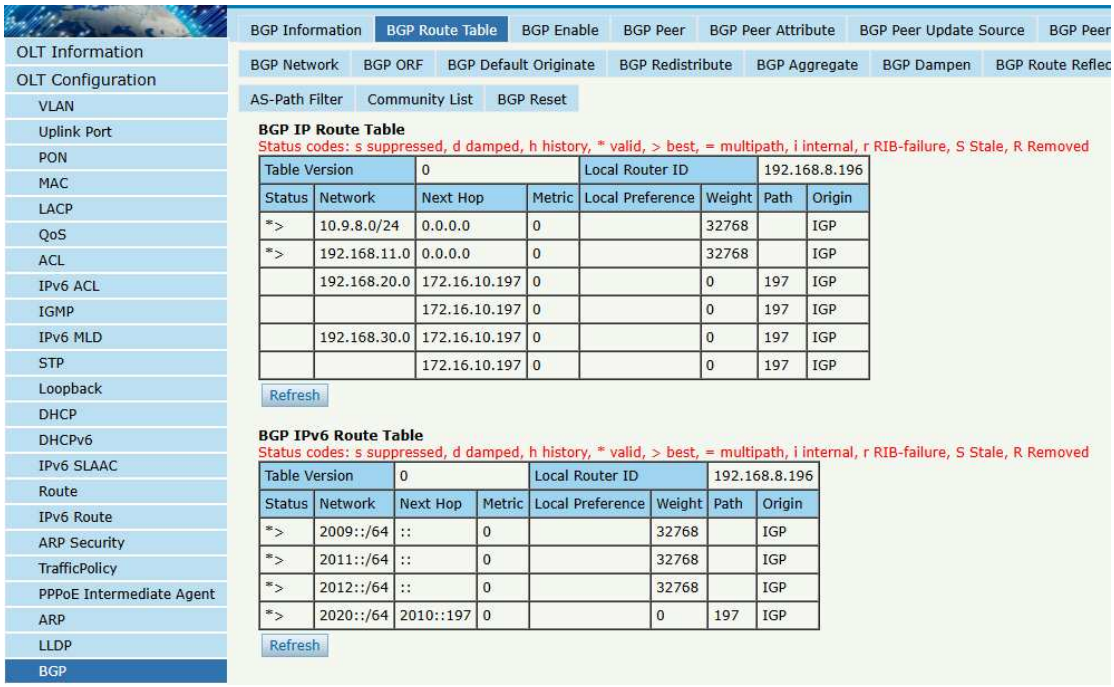


Figure 3.23-2: BGP Route Table

Illustrations of each attribute:

Attribute	Illustration
Network	Target network.
Next Hop	When a BGP Speaker publishes a certain route to an EBGP peer, it sets the next-hop attribute of the route information to the interface address where the local and the opposite end establish a BGP neighbor relationship. When a BGP Speaker publishes the local origin route to an IBGP peer, it sets the next-hop attribute of the route information to the interface address where the local and the peer establish a BGP neighbor relationship.
Metric	BGP itself does not calculate the cost of the path, but it needs to rely on IGP (such as OSPF) to determine the optimal internal

	path to the Next Hop of BGP. For example, if the attributes such as the AS path and Local Preference of multiple BGP paths are the same, the router will select the path with the smallest IGP Metric.
Local Preference	This attribute is only exchanged among IBGP peers and is not advertised to other AS. It indicates the priority of BGP routers. It is used to determine the best route when the traffic leaves the AS. When a BGP router obtains multiple routes with the same destination address but different next hops through different IBGP peers, it will give priority to the route with a higher attribute value.
Weight	It is a local attribute used to select the best path. Its core function is to help routers make priority choices among multiple BGP routes reaching the same destination. The larger the value, the higher the priority. In the BGP routing algorithm, "Weight" is the determination condition of the first priority. The router will give priority to selecting the route entry with the highest Weight value. It only takes effect on a single router and will not be propagated to other BGP neighbors.
Path	The AS_PATH attribute records all the AS numbers that a certain route has to pass through from the local to the destination address.
Origin	The ORIGIN attribute defines the source of the routing information and marks how a BGP route is generated. It has the following three types: · **IGP:** The highest priority, indicating that the route is generated within this AS. · **EGP:** The order of priority, indicating that the route is learned through EGP. · **Incomplete:** The lowest priority, indicating that the source of the route cannot be determined. For example, routing information introduced from other routing protocols.

Table 3.23-2 The Attribute of BGP Route Table

3.23.3 BGP Enable

OLT Configuration →BGP→BGP Enable

This interface is used to configure the switches and some parameters of the BGP protocol. To facilitate the explanation of some BGP parameters, you need to understand the concepts of IBGP and EBGP.

IBGP (Internal BGP) : It is used for exchanging BGP routing information among routers within the same autonomous system (AS), and peers must be located within

the same AS (with the same AS number).

EBGP (External BGP) : It is used for routers to exchange routing information between different autonomous systems. Peers are located in different ASes (with different AS numbers).

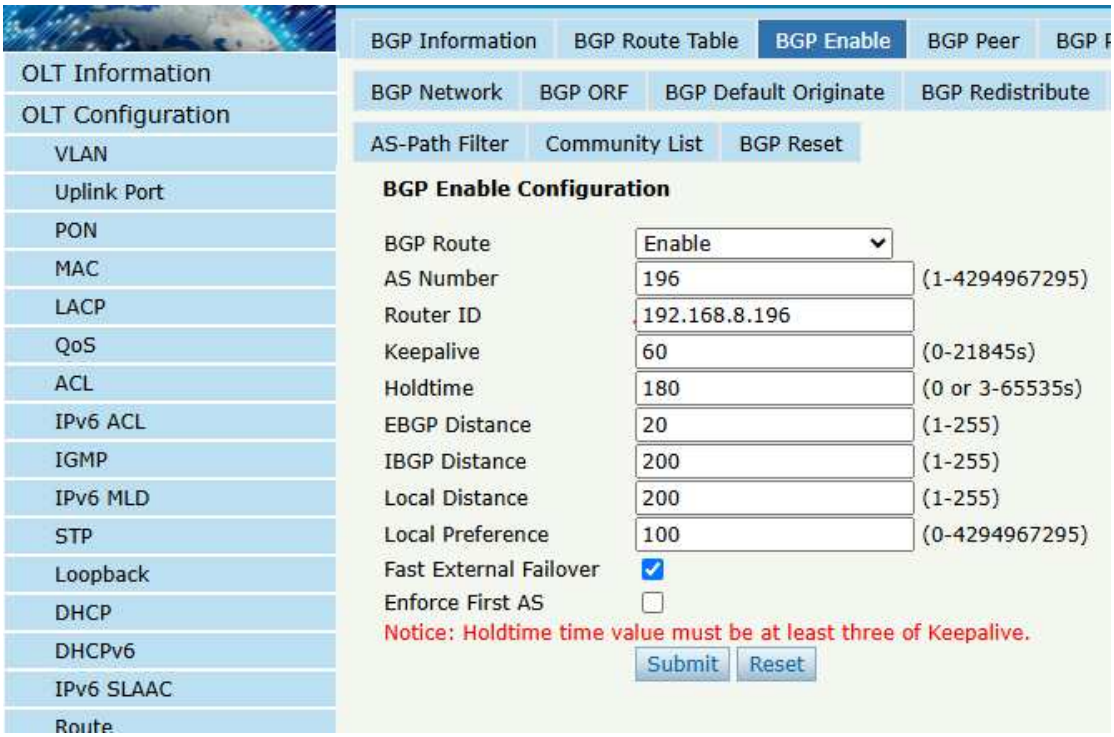


Figure 3.23-3: BGP Enable

Illustrations of each parameter:

Parameter	Illustration
AS Number	Configure the Autonomous System number of this device. A router can only be located within one AS.
Router ID	The Router ID of BGP is a 32-bit value used to identify a BGP device, usually in the form of an IPv4 address, and is carried in the Open message sent when a BGP session is established. When establishing a BGP session between peers, each BGP device must have a unique Router ID.Otherwise, a BGP connection cannot be established between peers.
Keepalive	Configure the sending interval of Keepalive packet ,which is used to keep the connection of BGP.
Holdtime	After the peer establishes a connection, the actual keepalive time value and hold time value are determined through negotiation between the two parties. Among them: Take the smaller value of the hold-time in the Open messages of both peers as the final hold-time value Take the smaller of (the negotiated hold-time value ÷3) and the

	locally configured keepalive time value as the final keepalive time value.
EBGP Distance	It is used to determine the priority of the routing information provided by different routing protocols. The smaller the value, the higher the priority. When a router learns the routes of the same destination network from multiple routing protocols, it will give priority to the route with a smaller administrative distance. The default administrative distance of EBGP is 20.
IBGP Distance	The default administrative distance of EBGP is 200.
Local Distance	It refers to the administrative distance allocated by the router for the locally generated BGP routes.
Local Preference	The Local Preference attribute indicates the BGP priority of the router and is used to determine the best route when the traffic leaves the AS. When BGP devices obtain multiple routes with the same destination address but different next hops through different IBGP peers, the route with a higher Local Preference attribute value will be preferentially selected. It is only valid among IBGP peers and will not be notified to other AS.
Fast External Failover	It is mainly used to immediately terminate the corresponding BGP session when a physical link or interface failure directly connected to an EBGP neighbor is detected (such as an interface being manually closed or a link layer failure), triggering the neighbor state to switch from Established to Idle, and preventing traffic from continuing to be transmitted through unreachable paths.
Enforce First AS	Its function is to verify whether the first AS number in the AS path (AS_PATH) of the received route update is consistent with the AS number of the BGP neighbor that sent the route. Its core purpose is to prevent the propagation of illegal or incorrect routes, thereby enhancing the security and stability of the network.

Table 3.23-3 The Parameters of BGP Protocol

3.23.4 BGP Peer

OLT Configuration →BGP→BGP Peer

This interface is used to configure BGP peers and peer groups. The difference between BGP protocol and routing protocols such as OSPF is that BGP does not automatically discover neighbors through broadcast or multicast. Instead, it requires administrators to explicitly specify the IP address and AS number of peers. It needs to initiate a TCP handshake with the peer to establish a session and ensure the reliable

transmission of route updates.

A peer group is a collection of peers with certain identical attributes. In large-scale BGP networks, there are a large number of peers, and configuration and maintenance are extremely inconvenient. For BGP peers with the same configuration, they can be added to a BGP peer group for batch configuration, simplifying the difficulty of management and improving the efficiency of route publication. When a peer joins a peer group, this peer will obtain the same configuration as the peer group it belongs to. When the configuration of the peer group changes, the configuration of the members within the group also changes accordingly.

Illustrations of peer configuration parameters:

Parameter	Illustration
Mode	You can choose to configure the peer or add the peer to the peer group.
Address Family	It is used to distinguish different network layer protocols: IPv4/IPv6. The routing information of different address families is processed independently to avoid policy conflicts.
Subsequent Address Family	Its function is to further subdivide the routing types within the same address family and apply specific strategies for different scenarios: **Unicast:** Handles regular point-to-point routing. **Multicast:** It is used for routing and distribution in multicast source trees (such as PIM).
Peer	Configure the IP address of the peer.
Remote As	Configure the autonomous system number of the peer.
Description	Configure the description information of the peer.

Table 3.23-4 BGP Peer Configuration

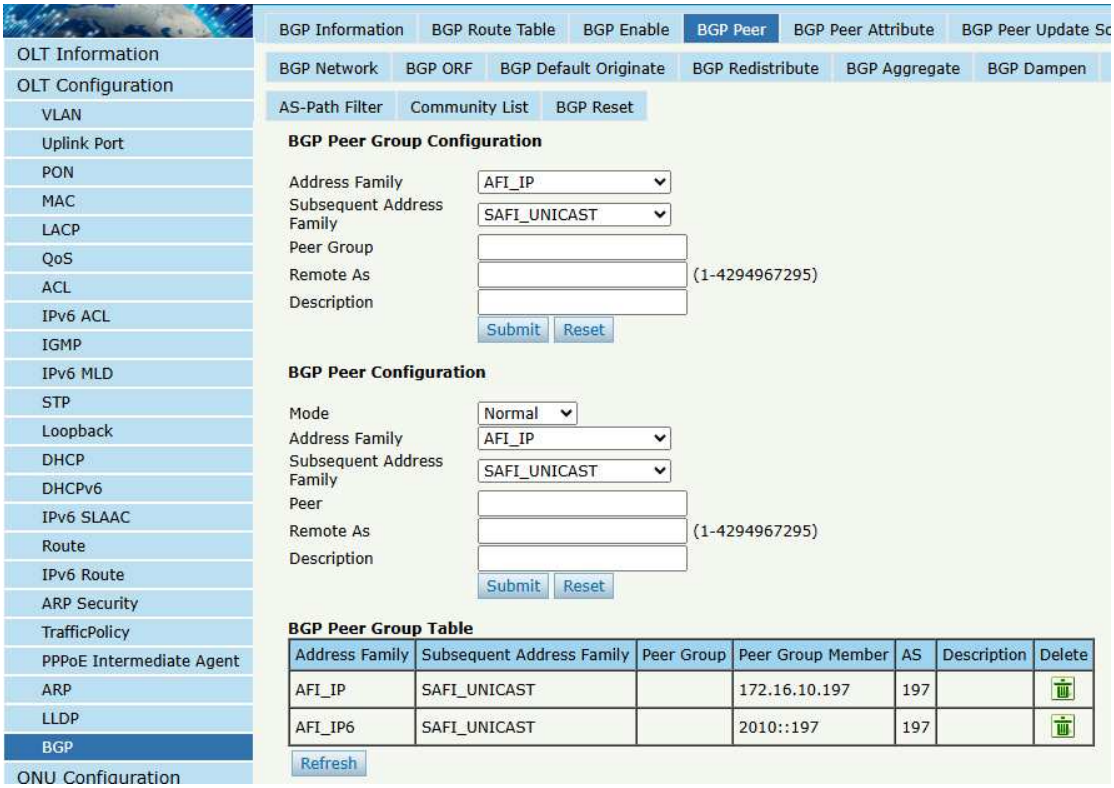


Figure 3.23-4: BGP Peer

3.23.5 BGP Peer Attribute

OLT Configuration →BGP→BGP Peer Attribute

This interface is used to configure the connection authentication of BGP peers and configure the BGP GTSM function, which can improve the security of the BGP network.

After the peer configures "Password", MD5 authentication will be enabled. It is implemented through the MD5 signature option of the TCP protocol. Both peers must configure the same key. The sender generates an MD5 hash value for the TCP message using the key. The receiver verifies whether this hash value matches. If they do not match, the message is discarded. Third-party devices without the key cannot forge legitimate messages and cannot establish BGP sessions. This can prevent unauthorized devices from posing as legitimate neighbors, and at the same time resist man-in-the-middle attacks or tampering with routing information.

The current router needs to establish an EBGP session with another router. There must be a direct physical link between them. If this requirement is not met, the value of Multi-hop must be configured to allow them to establish an EBGP session through multiple hops. It actually modifies the TTL field in the IP message header.

GTSM (Generalized TTL Security Mechanism) is a simple and feasible security mechanism for protecting upper-layer services based on IP protocols. GTSM determines whether the IP message is valid by checking whether the TTL value in the

received IP message header is within a predefined range, avoiding attacks of types such as CPU-utilization on network devices caused by attackers sending a large number of valid IP messages to network devices.
When configuring the BGP GTSM function, users can specify the maximum hop count for the local device to reach a certain peer as hop-count. Then, the legal TTL range of BGP messages received from this peer is 255- "hop-count" +1 to 255. Only when the TTL value of the message from this peer is within this legal range will the message be uploaded to the CPU for processing. Otherwise, discard the message directly.

"Remove Private AS" is a key function in the peer configuration of BGP, mainly used to filter or delete the private AS number in the path attribute AS_Path when receiving or publishing routes. Its core objective is to prevent the leakage of private AS numbers to the public Internet and avoid problems such as routing loops, routing policy failures or abnormal forwarding.

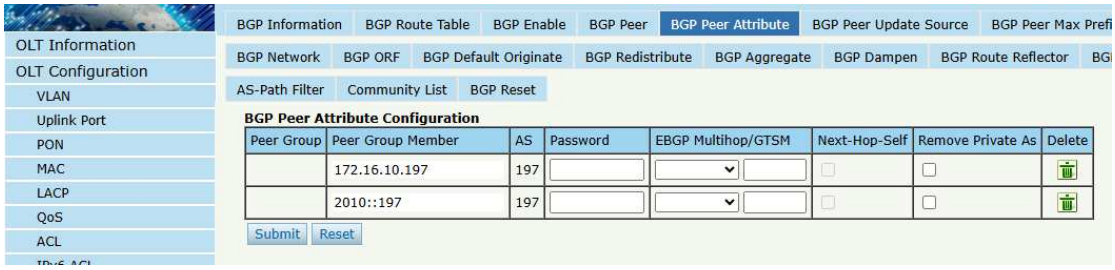


Figure 3.23-5: BGP Peer Attribute Configuration

3.23.6 BGP Peer Update Source

OLT Configuration →BGP→BGP Peer Update Source

This interface is used to configure the local source IP address used when establishing the BGP peer session.

Figure 3.23-6: BGP Peer Update Source Configuration

3.23.7 BGP Peer Max Prefix

OLT Configuration →BGP→BGP Peer Max Prefix

This interface is used to limit the maximum number of route prefixes received from peers. When the device is maliciously attacked or there is an incorrect configuration in the network, it will cause BGP to receive a large number of routes from neighbors, thereby consuming a large amount of device resources, leading to CPU overload or system crash. It is necessary to limit the maximum number of route prefixes for network security.

Illustrations of configuration parameters:

Parameter	Illustration
Max Prefix	Set the maximum number of prefixes that the router is allowed to receive from this peer.
Threshold	Set the percentage of the alarm threshold. When the percentage of the number of routes received by the router to the maximum configured value reaches the specified threshold, the router will generate log information.
Handle	Set the processing strategy for the router after it receives more than the configured number of routes: **Restart:**When the number of prefixes received by the router reaches the upper limit, the current BGP session will be reset and the session will be automatically re-established after the specified time. **Warning-only:**The router only generates log/alarm information and does not interrupt the BGP session.

Table 3.23-5 BGP Peer Max Prefix Limit

Figure 3.23-7: BGP Peer Max Prefix

3.23.8 BGP Peer Attribute Unchanged

OLT Configuration →BGP→BGP Peer Attribute Unchanged

This interface is used to control the modification of routing attributes to ensure that specific attributes (such as AS_PATH, NEXT_HOP, etc.) remain unchanged during

the transmission process.

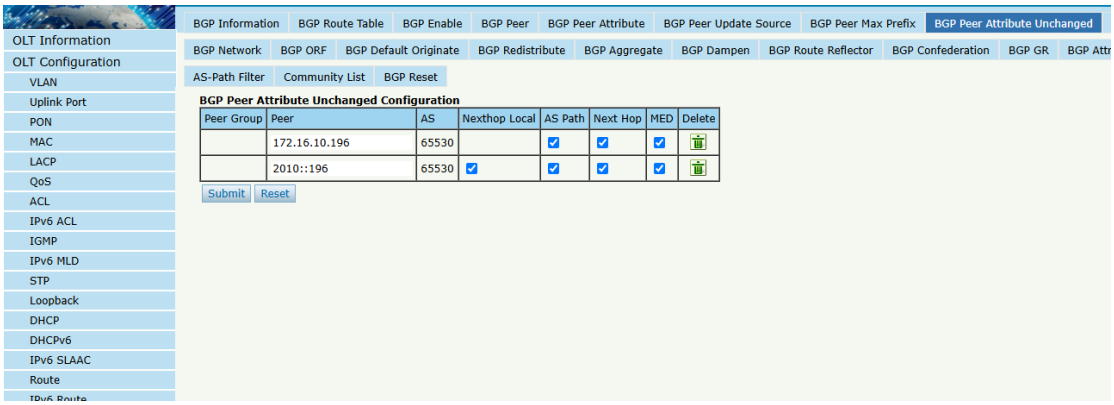


Figure 3.23-8: BGP Peer Attribute Unchanged

3.23.9 BGP Dual AS

OLT Configuration →BGP→BGP Dual As

BGP Dual AS allows a BGP router to use both the old and new AS numbers simultaneously when establishing a BGP session with the same neighbor during AS migration (changing the autonomous system number). Its core objective is to achieve a smooth and seamless migration of AS numbers and minimize network disruptions to the greatest extent.

“Dual As” is used to configure the new AS number. The router will use this new AS number to send BGP OPEN packets.
After enabling No-Prepend, when the router announces the route to the routers of other AS, it will not add its own AS number to the AS_PATH attribute.
“Replace AS” can replace the internal AS number with a unified public AS number to hide network details externally and enhance security.

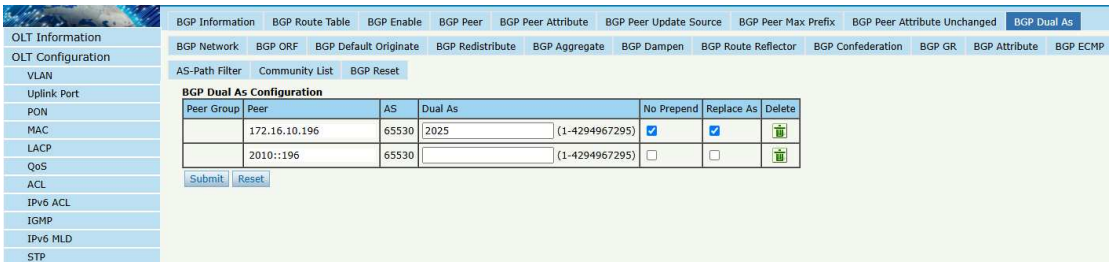


Figure 3.23-9: BGP Dual AS Configuration

3.23.10 BGP Network

OLT Configuration →BGP→BGP Network

This interface is used to configure the network segment that the router is to advertise. After configuring the backdoor, the administrative distance of a specific EBGP route is changed to 200 (the same as IBGP), making its priority lower than that of IGP routes. Other routers thus give priority to the routes learned by IGP to implement the traffic taking the internal path rather than directly connecting to the EBGP link.

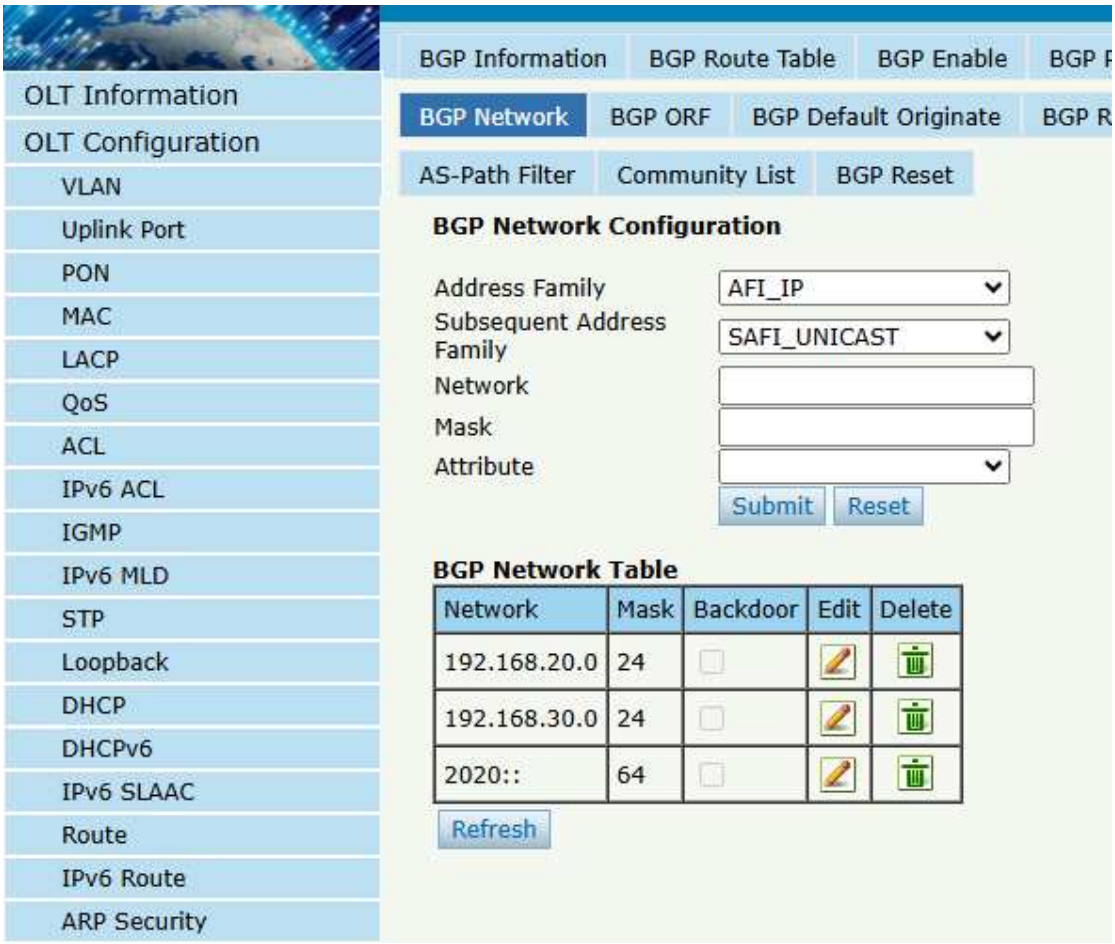


Figure 3.23-10: BGP Network

3.23.11 BGP ORF

OLT Configuration →BGP→BGP ORF

The role of BGP ORF (Outbound Route Filtering) is to allow the recipients of BGP routes to actively control which routes their peers (neighbors) send to them, thereby optimizing network performance and resource utilization.

If the ORF is configured to the send mode, the router will actively send the local entry route filtering policy to the BGP peer/neighbor, requiring the neighbor to filter out those routes rejected by the local ORF Prefif-list in advance according to these policies when sending route updates. Ultimately, the local router will only receive those routes that are both allowed by the local outbound policy of the neighbors and comply with the PrefiF-list policy sent by the local router through ORF. This saves the link bandwidth between BGP peers and avoids the CPU overhead that the local router

needs to process and immediately discard a large number of unnecessary routes.

If the ORF is configured in the receive mode, the router will allow the reception and application of ORF policies sent by neighbors, and dynamically filter the routes sent from this end to the neighbors. Configure the both mode, and the router will support both sending and receiving ORF policies simultaneously.

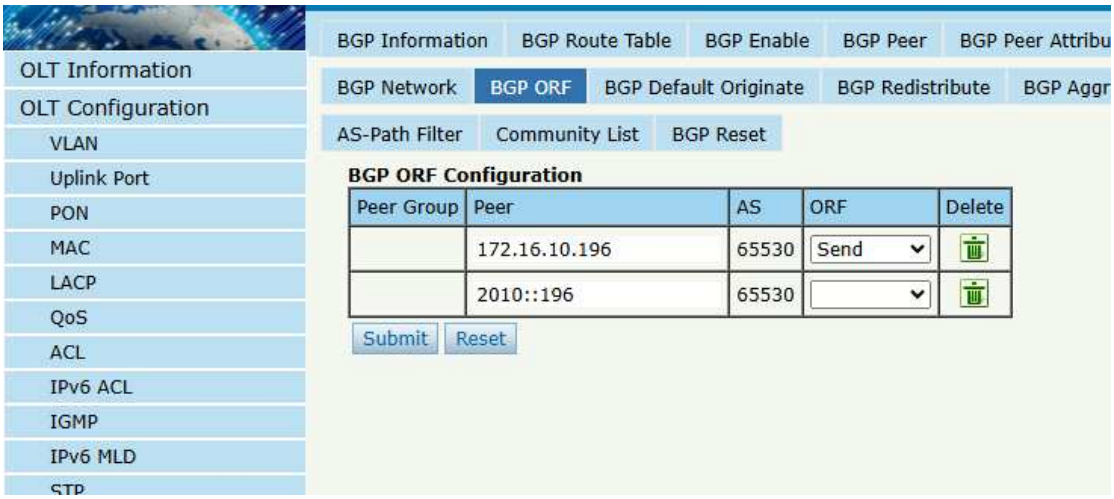


Figure 3.23-11: BGP ORF Configuration

3.23.12 BGP Default Originate

OLT Configuration →BGP→BGP Default Originate

When Default Originate is enabled, the device publishes a default route to the specified peer/peer group with the next-hop address being the local address.

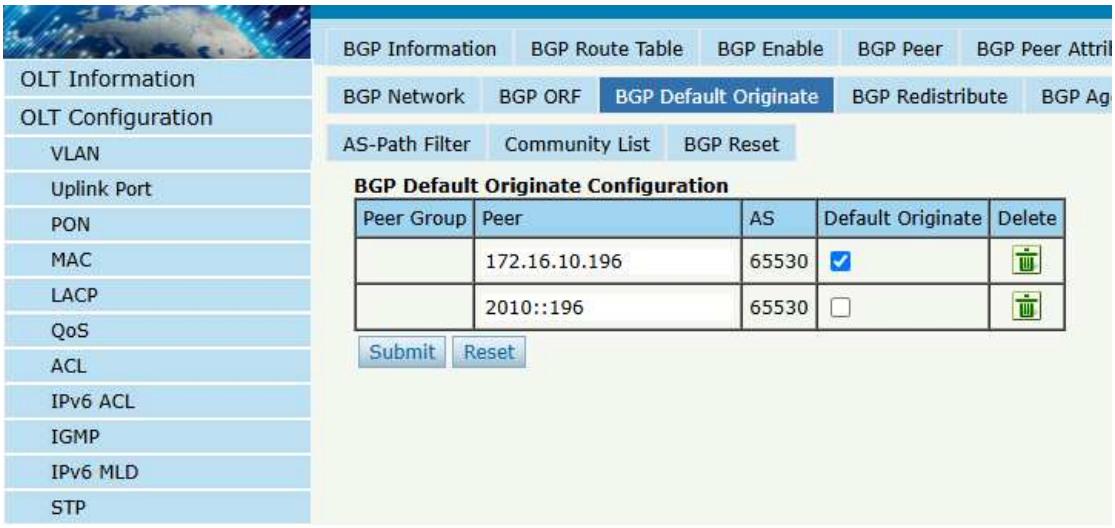


Figure 3.23-12: BGP Default Originate

3.23.13 BGP Redistribute

OLT Configuration →BGP→BGP Redistribute

This interface is used to introduce the routing table information of other routing protocols, such as OSPF, into the BGP routing table.

Figure 3.23-13: BGP Redistribute

3.23.14 BGP Aggregate

OLT Configuration →BGP→BGP Aggregate

When a router advertises routing information to its peers, route aggregation can be configured to reduce the number of advertised routes and minimize the size of the routing table. IPv4 BGP supports two aggregation methods: automatic aggregation and manual aggregation. Additionally, when both methods are configured simultaneously, manual aggregation takes precedence over automatic aggregation. IPv6 BGP, on the other hand, only supports manual aggregation.

The AS Set will put all the AS numbers passed through by the aggregated routes into an unordered Set and append it to the AS_Path of the aggregated routes. BGP routers can detect and reject loop routes by checking whether the AS Set contains its own AS number. It records all the AS (after deduplication) that the aggregated routes pass through, providing more complete path visibility.

"Summary Only" can combine multiple more specific (with a longer prefix) routing entries into a broader (with a shorter prefix) routing entry for advertisement.

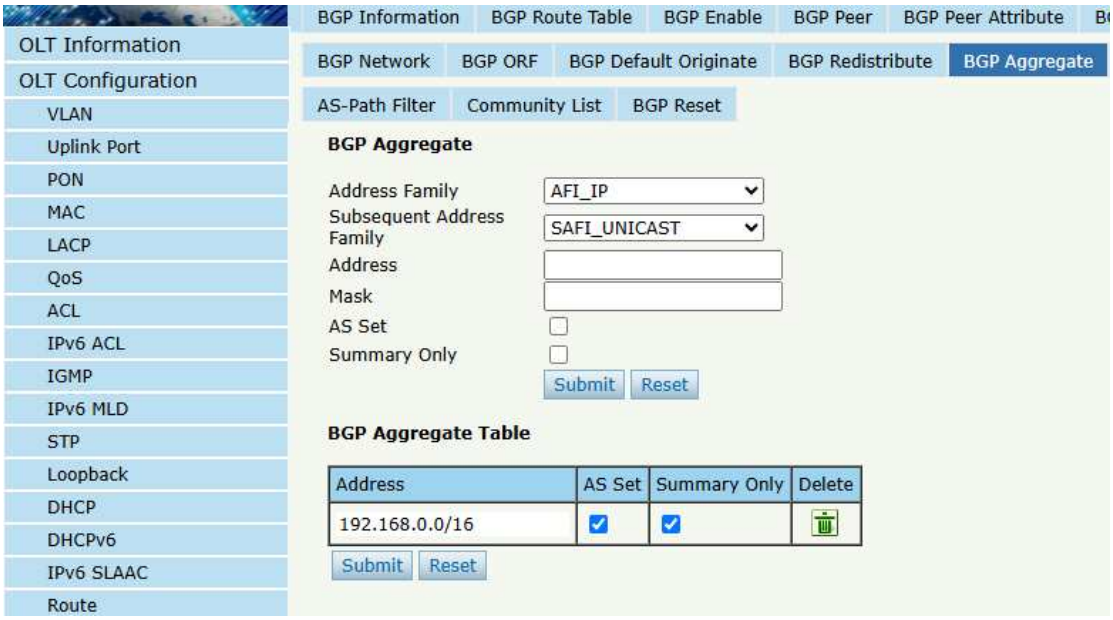


Figure 3.23-14: BGP Aggregate

3.23.15 BGP Dampen

OLT Configuration →BGP→BGP Dampen

When the route changes, the routing protocol will issue a route update to the neighbors. The router that receives the route update needs to recalculate the route and modify the routing table. If routing oscillation occurs, that is, the routing is unstable, and a certain route in the routing table repeatedly disappears and reappears, it will consume a large amount of bandwidth resources and CPU resources, and in severe cases, it will affect the normal operation of the network. BGP uses route attenuation to suppress unstable routes.

BGP Dampen uses penalty values to measure the stability of a route. The higher the penalty value, the more unstable the route is. Each time a route undergoes an oscillation (when a route changes from an active state to an inactive state, it is called a route oscillation), BGP will add a certain penalty value (1000, which is fixed by the system and cannot be modified) to this route. When the penalty value exceeds the suppression threshold, this route is suppressed, not added to the routing table, and no update messages are advertised to other BGP peers.

After a certain period of time, the penalty value of the suppressed route will be reduced by half. This period of time is called half-life. When the penalty value drops to the reuse threshold (reuse value), this route becomes available and is added to the routing table, and update messages are simultaneously published to other BGP peers. The time from when a route is suppressed to when it becomes available for route recovery is called the suppress time.

BGP Dampen only affects EBGP routes and has no effect on IBGP routes. This is

because the IBGP routing may contain the routing of this AS, while the IGP network requires that the routing tables within the AS be as consistent as possible. If route attenuation has an effect on IBGP routing, then when the attenuation parameters of different devices are inconsistent, it will lead to inconsistent routing tables.

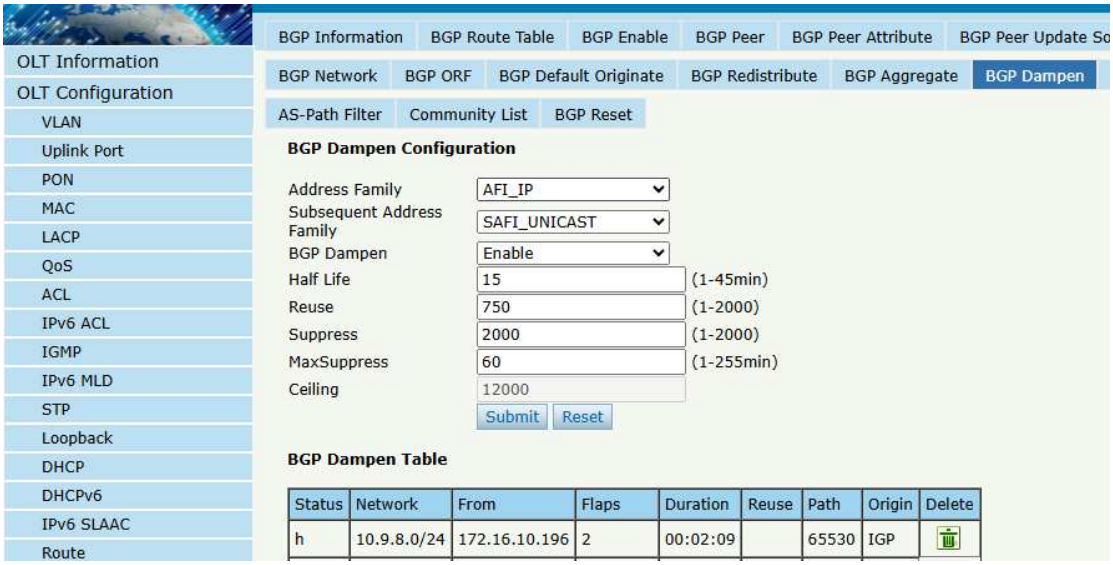


Figure 3.23-15: BGP Dampen

3.23.16 BGP Route Reflector

OLT Configuration →BGP→BGP Route Reflector

In traditional IBGP deployments, to prevent routing loops, all routers running IBGP must establish fully interconnected neighbor relationships with all other IBGP routers within the same AS. When the network scale grows to a certain extent, the router needs to maintain a large number of TCP sessions, consuming the router's memory and CPU usage.

The core function of BGP route reflectors is to address the scalability issues caused by full-mesh IBGP. They enable IBGP routers to learn and propagate BGP routes without establishing full-mesh sessions with all other IBGP routers within an AS. By allowing BGP devices to reflect routes learned from IBGP peers to other IBGP peers, route reflectors overcome the limitation that "BGP routes learned from an IBGP peer are advertised only to EBGP peers."

Within an AS, there are several roles regarding the routing reflector:

Route Reflector(RR): It allows the routes learned from IBGP peers to be reflected to the BGP devices of other IBGP peers.
Client: An IBGP device that forms a reflection neighbor relationship with RR. Inside AS, the client only needs to be directly connected to RR.
Non-Client: An IBGP device that is neither the RR nor the client. Full connection

relationships must still be established between non-clients and RR within AS, as well as among all non-clients.
Originator: A device that initiates routes within the AS. The Originator_ID attribute is used to prevent the generation of routing loops within the cluster.
Cluster: A collection of route reflectors and their clients. The Cluster_List attribute is used to prevent routing loops from being generated between clusters.

If there are multiple BGP routers in the same AS, in order to reduce the number of IBGP connections established within the same AS, several BGP routers can be divided into a cluster. One of the routers can be configured as a route reflector, and the other routers can act as clients. Routes are reflected between clients through the route reflector.
To enhance the reliability of the network and prevent single point of failure, more than one routing reflector can be configured in a cluster. At this time, the network administrator must configure the same cluster ID for each routing reflector located in the same cluster to avoid routing loops.

The Client to Client Reflection configuration in BGP (usually set on the route reflector) mainly serves to control whether the route reflector allows direct reflection of routes between its clients. Clients located under the same RR directly exchange routing information through RR without establishing a direct BGP neighbor relationship.

After enabling the Allow Outbound Policy, when the route reflector reflects the routes to the specified client or non-client neighbors, it applies the route policy configured in the outbound direction of that neighbor.

Users can configure specific peers/peer groups in the BGP Route Reflector Table as the clients of the route reflectors. Meanwhile, this device will serve as a routing reflector.

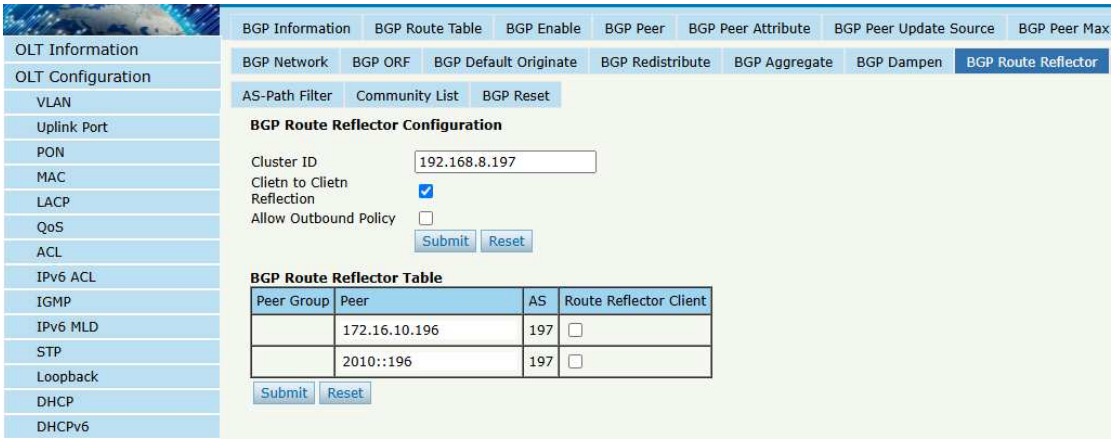


Figure 3.23-16: BGP Route Reflector

3.23.17 BGP Confederation

OLT Configuration →BGP→BGP Confederation

BGP Confederation is another method to handle the surge of IBGP network connections within an autonomous system. It divides an autonomous system into several sub-autonomous systems. The IBGP peers within each sub-autonomous system establish a full connection relationship, and the sub-autonomous systems establish an internal EBGP connection relationship within the confederation.

From the perspective of BGP speakers who do not belong to the confederation, multiple sub-autonomous systems belonging to the same confederation form a whole. The outside device does not need to know the situation of the internal sub-autonomous systems. The Confederation ID is the autonomous system number that identifies the confederation as a whole.

If a router establishes an EBGP neighbor relationship with other sub-autonomous systems of this confederation, it is necessary to specify which sub-autonomous systems are included in the confederation besides itself by configuring Confederation Peer AS.

A confederation can include up to 32 sub-autonomous systems. The autonomous system number used when configuring sub-autonomous systems belonging to the confederation is only valid within the confederation.

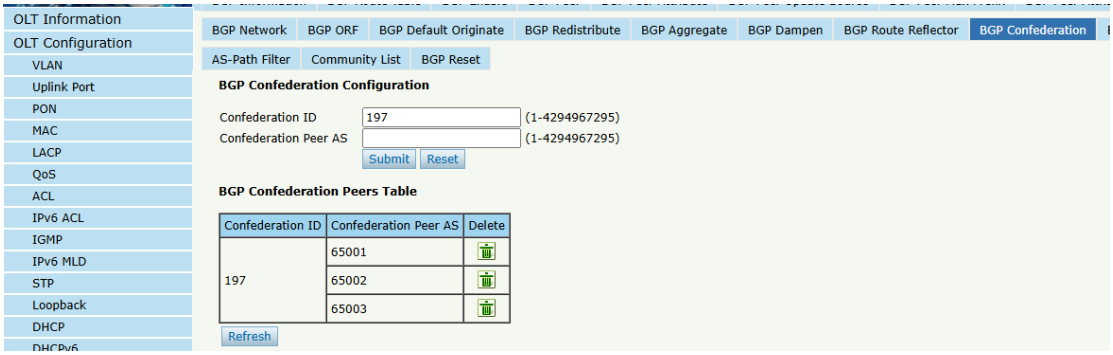


Figure 3.23-17: BGP Confederation Configuration

3.23.18 BGP GR

OLT Configuration →BGP→BGP GR

BGP GR (Graceful Restart) is a mechanism that ensures the forwarding service is not interrupted when the BGP protocol restarts. GR has two roles:

· GR Restarter: A device that undergoes protocol restart and has GR capabilities.

· GR Helper: A device that has a neighbor relationship with GR Restarter and assists in completing the GR process. GR Helper also has GR capabilities.

The device can act as both GR Restarter and GR Helper. The role of the device is

determined by its role in the BGP GR process.

"StalePath Time" refers to the time spent waiting to notify the RIB (Routing Information Base) aging and failure table entries during the BGP GR process. When performing a BGP protocol restart, the GR Restarter does not delete RIB or FIB (Forwarding Information Base) entries. It continues forwarding packets based on the existing forwarding entries while initiating the RIB route aging timer.

"Restart Time" refers to the maximum time for the peer to reestablish a BGP session connection. GR Restarter will notify the GR Helper of the Restart time. If the BGP session is not successfully established within the BGP session reconstruction time announced by GR Restarter, GR Helper will delete the routes marked as invalid.

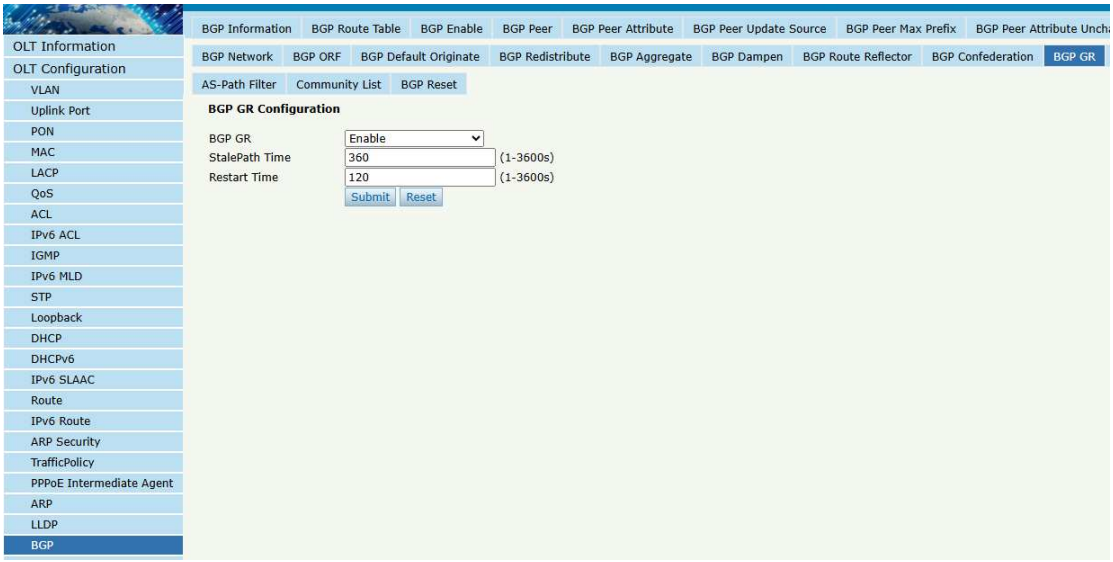


Figure 3.23-18: BGP GR Configuration

3.23.19 BGP Attribute

OLT Configuration →BGP→BGP Attribute

This interface is used to configure the attributes related to BGP route optimization.

The MED attribute is equivalent to the Metrics used by IGP and is used to determine the best route when the traffic enters AS. When a device running BGP obtains multiple routes with the same destination address but different next hops through different EBGP peers, under the same other conditions, the one with the smaller MED value will be preferred as the best route.

Illustrations of configuration parameters:

Parameter	Illustration
Always Compare MED	Force BGP to compare the MED attribute values of routes from different ASes. By default, it is not allowed to compare the

	MED attribute values from different AS routes.
Deterministic MED	Configure to perform MED sorting and optimization on routes from the same AS. By default, BGP compares each route in the order of the time they were received (the latest route is compared first). This may cause different routes with the same prefix to generate different optimal paths due to different receiving orders, triggering route oscillations or suboptimal path selection.
Compare Router ID	If a unique and optimal path still cannot be selected after comparing other attributes, the Router will choose the path announced by the BGP Speaker with the lowest Router ID as the optimal path.
AS-PATH Ignore	The AS_Path attribute is not used as the routing condition. By default, BGP takes the AS_Path attribute as a condition for selecting the optimal route.
AS-PATH Confed	Its main function is to control the handling method of the internal path of the confederation and ensure that behaves as a single AS externally.
AS-PATH Multipath Relax	After enabling , when BGP routers determine whether multiple EBGP paths meet the multipath condition, they will relax the requirement that the AS_PATH sequence must be exactly the same, while still requiring that the length of the AS_PATH must be the same. It allows routers to install and load balance those EBGP paths with the same AS_PATH length but different sequences.
MED Confed	Compare the MED values of the routes within the confederation. By default, BGP only compares the MED attribute values of routes from the same AS.
MED Missing AS Worst	When AS_PATH fails to provide the original AS information, the router regards the MED values of these paths as infinite (the worst). This will force the router to prioritize the path that can clearly identify the original AS, and compare MED only when there is no such path.

Table 3.23-6 BGP Route Optimization

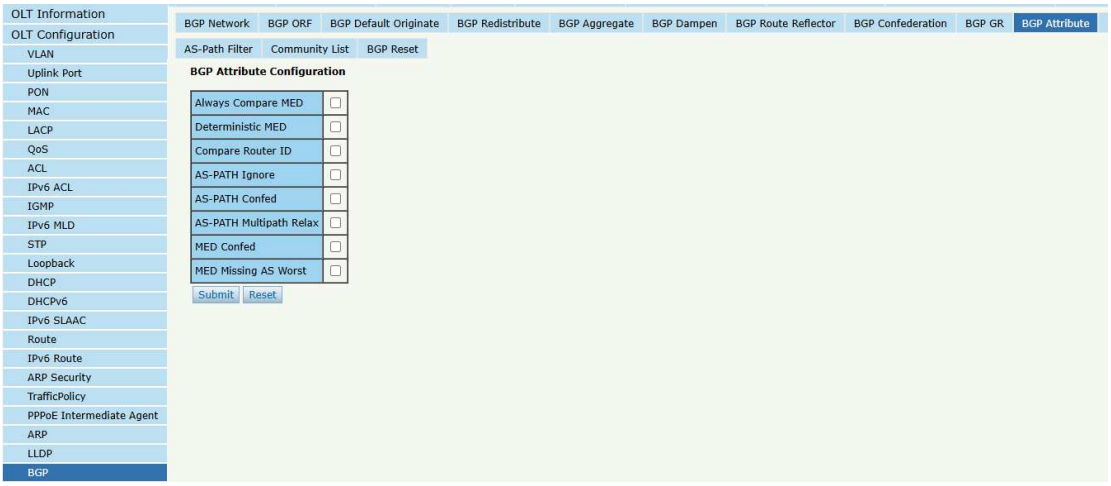


Figure 3.23-19: BGP Attribute Configuration

3.23.20 BGP ECMP

OLT Configuration →BGP→BGP ECMP

The full name of ECMP is Equal-Cost Multi-path, which means that multiple paths reaching the same destination network have the same "cost". In BGP, this "cost" usually refers to the fact that the final attribute values (such as weight, local priority, AS_PATH length, origin type, MED, etc.) compared during the path selection process are equal.

This interface is used to configure the maximum number of equivalent routes for BGP load balancing. By default, the maximum number of equivalent routes for BGP load balancing is set to 1, which implies that load balancing is not performed.

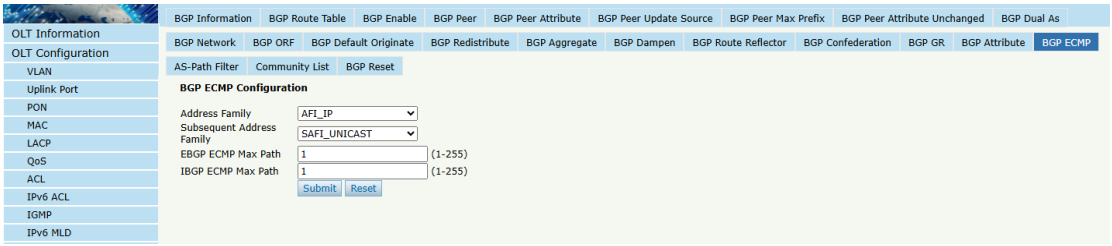


Figure 3.23-20: BGP ECMP

3.23.21 AS-Path Filter

OLT Configuration →BGP→AS-Path Filter

The AS path filter is a set of rules for filtering the AS_Path attribute of BGP routes. In the routing information of BGP, there is the AS_Path attribute. The AS_Path attribute records all the AS numbers that the BGP route passes through from the local to the destination address in vector order. Therefore, by defining some filtering rules based on the AS_Path attribute, the filtering of BGP routing information can be achieved.

The matching conditions of the AS path filter are specified using regular expressions.

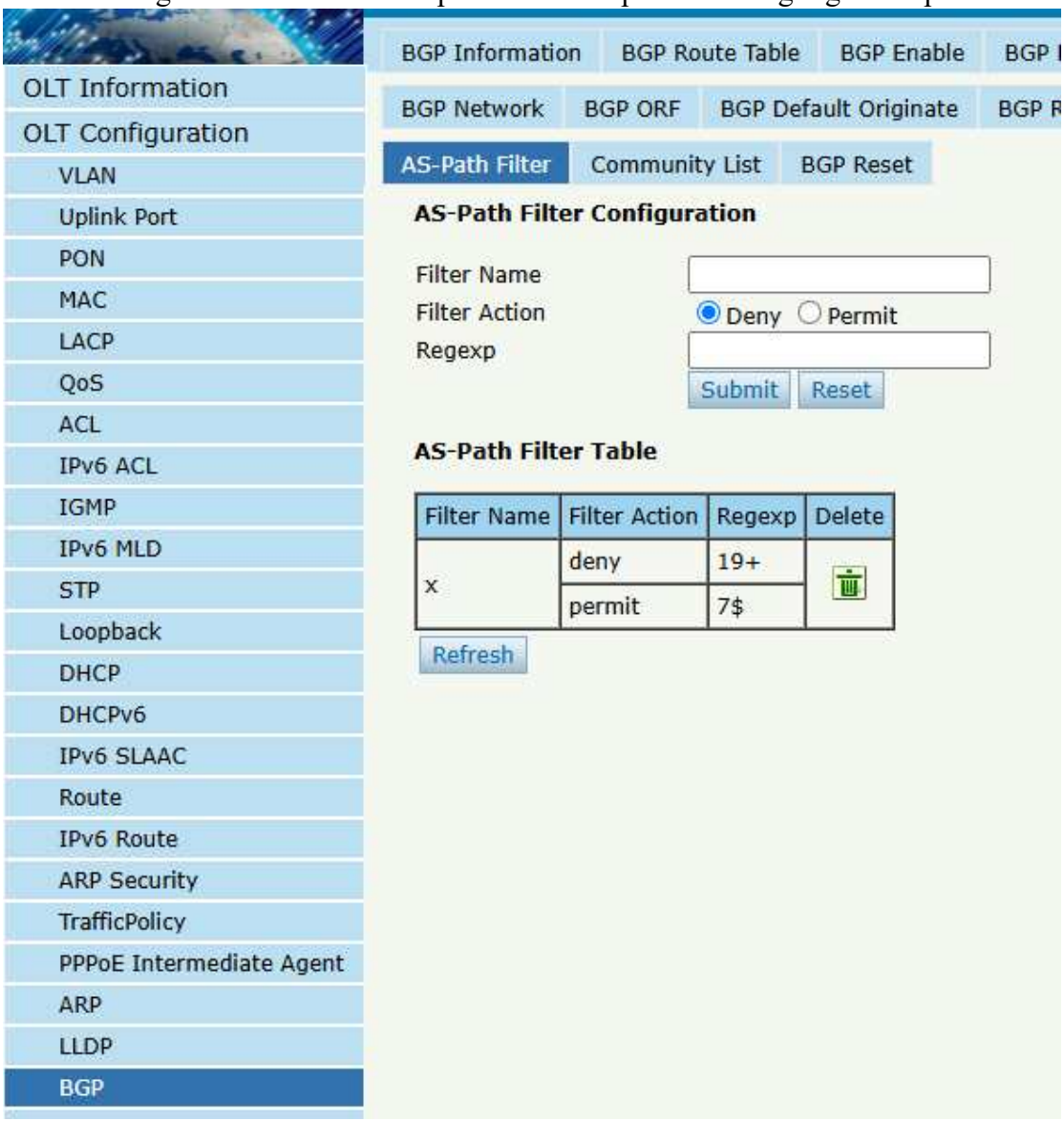


Figure 3.23-21: AS-Path Filter

3.23.22 BGP Community List

OLT Configuration →BGP→BGP Community List

In the routing information packet of BGP, there exists a community attribute field, which is utilized to identify a specific group. The community list specifies matching conditions for the attribute domain of the group. Group attributes can identify routes with similar characteristics without taking into account dispersed route prefixes or numerous AS numbers. When used in conjunction with group attributes, the community list can simplify route management when it is impractical to use address prefix lists or AS path access control lists.

There are two types of group attribute lists: standard group attribute lists and extended group attribute lists. The extended group attribute list supports regular expressions,

which is more flexible than the standard group attribute list in matching group attributes.

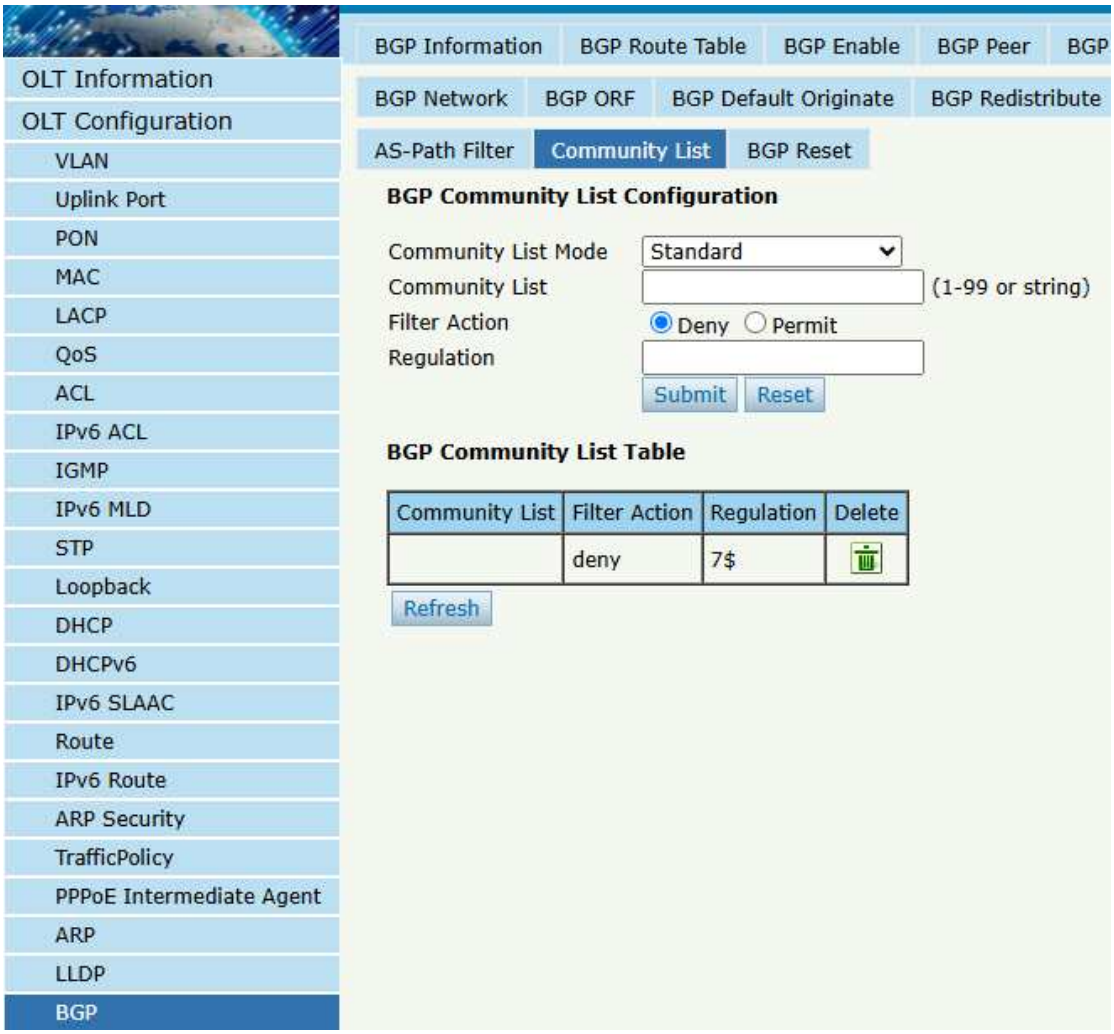


Figure 3.23-22: BGP Community List

3.23.23 BGP Reset

OLT Configuration →BGP→BGP Reset

When there is a change in the BGP routing policy or protocol, devices that support the BGP Route-refresh capability will automatically perform a routing update. If this feature is not supported, the update must be initiated by resetting the BGP session. BGP reset can be categorized into hard reset and soft reset. A hard reset disconnects the BGP peer connection, rendering all associated information invalid and causing its deletion. In contrast, a soft reset does not terminate the BGP peer connection but instead triggers an Update operation to enforce the new routing policy. Soft reset can be applied simultaneously or independently to both inbound and outbound policies. An inbound soft reset sends a Route-refresh message to all BGP peers, while an outbound soft reset transmits an UPDATE message to implement the new routing policy.

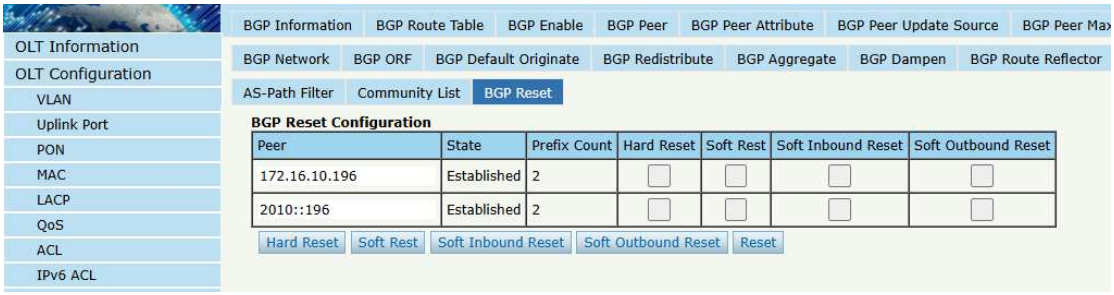


Figure 3.23-23: BGP Reset

Chapter 4 ONU Configuration

This chapter is about the ONU management by OLT.

4.1 ONU AuthList

4.1.1 ONU List

ONU Configuration→ONU AuthList→ONU List
Select PON port ID, all ONU will be displayed in this interface. You can check ONU using profile, Registration mode and do some operations to every ONU.

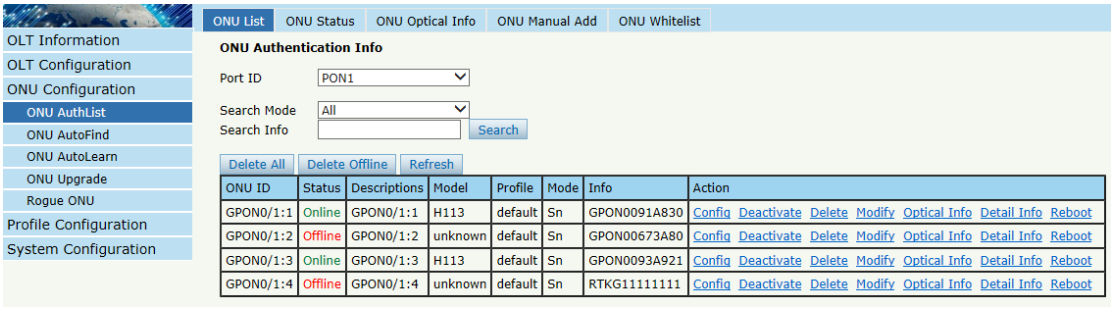


Figure 4.1-1: ONU List

4.1.1.1 Config

ONU Configuration→ONU AuthList→ONU List→Config
Configure ONU parameter information which you selected.

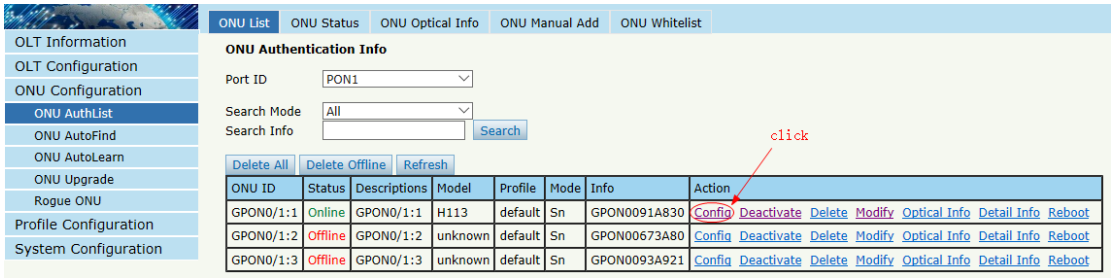


Figure 4.1-2: Configure ONU

4.1.1.1.1 Tcont

ONU Configuration→ONU AuthList→ONU List→Config→Tcont
Create Tcont ID and bind DBA profile. Tcont name is optional.

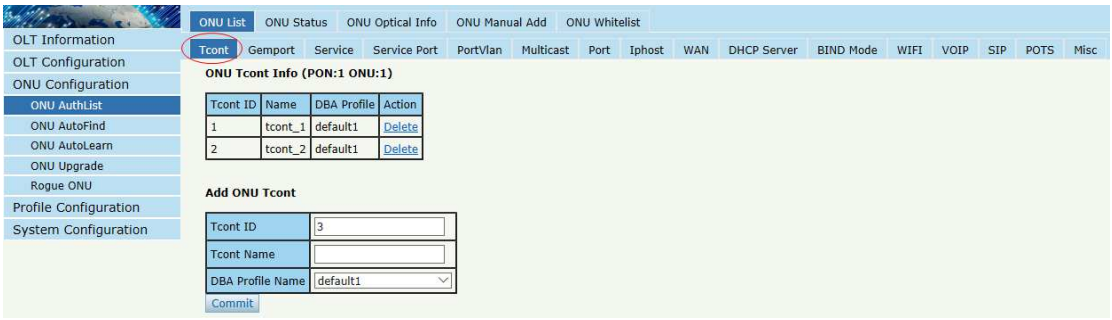


Figure 4.1-3: Create Tcont

4.1.1.1.2 Gemport

ONU Configuration→ONU AuthList→ONU List→Config→Gemport

Create Gemport ID and bind Tcont ID.

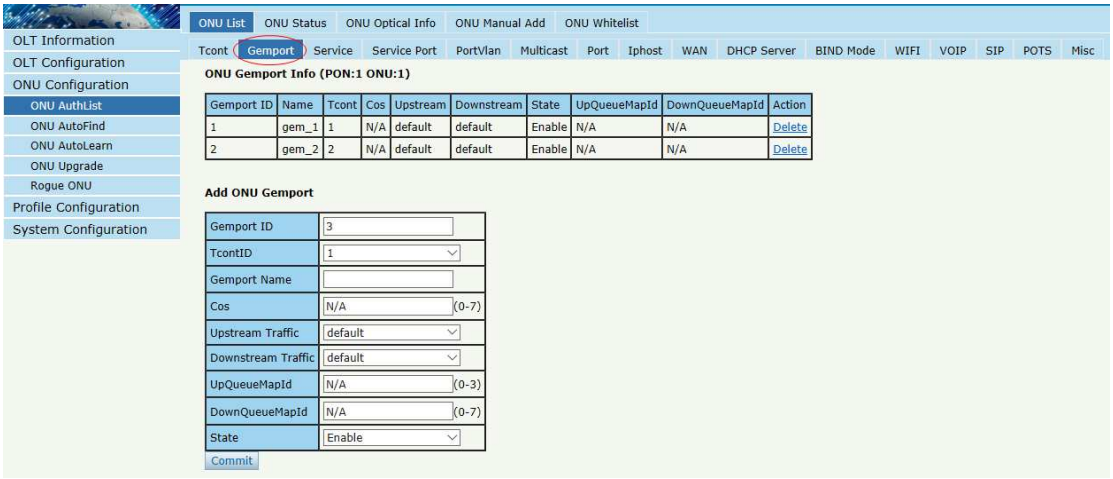


Figure 4.1-4: Create Gemport

4.1.1.1.3 Service

ONU Configuration→ONU AuthList→ONU List→Config→Service

Create a service, set the VLAN and VLAN mode and bind one Gemport ID.

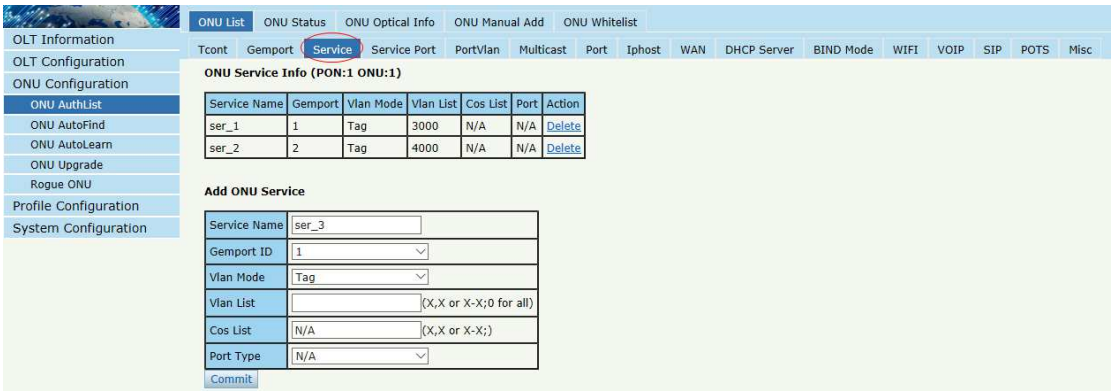


Figure 4.1-5: Create service

4.1.1.1.4 Service Port

ONU Configuration→ONU AuthList→ONU List→Config→Service Port

Create a service port, set the user VLAN and translate VLAN and bind one Gemport ID. If don't need VLAN translation, just set translate VLAN the same as user VLAN.

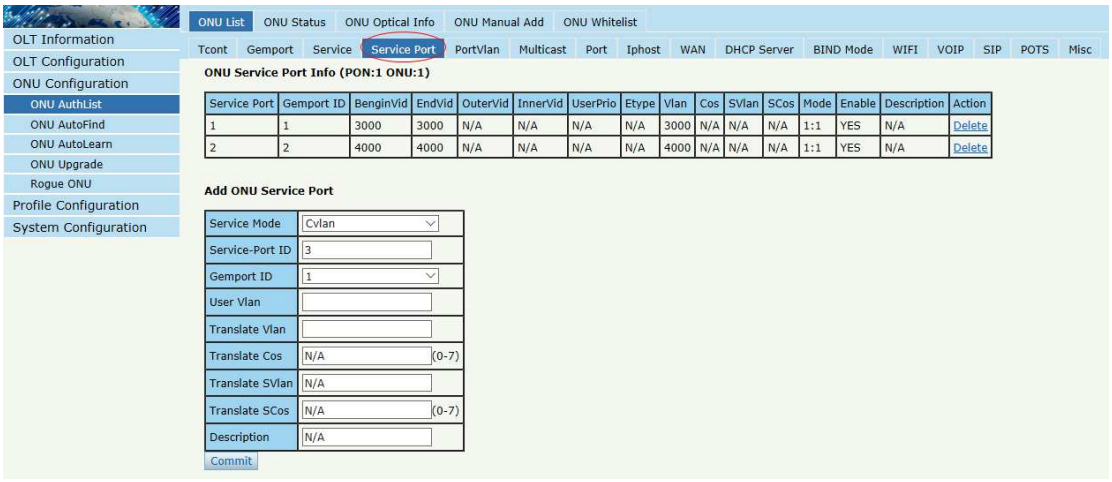


Figure 4.1-6: Create service port

4.1.1.1.5 PortVlan

ONU Configuration→ONU AuthList→ONU List→Config→ PortVlan

Set the VLAN mode of the ONU port. For HGU, need to configure veip 1 transparent; for SFU, configure Ethernet port directly.

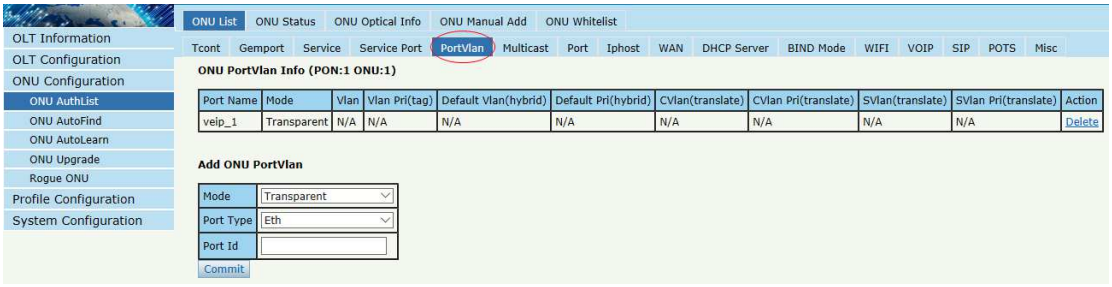


Figure 4.1-7: Configure port VLAN mode

4.1.1.1.6 Multicast

ONU Configuration→ONU AuthList→ONU List→Config→ Multicast

Set the Multicast VLAN of ONU and the Multicast VLAN mode of ONU port.

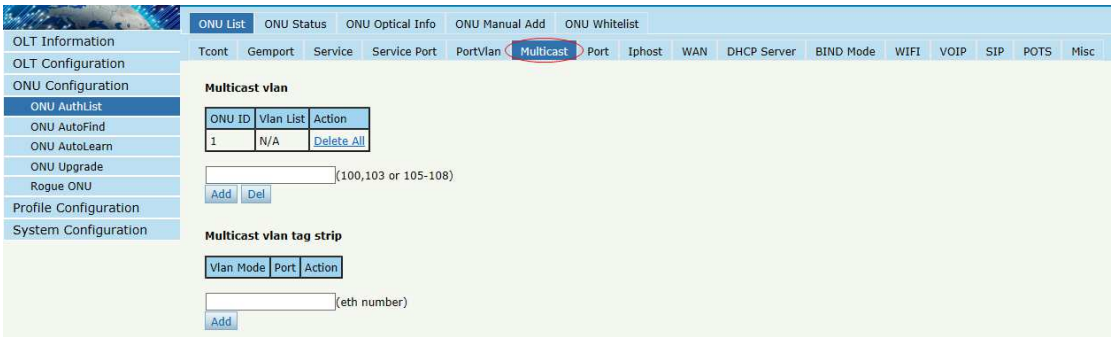


Figure 4.1-8: Configure multicast VLAN

4.1.1.1.7 Port

ONU Configuration→ONU AuthList→ONU List→Config→Port

Set attribute of ONU LAN port.

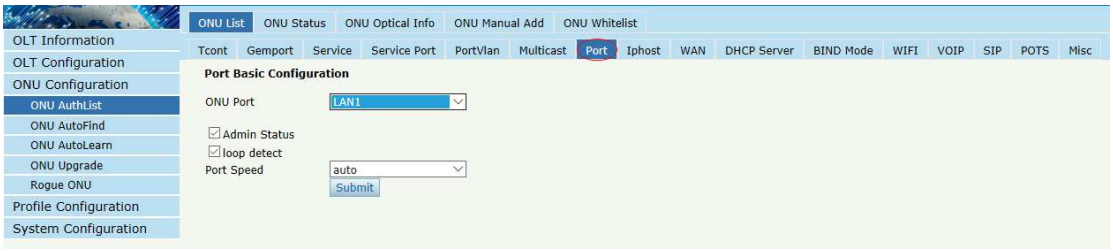


Figure 4.1-9: ONU port attibute

4.1.1.1.8 Iphost

ONU Configuration→ONU AuthList→ONU List→Config→Iphost

Create Iphost for ONU wan connection. It is used for ONU management.

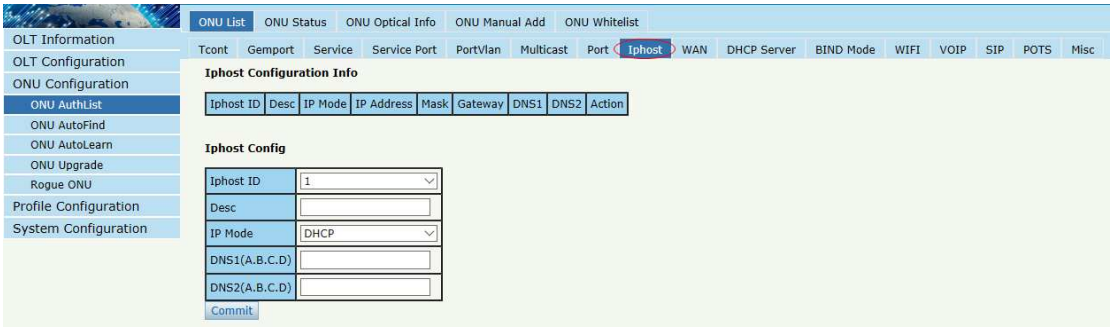


Figure 4.1-10: Configure IPhost

4.1.1.1.9 WAN

ONU Configuration→ONU AuthList→ONU List→Config→WAN

ONU WAN connection is configured by private OMCI between OLT and ONU. When the connected ONU supports this function, the option "WAN" can be shown on this page.

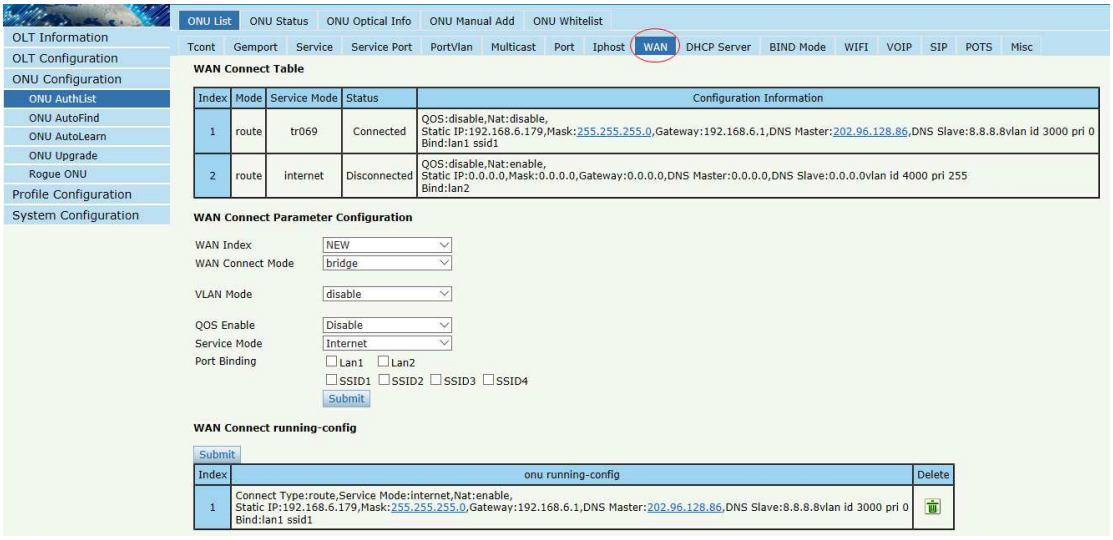


Figure 4.1-11: Configure WAN

4.1.1.1.10 DHCP Server

ONU Configuration→ONU AuthList→ONU List→Config→DHCP Server

ONU LAN and DHCP server are configured by private OMCI between OLT and ONU. When the connected ONU supports this function, the option "DHCP Server" can be shown on this page.

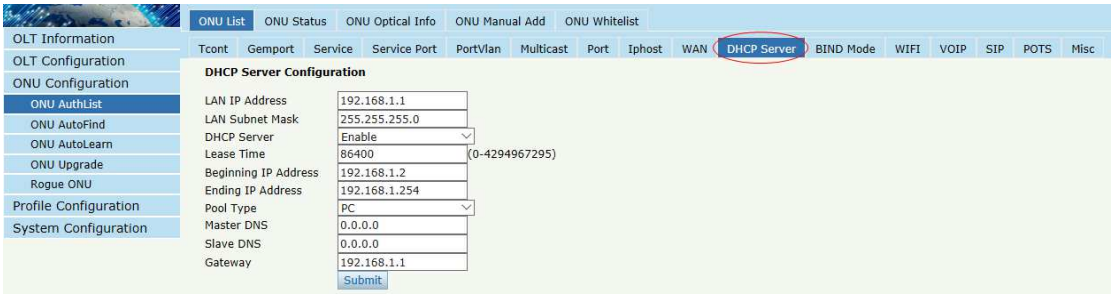


Figure 4.1-12: ONU DHCP Server

4.1.1.1.11 Bind Mode

ONU Configuration→ONU AuthList→ONU List→Config→BIND Mode

ONU LAN bind mode is configured by private OMCI between OLT and ONU. When the connected ONU supports this function, the option "Bind Mode" can be shown on this page.

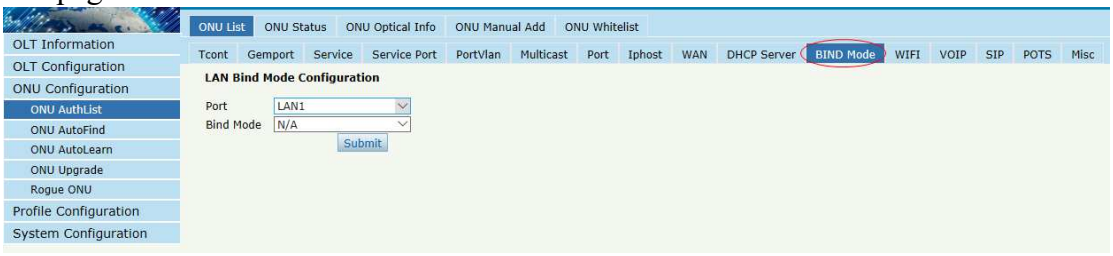


Figure 4.1-13: LAN Bind Mode Configuration

4.1.1.1.12 WIFI

ONU Configuration→ONU AuthList→ONU List→Config→WIFI

ONU WIFI is configured by private OMCI between OLT and ONU. When the connected ONU supports this function, the option "WIFI" can be shown on this page.

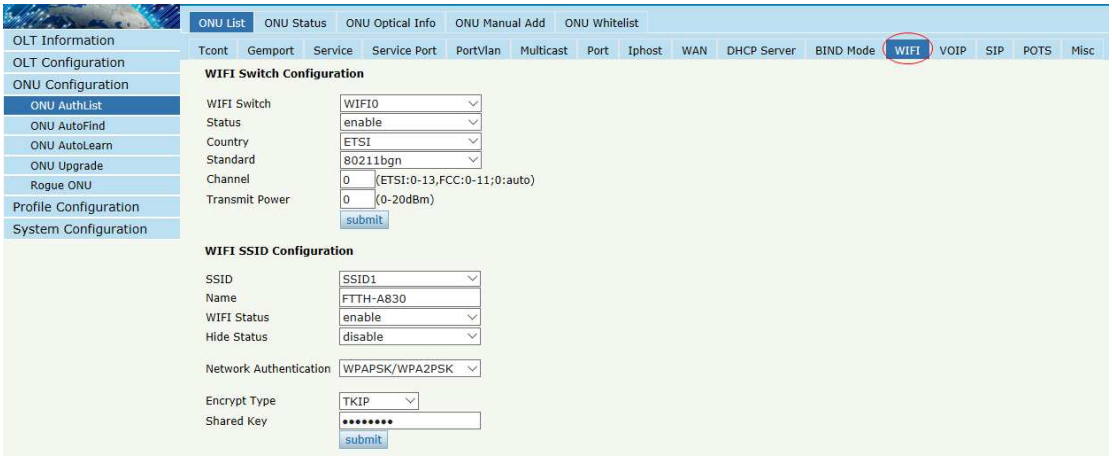


Figure 4.1-14: WIFI Configuration

4.1.1.1.13 VOIP

ONU Configuration→ONU AuthList→ONU List→Config→VOIP

This page shows WAN information of VOIP service, including IP address and VLAN. You can also operate VOIP module on this page. When the connected ONU supports VOIP, the option "VOIP" can be shown on this page.

Figure 4.1-15: Voice Wan Information

4.1.1.1.14 SIP

ONU Configuration→ONU AuthList→ONU List→Config→SIP

ONU VoIP SIP parameter can be configured on this page, including SIP server, proxy server, digit map and so on. When the connected ONU supports VOIP, the option "SIP" can be shown on this page.

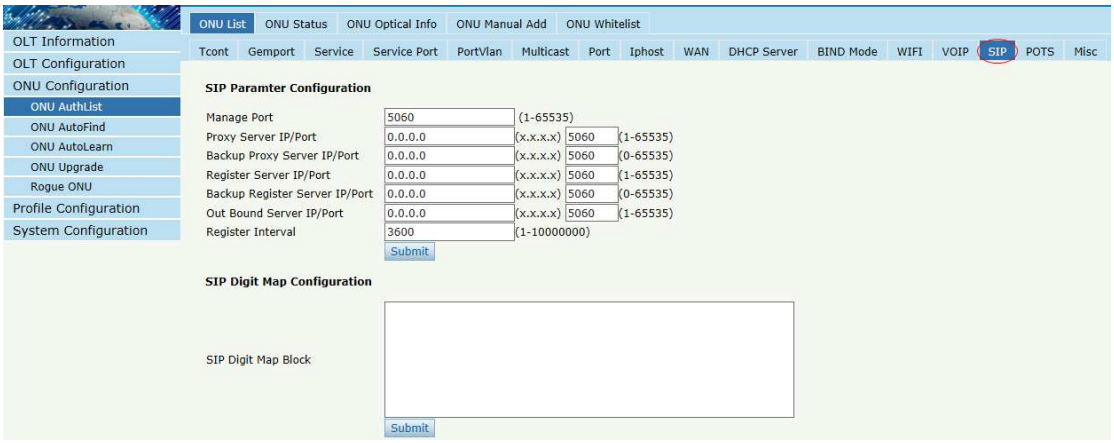


Figure 4.1-16: SIP Parameter

4.1.1.1.15 POTS

ONU Configuration→ONU AuthList→ONU List→Config→POTS

ONU VoIP POTS account, password and other VOIP parameters of POTS can be configured on this page; the length of SIP account can't be more than 16 bits. When the connected ONU supports VOIP, the option "POTS" can be shown on this page.

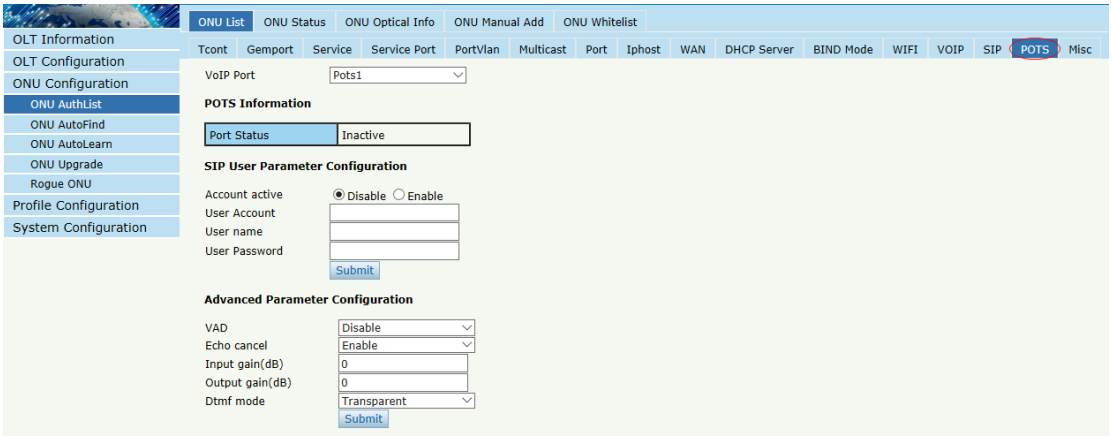


Figure 4.1-17: POTS Configuration

4.1.1.1.16 Misc

ONU Configuration→ONU AuthList→ONU List→Config→Misc

Misc includes other features of ONU which are configured by private OMCI.

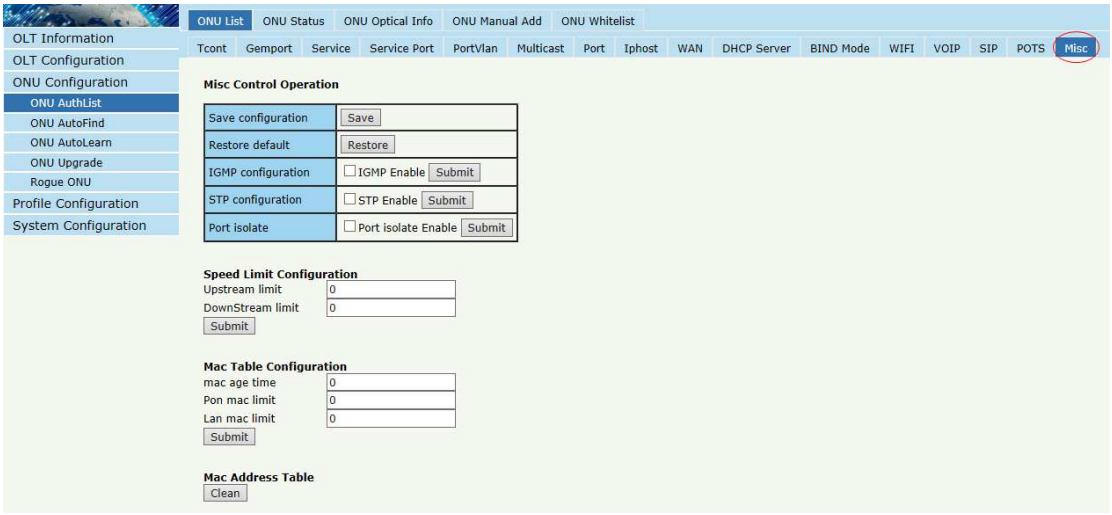


Figure 4.1-18: Misc Configuration

4.1.1.2 Deactivate

ONU Configuration→ONU AuthList→ONU List→Deactivate (Activate)

Deactivate ONU which you selected, the ONU will be disabled and the registration failed. Activate selected ONU, this ONU will register successfully.

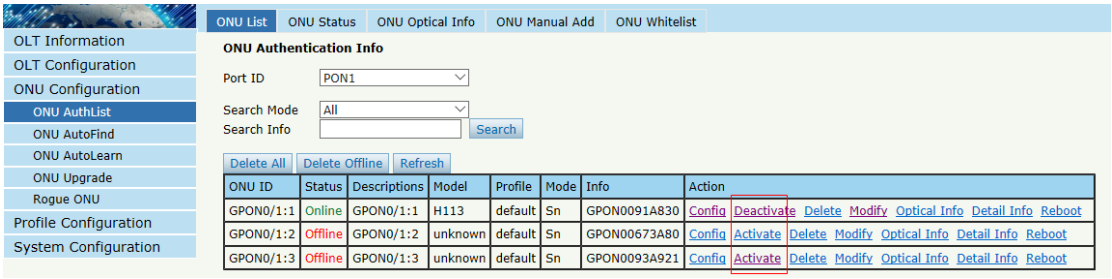


Figure 4.1-19: Deactivate/Activate ONU

4.1.1.3 Delete

ONU Configuration→ONU AuthList→ONU List→Delete

Delete ONU which you selected, the ONU will be deleted and the registration failed. All the configurations related this ONU will be deleted as well.

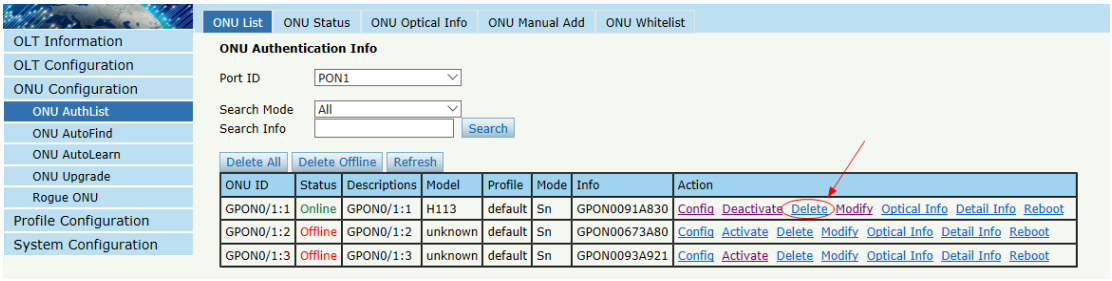


Figure 4.1-20: Delete ONU

4.1.1.4 Modify

ONU Configuration→ONU AuthList→ONU List→Modify

This is used to modify ONU authentication mode.

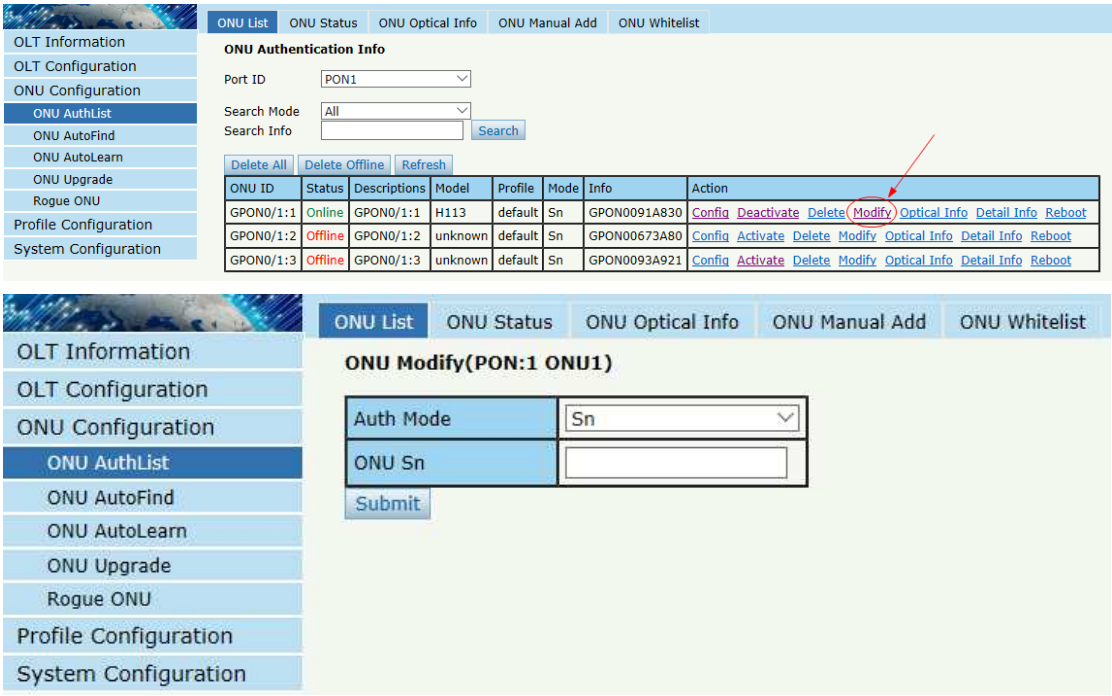
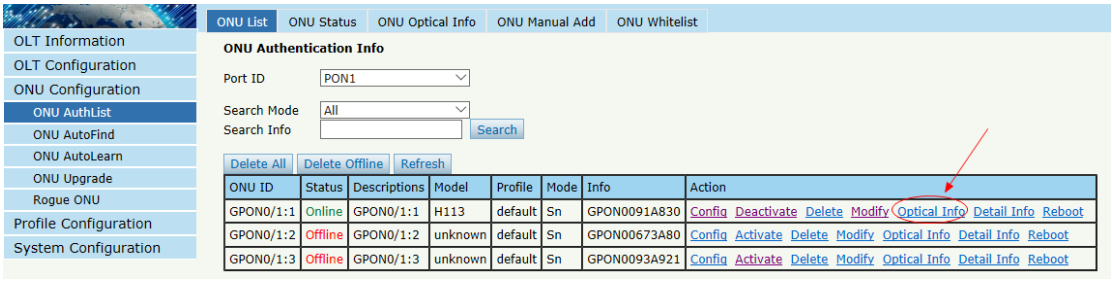


Figure 4.1-21: Modify ONU Authentication mode

4.1.1.5 Optical Info

ONU Configuration→ONU AuthList→ONU List→Optical Info

Check the Optical Information of ONU PON module which you selected.



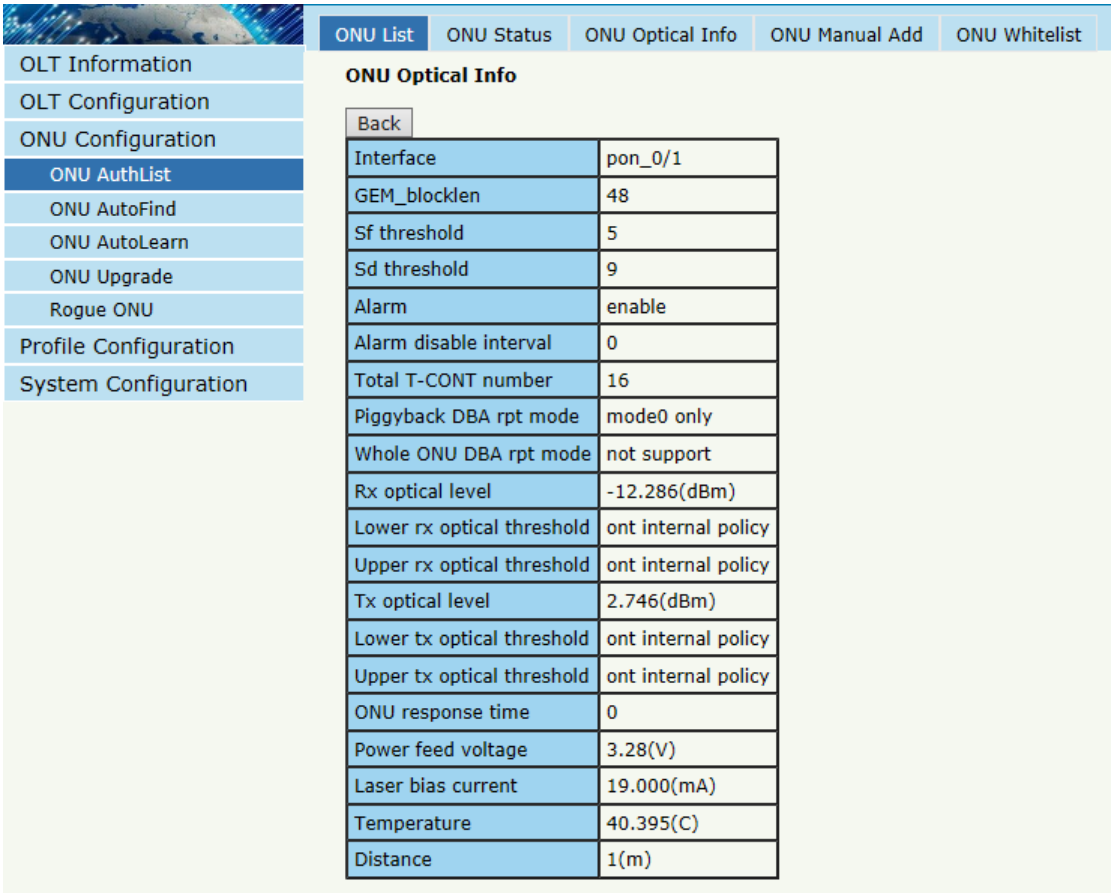
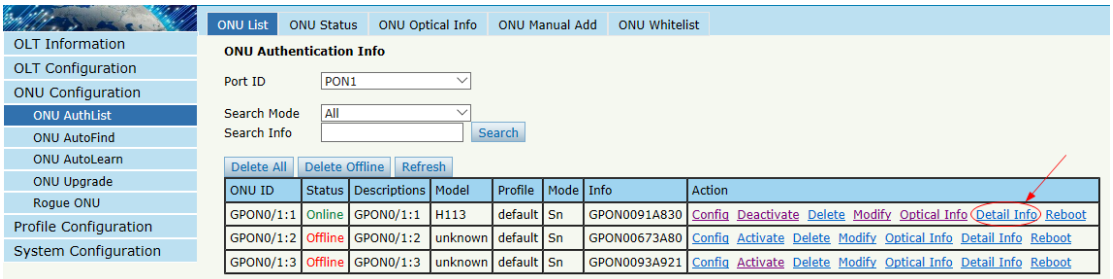


Figure 4.1-22: Optical info of ONU

4.1.1.6 Detail Info

ONU Configuration→ONU AuthList→ONU List→Detail Info

Check the Detail Info of ONU which you selected.



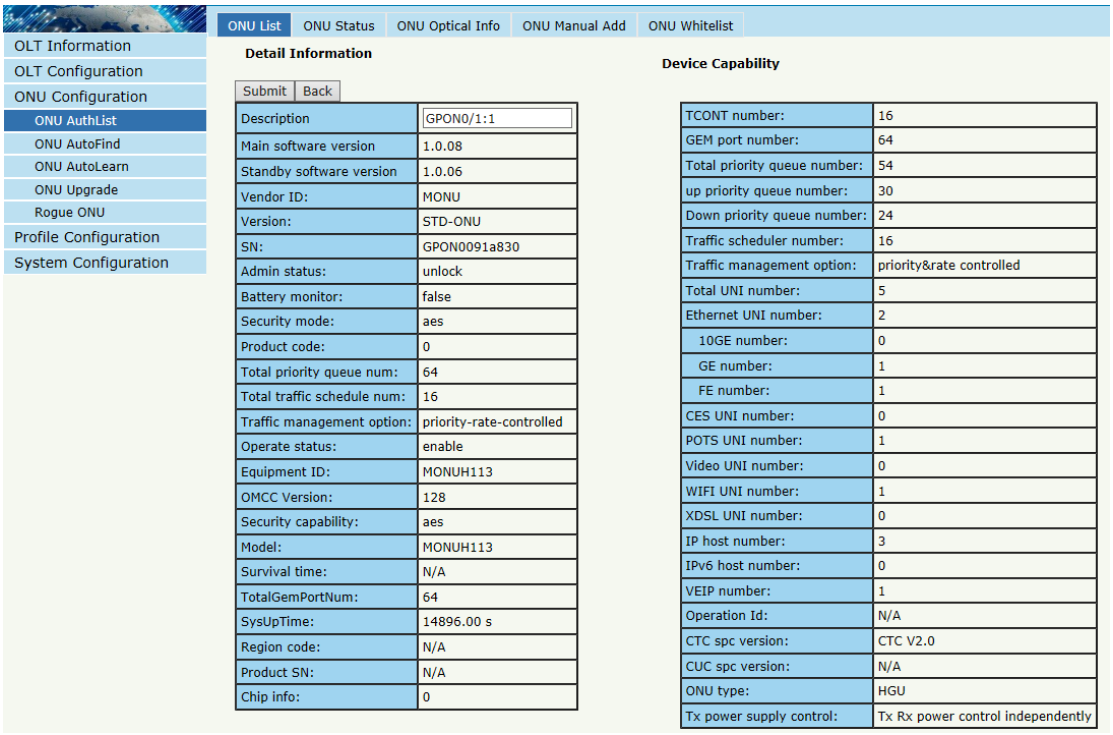


Figure 4.1-23: Detail info of ONU

4.1.1.7 Reboot

ONU Configuration→ONU AuthList→ONU List→Reboot

Reboot ONU which you selected.

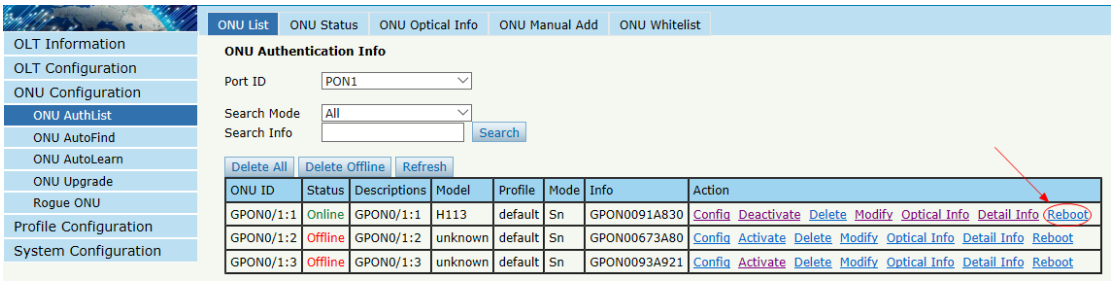


Figure 4.1-24: Reboot ONU

4.1.2 ONU Status

ONU Configuration→ONU AuthList→ONU Status

This pages shows the ONU information of the activity. User can check "Last Register Time", "Last Deregister Reason" and "Active Time" of each ONU.

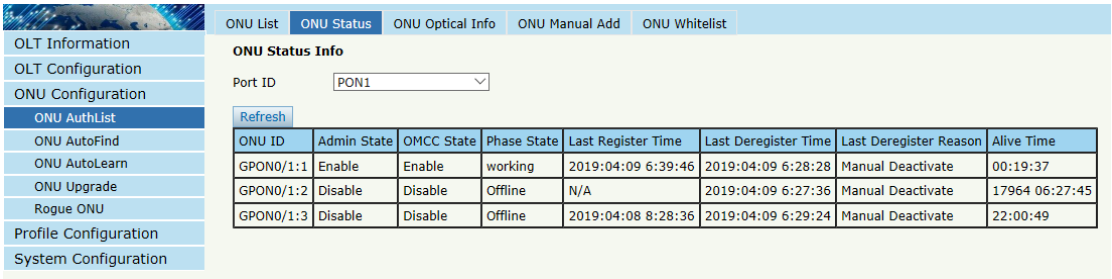


Figure 4.1-25: ONU Status

4.1.3 ONU Optical Info

ONU Configuration→ONU AuthList→ONU Optical Info

This page displays ONU Rx and Tx power. A batch of ONU optical power information can be shown in a list. Clearly to check the register power when register issue happens.

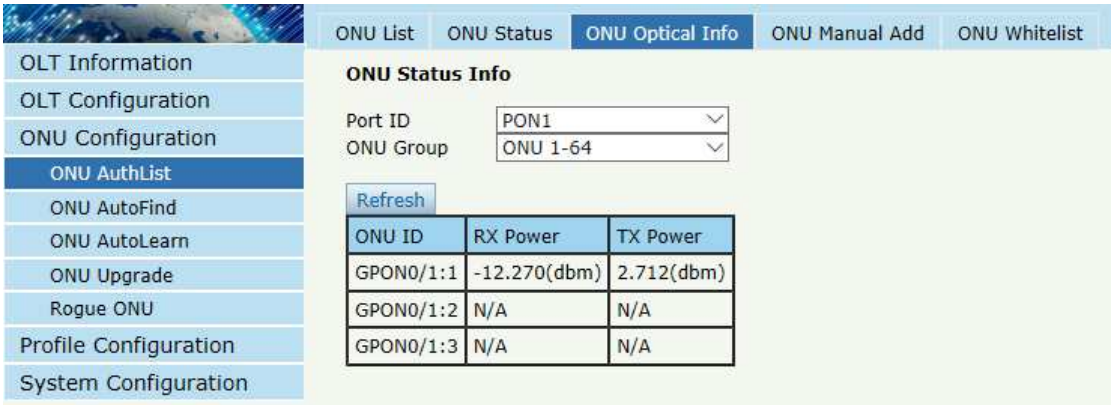


Figure 4.1-26: ONU Optical Info

4.1.4 ONU Manual Add

ONU Configuration→ONU AuthList→ONU Manual Add

You can manually add ONU to a selected PON port. ONU will appear in the ONU list after you added.

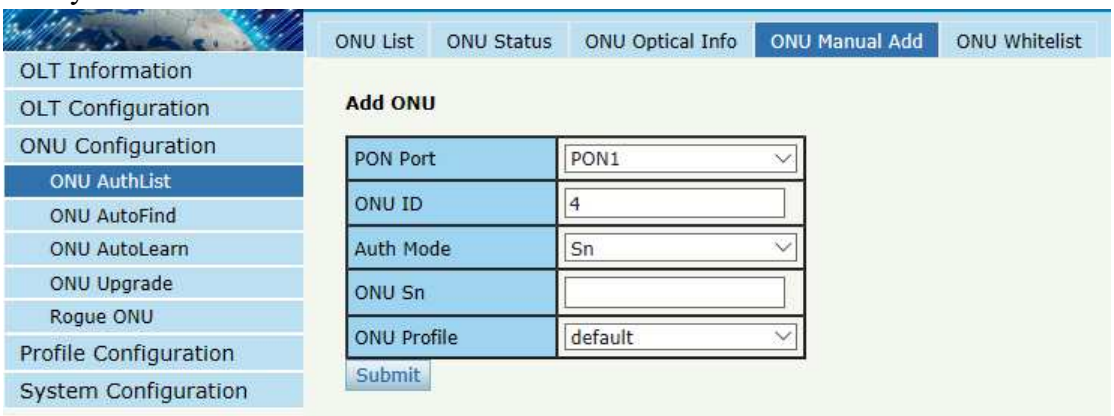


Figure 4.1-27: Add ONU Manually

4.1.5 ONU Whitelist

ONU Configuration→ONU AuthList→ONU Whitelist

You can set up whitelist on this page.

Whitelist can limit illegal ONU to register. Only the GPON SN in the whitelist can register, but only effective for the ONU which has not been added to OLT.

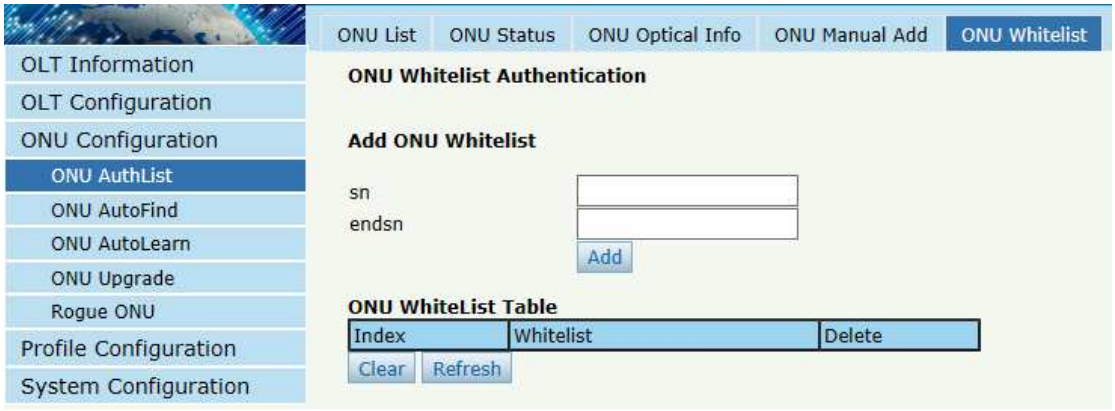


Figure 4.1-28: ONU Whitelist

4.1.6 ONU Statistics

ONU Configuration→ONU AuthList→ONU Statistics

This page displays the information of package count about ONU ports.

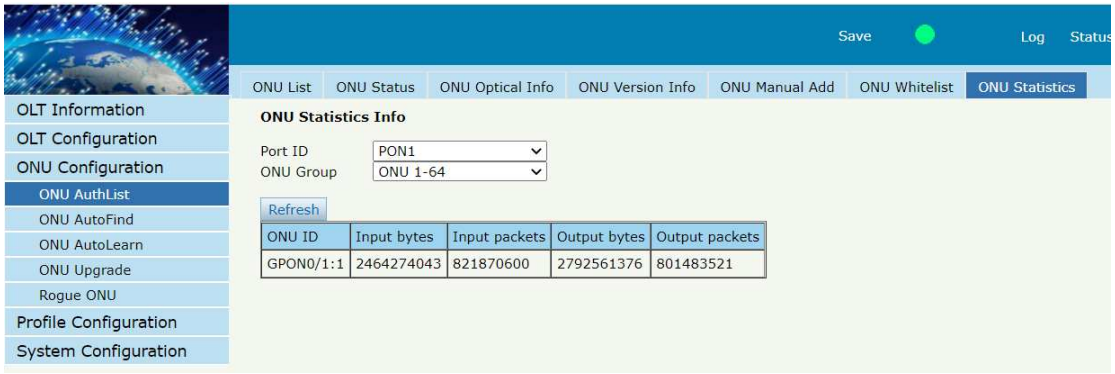


Figure 4.1-29: ONU Statistics

4.2 ONU AutoFind

4.2.1 ONU Discovery

ONU Configuration→ONU AutoFind→ONU Discovery

After selecting PON port number, all ONU which are authenticated failed or not authenticated will be displayed in this interface. You can check the serial number of ONU.

More information will be shown under the ONU Detail menu.

Figure 4.2-1: Automatic Discovery

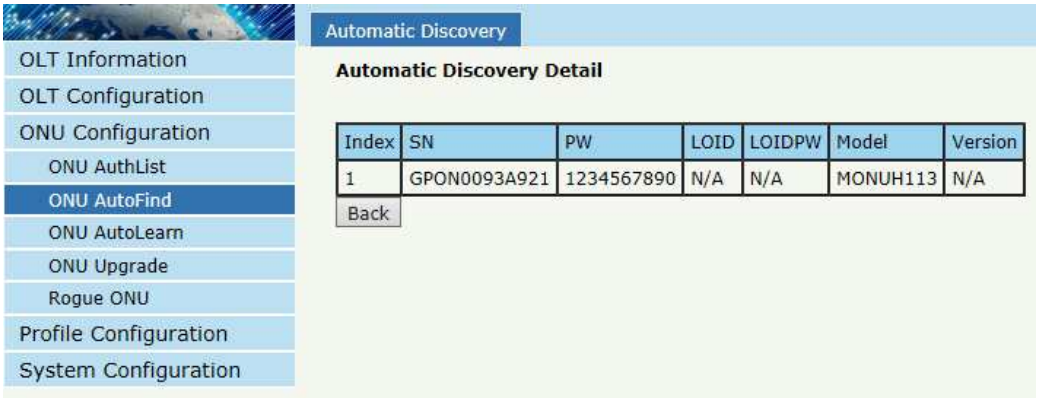


Figure 4.2-2: Detail info

4.2.2 Aging Time

ONU Configuration→ONU AutoFind→Aging Time

This interface is used to configure the aging time of the port AutoFind list.

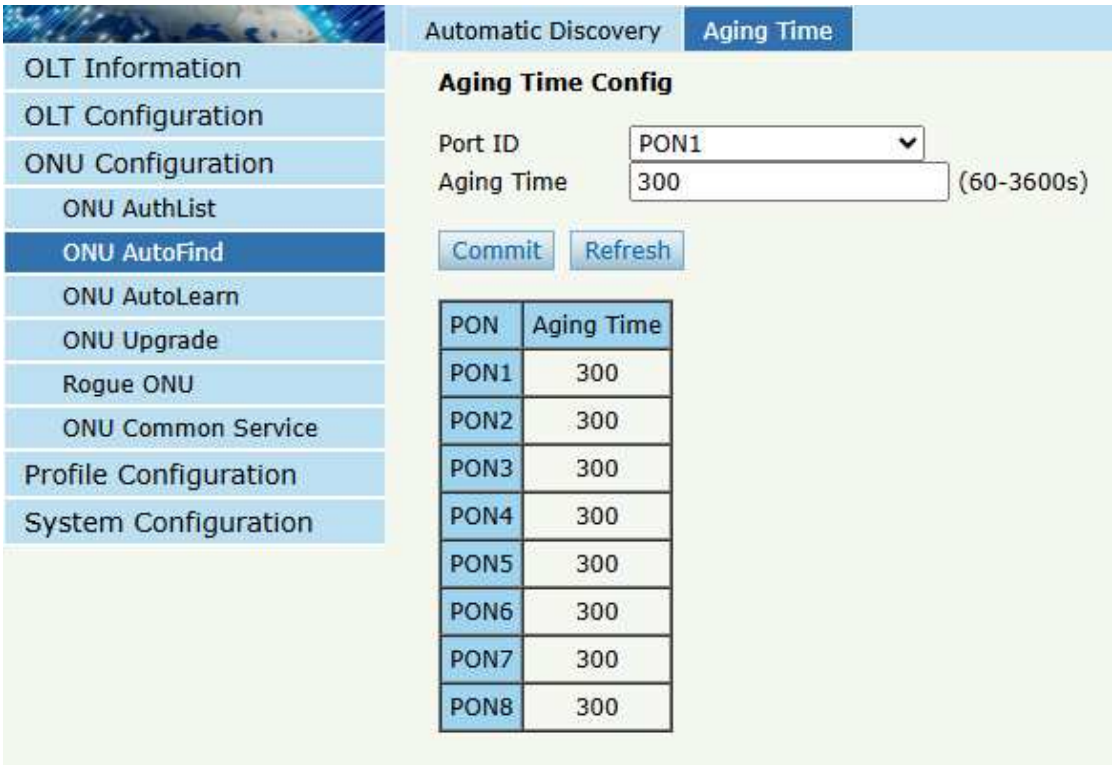


Figure 4.2-3: Aging Time

4.3 ONU AutoLearn

4.3.1 ONU AutoLearn

Configuration→AutoLearn→ONU AutoLearn

ONU can be authenticated automatically after enabling PON port automatic learning.

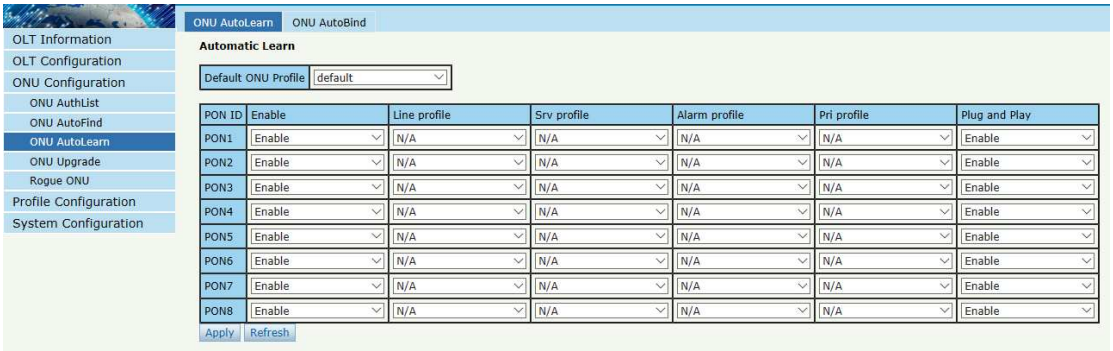


Figure 4.3-1: Automatic learn

4.3.2 ONU AutoBind

Configuration→AutoLearn→ONU AutoBind

Input the Equipment ID and bind the profile you need

Note: you must create profile first.

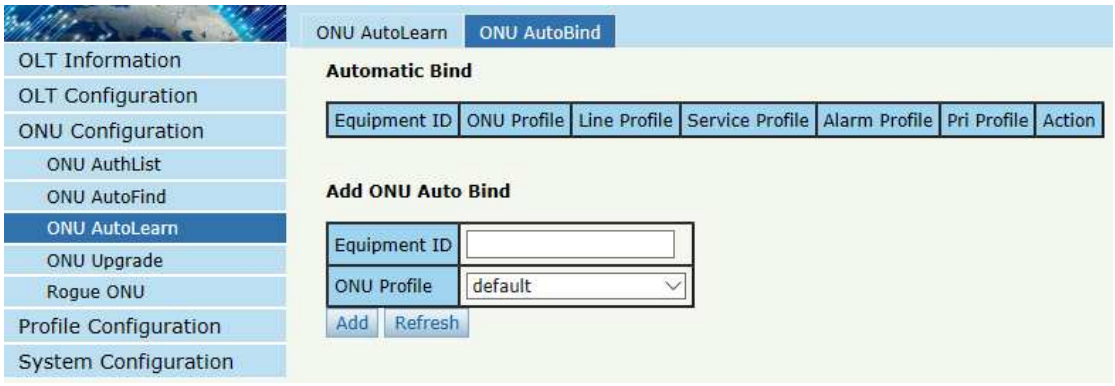


Figure 4.3-2: Bind profile

4.3.3 ONU AutoDelete

Configuration→AutoLearn→ONU AutoDelete

After this function is enabled, ONU registrations that are offline but remain offline for a certain period of time will be deleted.

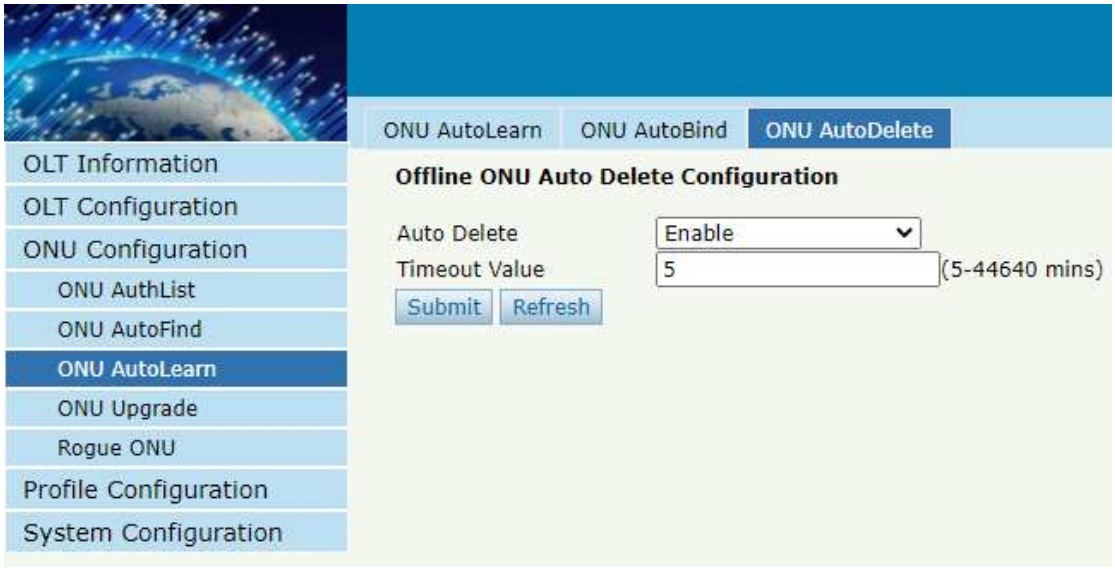


Figure 4.3-3: ONU AutoDelete

4.3.4 ONU Scheduled Reboot

ONU Configuration→ ONU AutoLearn→ ONU Scheduled Reboot

This interface is used to specify the scheduled reboot of the ONU.

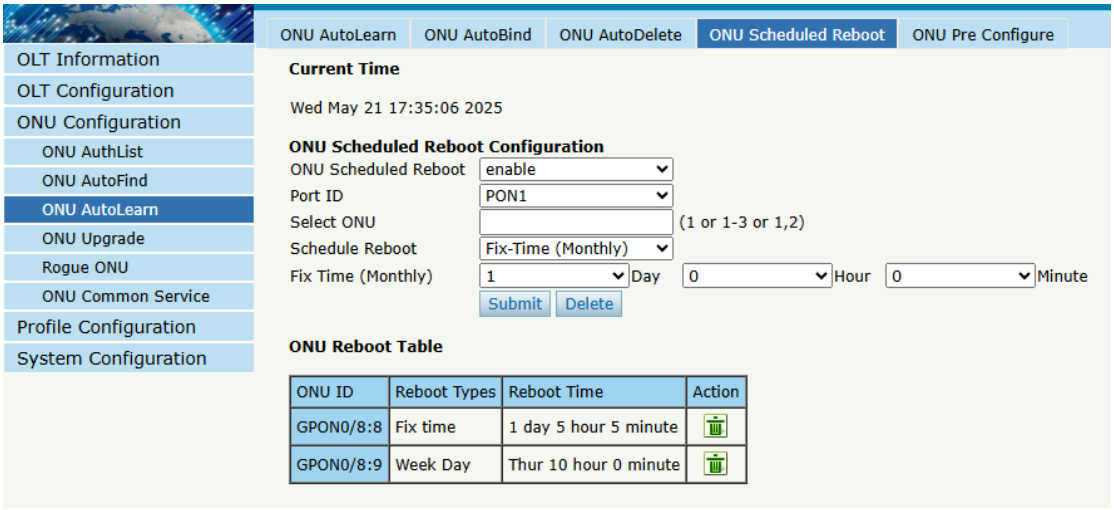


Figure 4.3-4: ONU Scheduled Reboot

4.3.5 ONU ONU Pre Configure

ONU Configuration→ ONU AutoLearn→ONU Pre Configure

ONU Pre Configure supports binding templates to specified batch ONU. When an ONU is authenticated and successfully registered and launched, templates will be automatically bound according to ONU Pre Configure. Its priority is higher than that of the PON port-based binding template in ONU Autolearn.

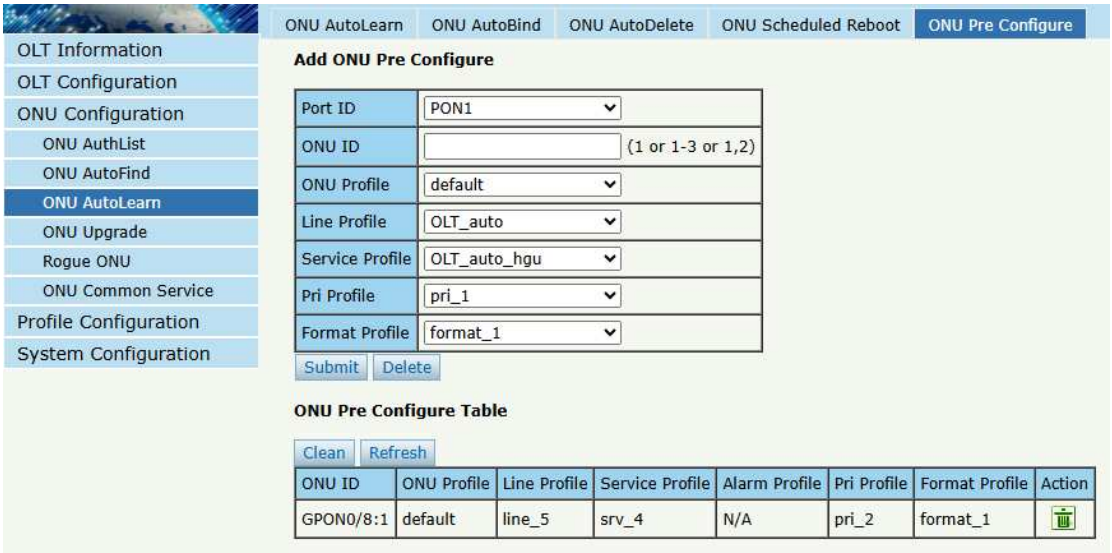


Figure 4.3-5: ONU Pre Configure

4.4 ONU Upgrade

ONU firmware can be upgraded by OLT. OLT supports manual upgrade and automatic upgrade.

4.4.1 UpLoad Image

Configuration→ONU Upgrade→ONU Image

Upload ONU firmware image which you need, the image will upload to OLT RAM.

Figure 4.4-1: Upload image

4.4.2 Manual Upgrade

Configuration→ONU Upgrade→Manual Upgrade

Select the ONU image and the ONU that need upgrade, click commit button to start upgrading. You can upgrade the ONU under one PON port every time.

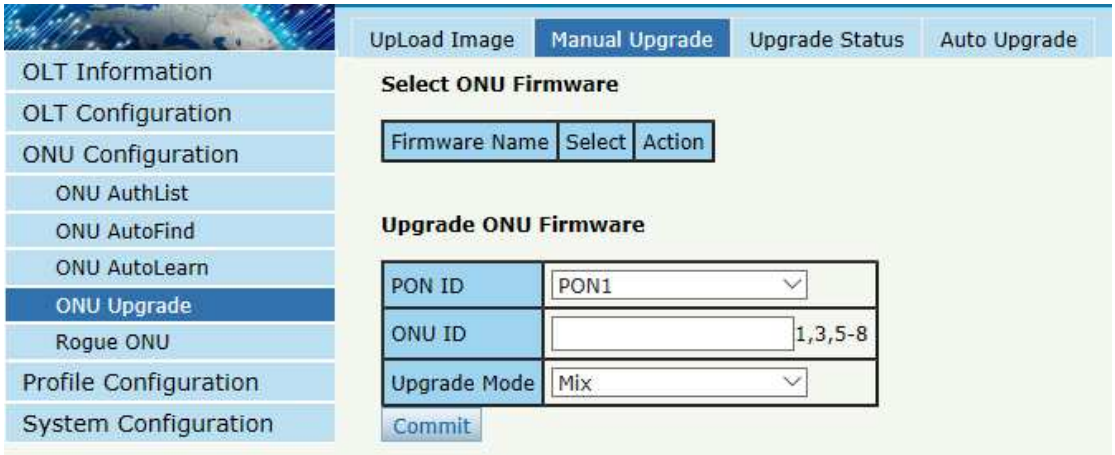


Figure 4.4-2: Manual Upgrade

4.4.3 Upgrade Status

Configuration→ONU Upgrade→Upgrade Status

When ONU is upgrading, the upgrading status will be shown on this page.

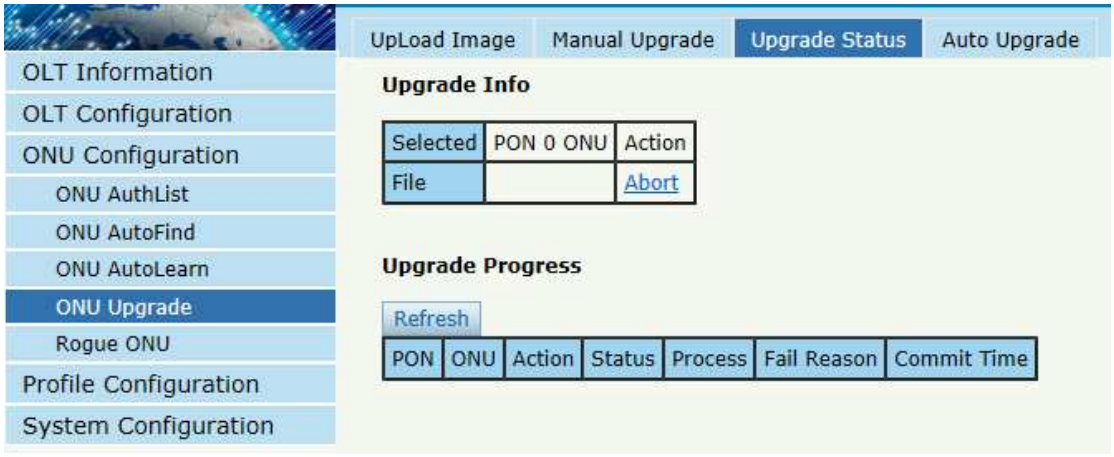


Figure 4.4-3: ONU Upgrade Status

4.4.4 Auto Upgrade

Configuration→ONU Upgrade→Auto Upgrade

After uploaded the ONU firmware image, configured automatic upgrade conditions, once the ONU which has the same equipment ID and different software version come online, they will be upgraded automatically.

Each ONU has its own equipment ID, which you can check in ONU detail info. Software version is the firmware image version which has uploaded to the OLT.

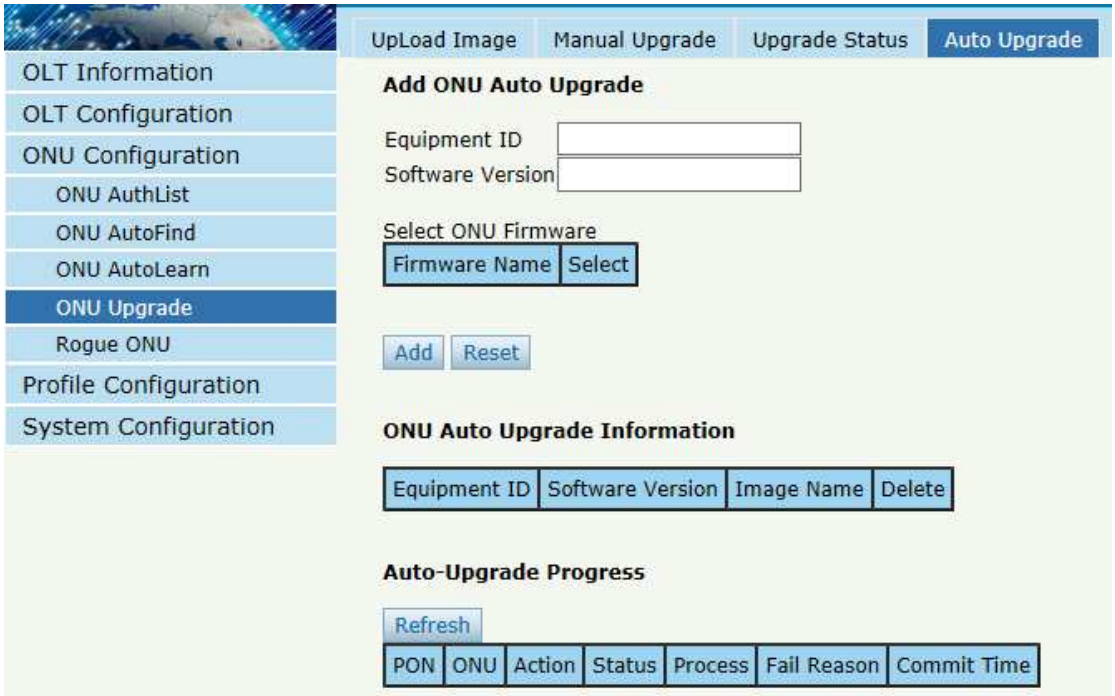


Figure 4.4-4: Auto Upgrade

4.4.5 Auto Upgrade Status

Configuration→ONU Upgrade→Auto Upgrade Status

When ONU is auto upgrading, the upgrading status will be shown on this page.

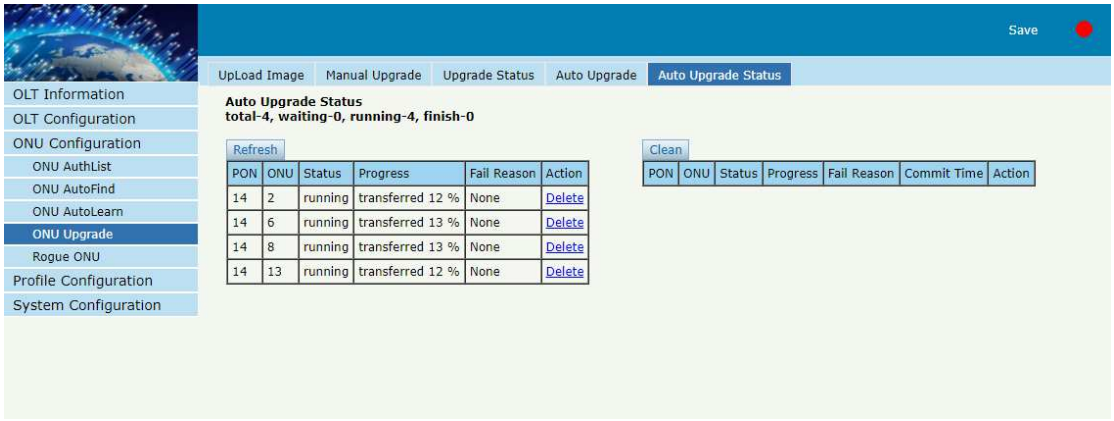


Figure 4.4-5: Auto Upgrade Status

4.5 Rogue ONU

ONU Configuration→Rogue ONU

After enabled rogue ONU detect, if there is a rogue ONU trying to register, it will appear in the list.

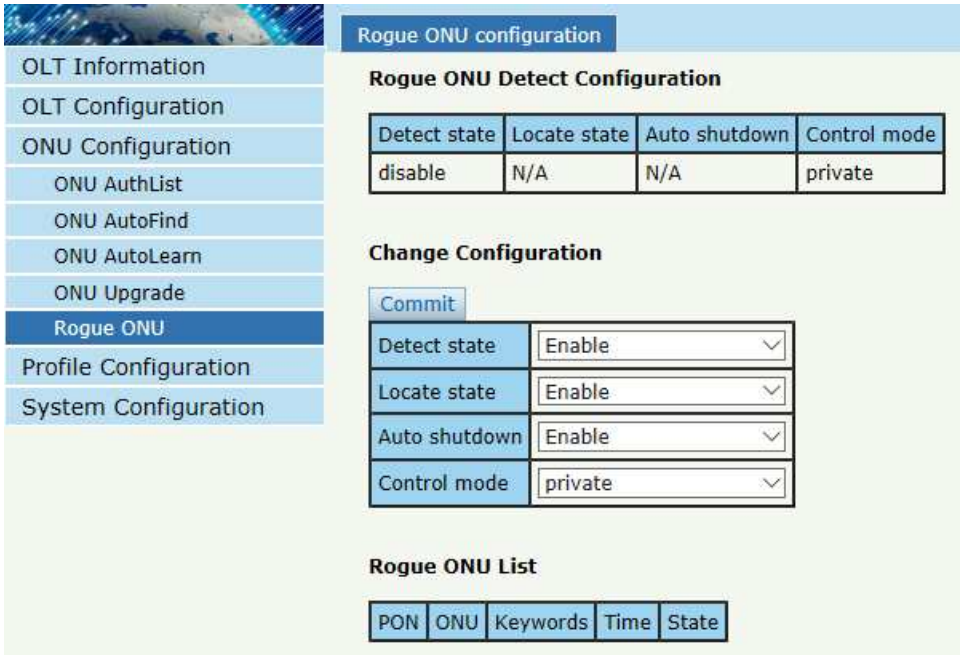


Figure 4.5-1: Rogue ONU detect

4.6 ONU Common Service

ONU Configuration→ONU Common Service

You have more flexibility to create Tcont ID and other items for the specified ONU you select.

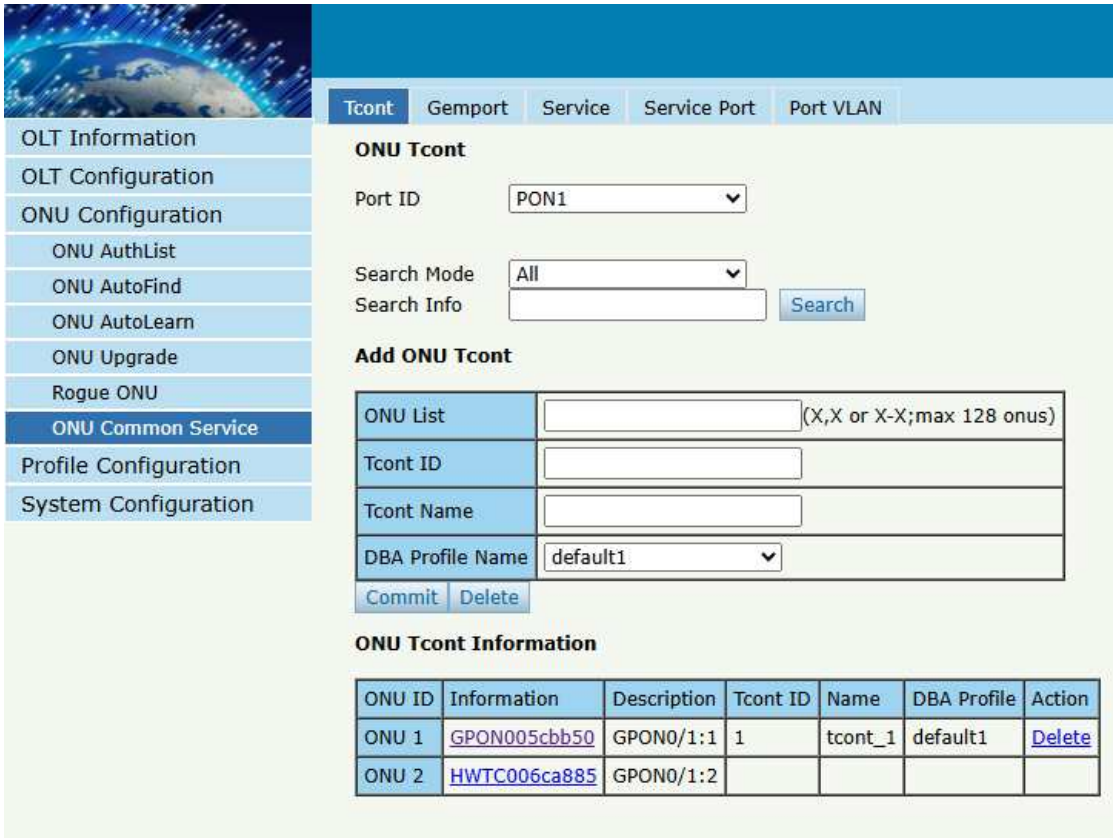


Figure 4.6-1: ONU Common Service

Chapter 5 Profile Configuration

This chapter is about the ONU profile configuration. It is designed for batch ONU management by OLT.

5.1 ONU Profile

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

5.1.1 Information

Profile Configuration→ ONU profile→Information
The table displays ONU profile list. You can also do some operations, such as delete and check details info.

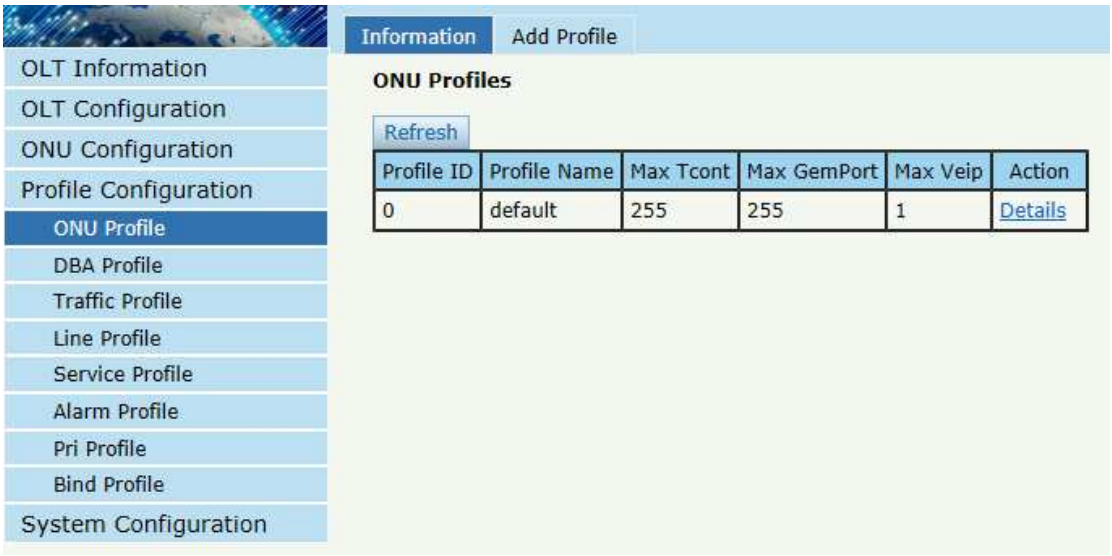


Figure 5.1-1: ONU profile list

5.1.2 Add profile

Create a new ONU profile what you need. Generally, ONU has two different modes.
SFU mode (only using bridge mode):
Usually, only need to set correct eth port and POTS port number of ONU, others can be kept default.

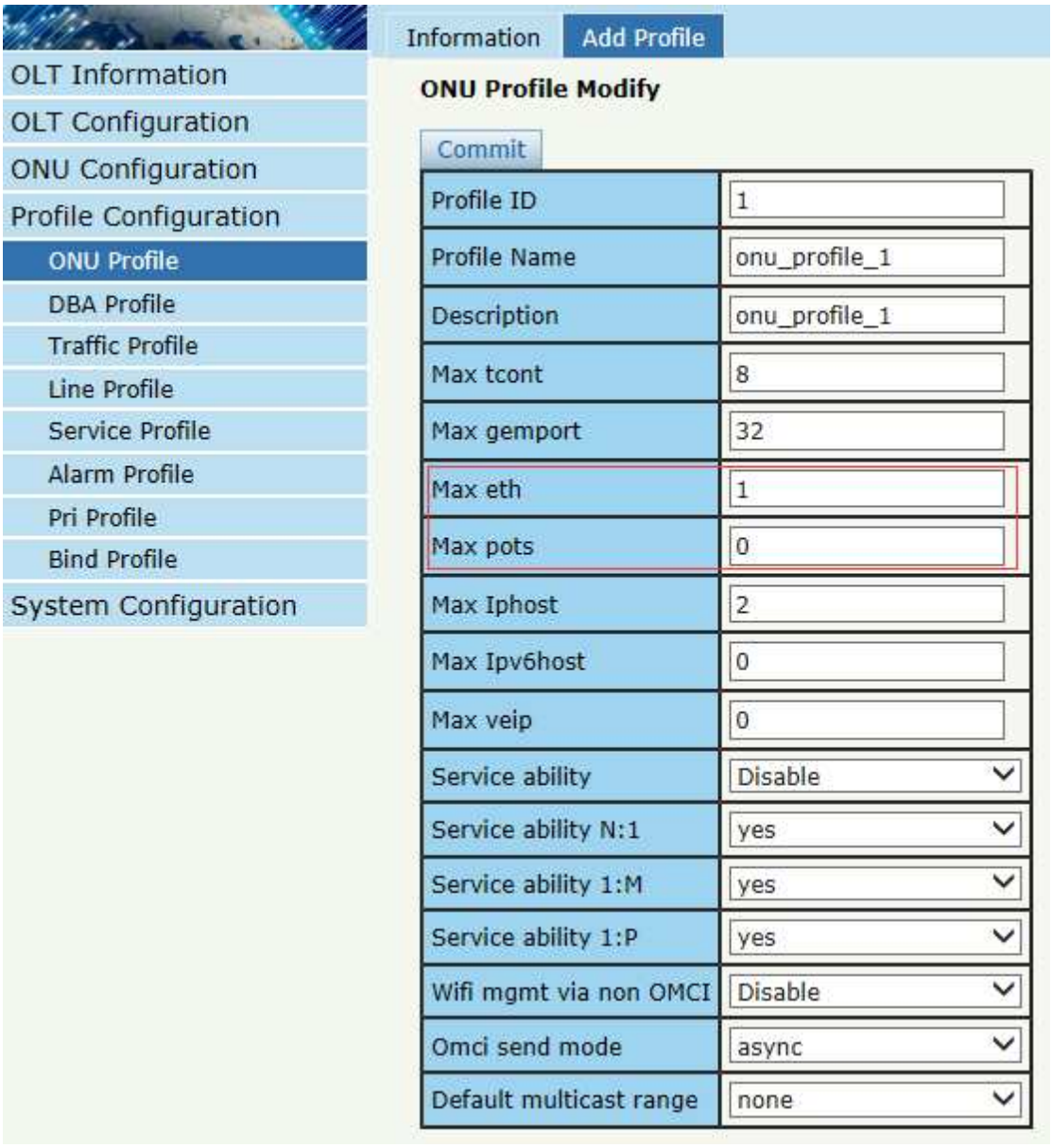


Figure 5.1-2: Add SFU profile

HGU mode (with the routing wan connection mode):
For HGU mode, need to set correct eth port and POTS port number and set veip to be 1, keep others default.

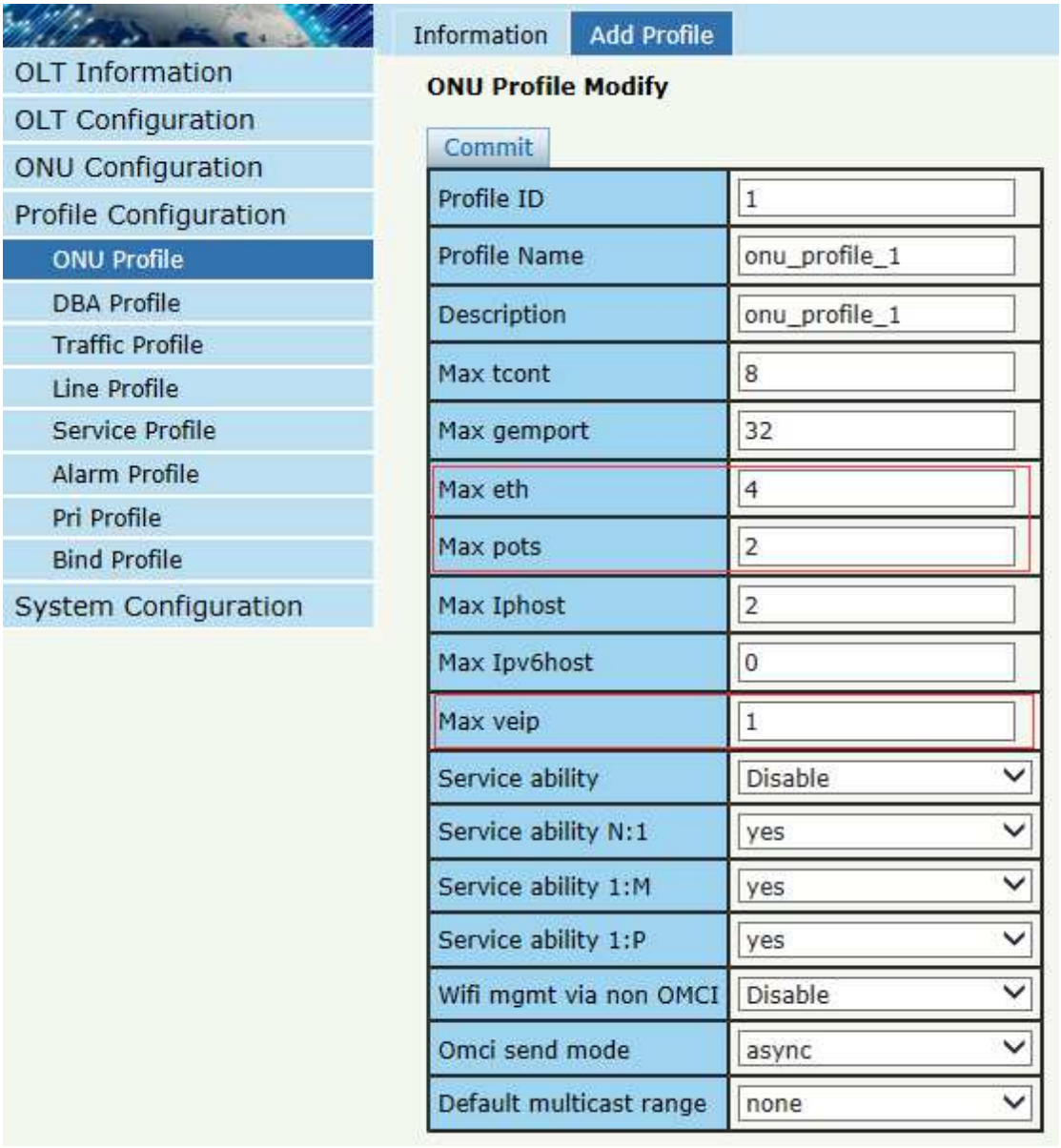


Figure 5.1-3: Add HGU profile

5.2 DBA Profile

DBA is a bandwidth allocation strategy that changes uplink bandwidth assigned to each T-CONT in real time according to the instant service status of each ONU. There are five BW types supported and make sure that fixed <= assured <= max.

5.2.1 DBA profiles

Profile Configuration→DBA Profile →DBA Profiles

The table displays DBA profile list. You can also do some operations, such as delete and modify.

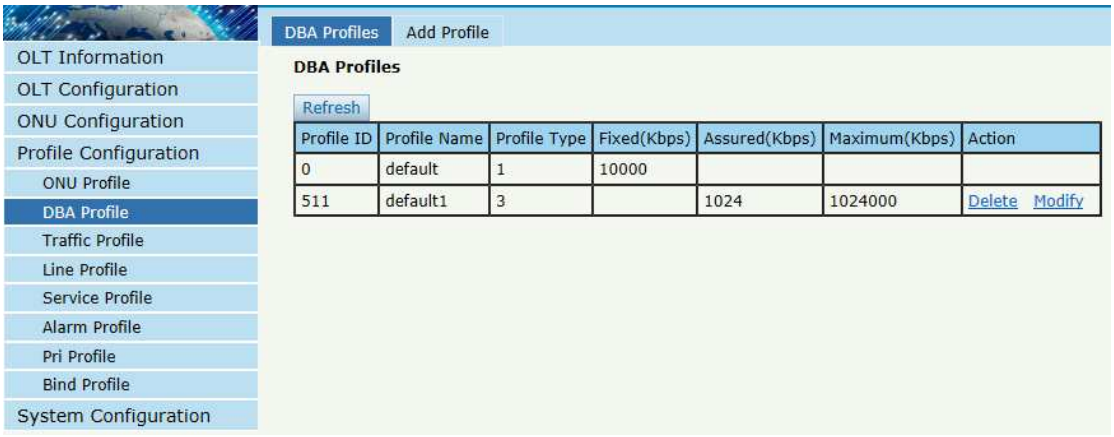


Figure 5.2-1: DBA profile list

5.2.2 Add profile

Profile Configuration→DBA Profile → Add profile

There are five types of DBA profile. In general, we use type3.

Type	Fixed	Assured	Maximum
Type_1	√		
Type_2		√	
Type_3		√	√
Type_4			√
Type_5	√	√	√

Table 5.2-1 DBA profile types

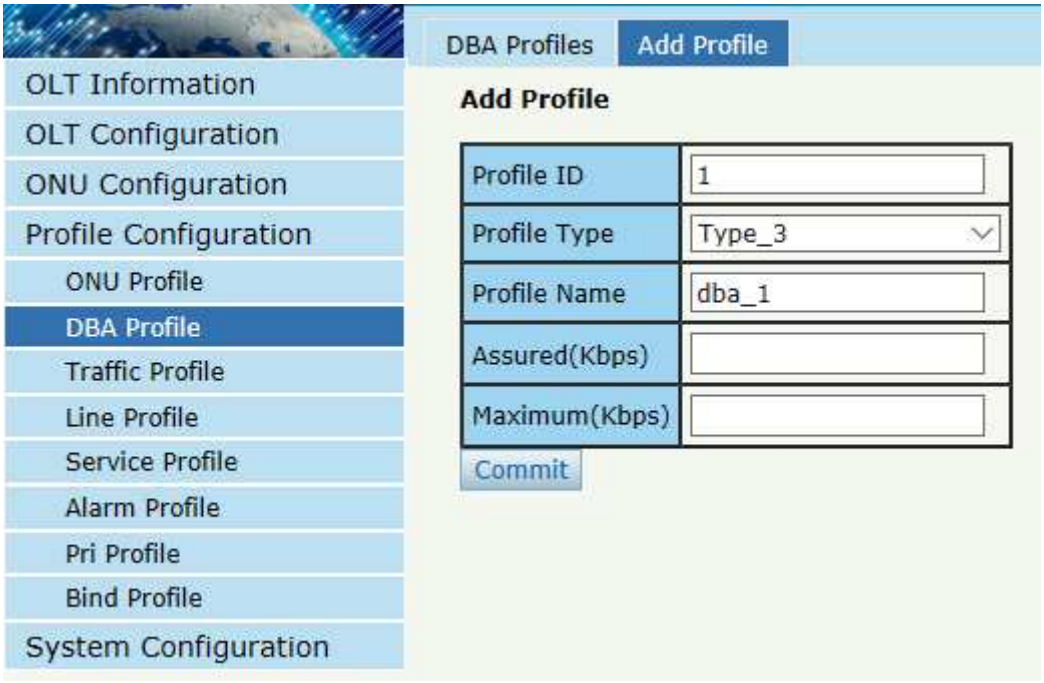


Figure 5.2-2: Add a DBA profile

5.3 Traffic Profile

Traffic profile is used by Gemport to specify the upstream/downstream bandwidth.

5.3.1 Traffic profiles

Profile Configuration→Traffic Profile → Traffic Profiles

The table displays Traffic profile list. You can also do some operation, such as delete and modify.

Figure 5.3-1: Traffic Profile list

5.3.2 Add profile

Profile Configuration→Traffic Profile → Add Profile
Configure Gemport to specify the upstream/downstream bandwidth.
SIR: Committed Information Rate
PIR: Peak Information Rate
CBS: Committed Burst Size
PBS: Peak Burst Size

Figure 5.3-2: Add a traffic Profile

5.4 Line Profile

Line profile is used to configure the ANI side services of ONU such as t-cont, gem-port, service-port, and so on.

5.4.1 Line profile

Profile Configuration→Line Profile → Line Profile
The table displays Line profile list. You can also do some operations, such as delete and modify.

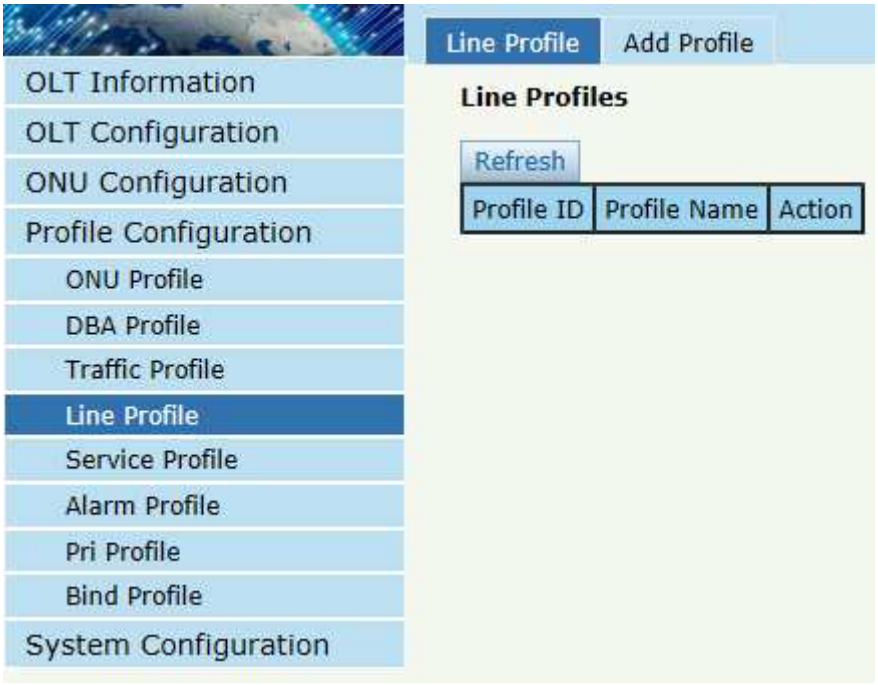


Figure 5.4-1: Line Profile list

5.4.2 Add profile

Profile Configuration→Line profile→Add profile

Create a new line profile.

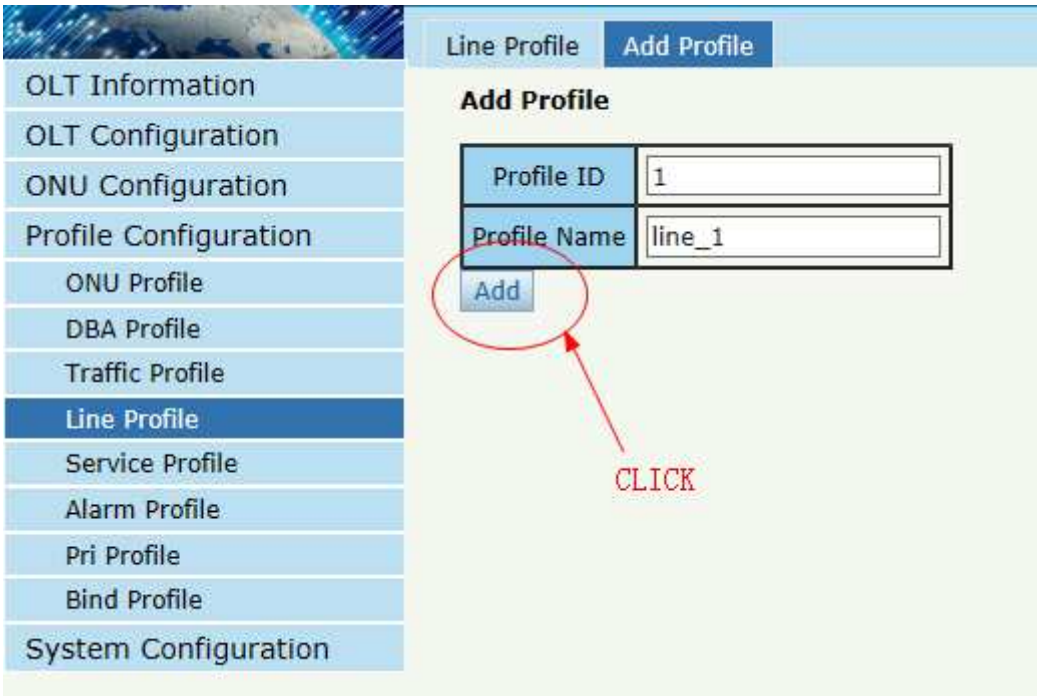


Figure 5.4-2: Add Line Profile

Modify the line profile parameters.

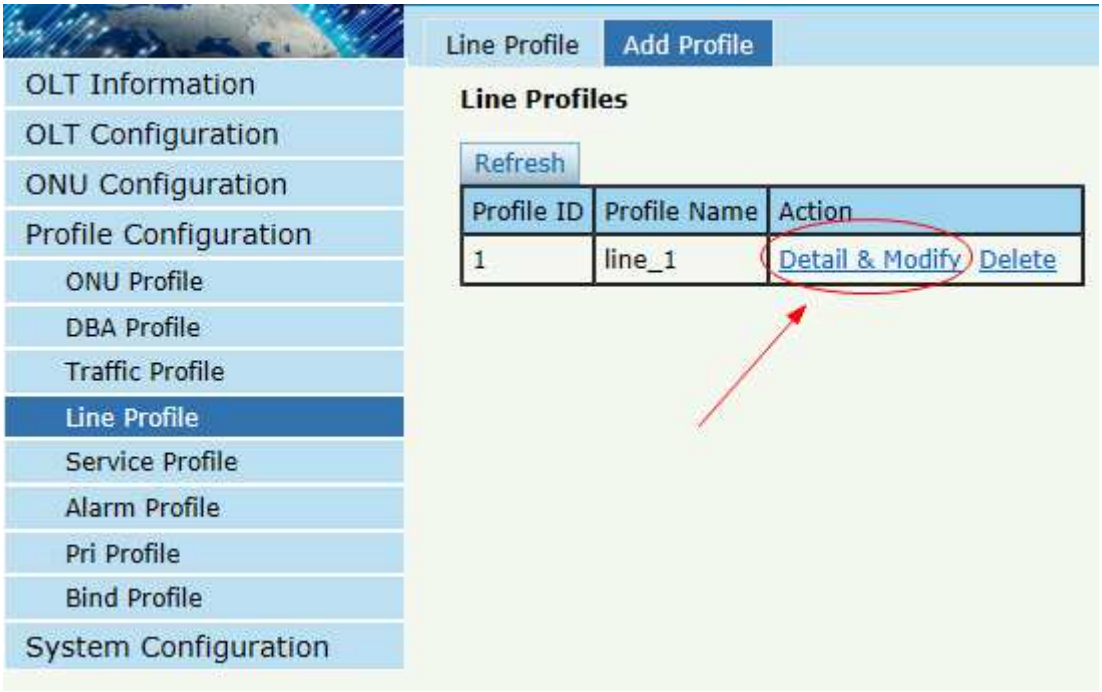


Figure 5.4-3: Modify Line Profile

5.4.2.1 Tcont

Add Tcont ID and bind DBA profile.

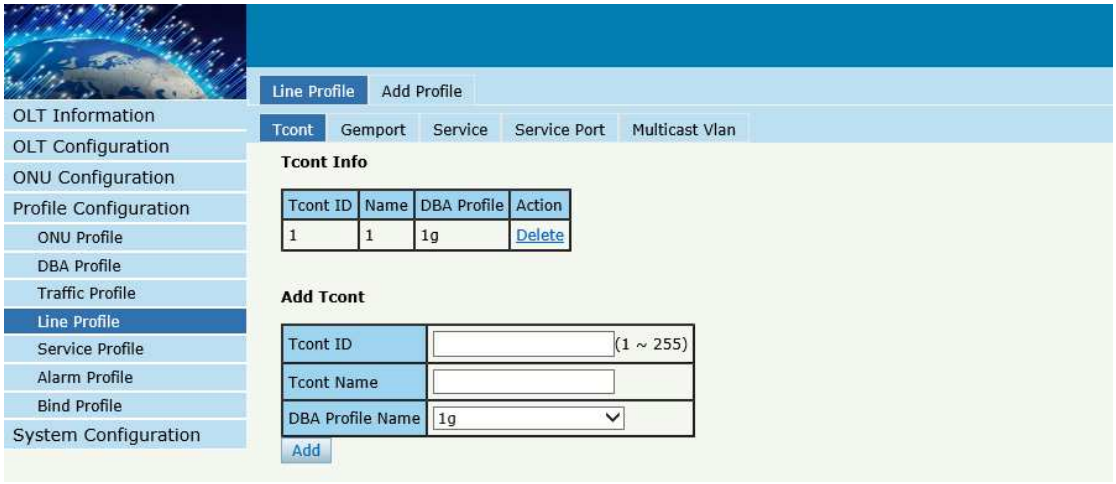


Figure 5.4-4: Add Tcont

5.4.2.2 Gemport

Add Gemport ID and bind Tcont ID.

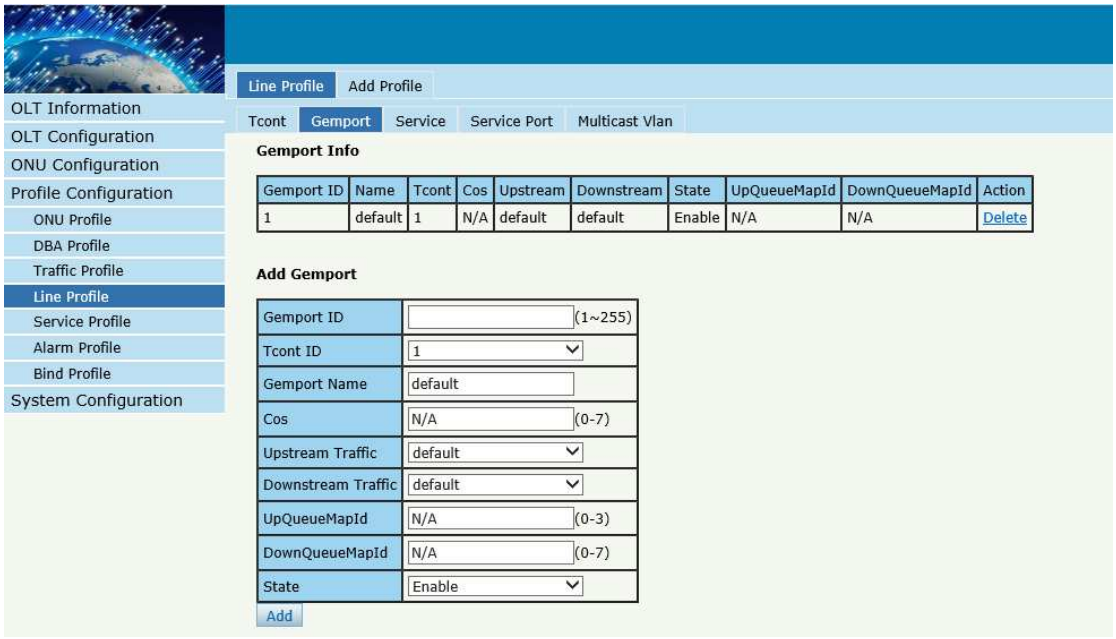


Figure 5.4-5: Add Gemport

5.4.2.3 Service

Add service, set the VLAN mode and VLAN ID and bind one Gemport ID.

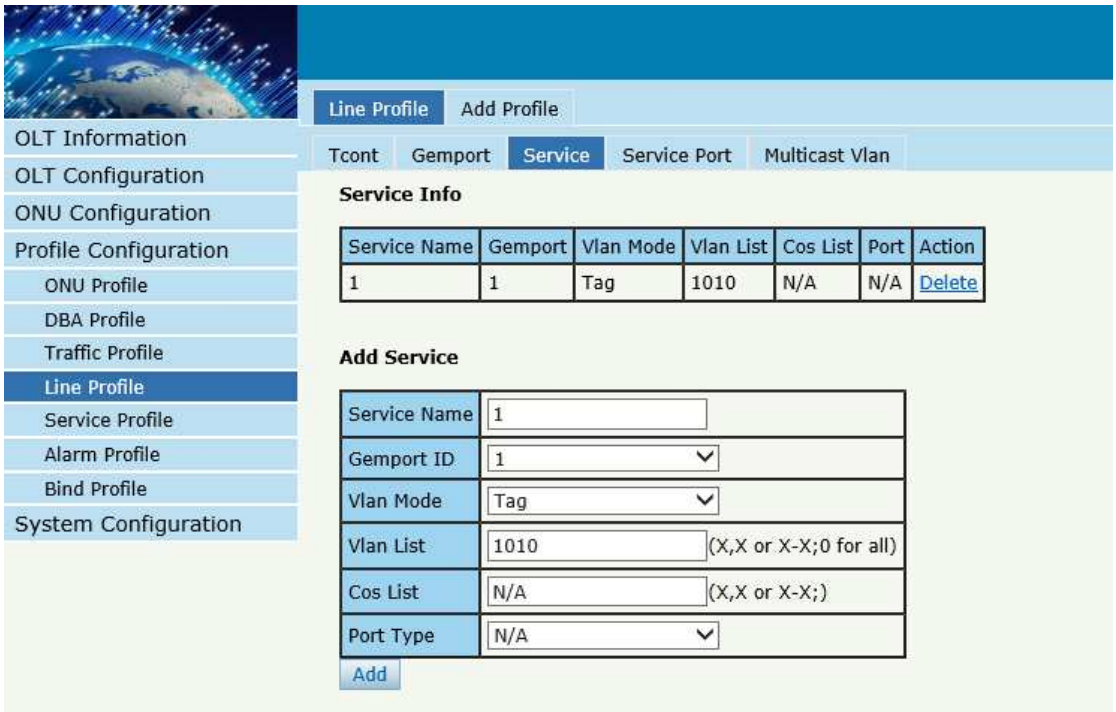


Figure 5.4-6: Add Service

5.4.2.4 Service Port

Create a service port, set the user VLAN and translate VLAN and bind one Gemport ID. If don't need VLAN translation, just set translate VLAN the same as user VLAN.

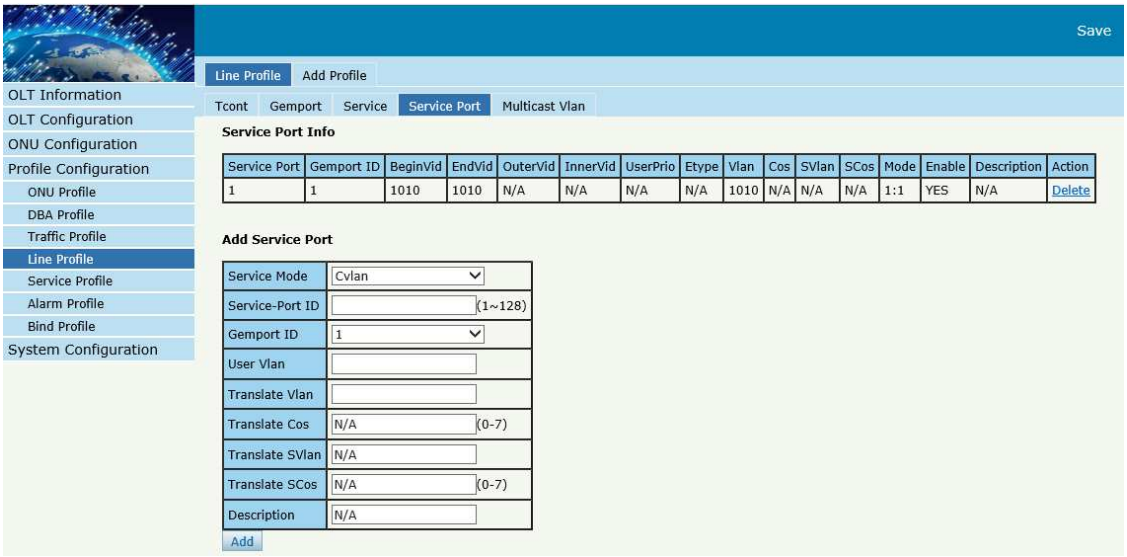


Figure 5.4-7: Add Service Port

5.4.2.5 Multicast VLAN

Set the Multicast VLAN of ONU.

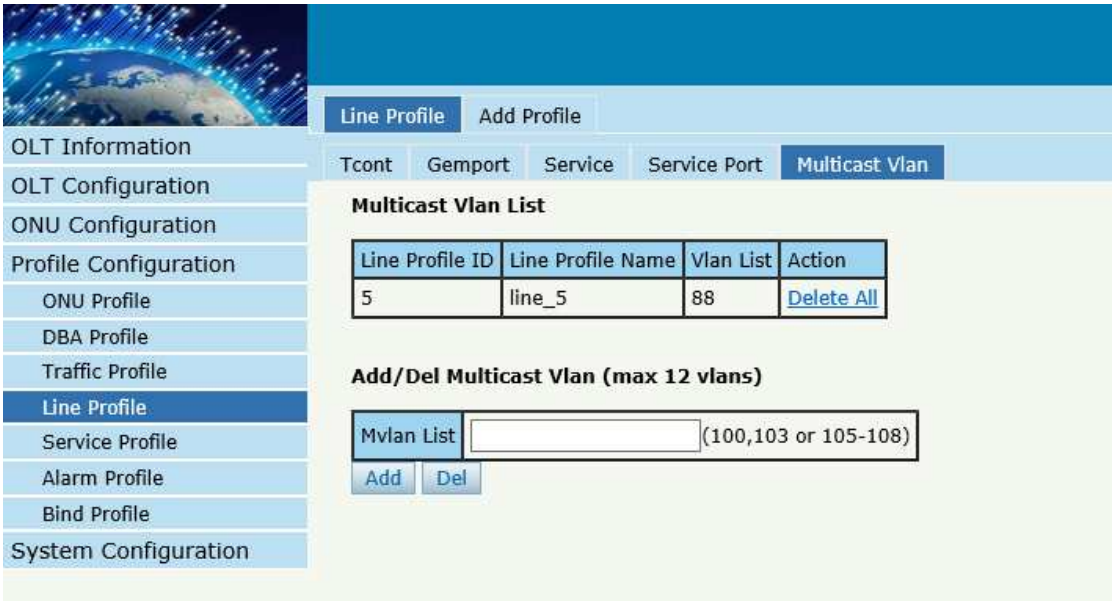


Figure 5.4-8: Configure Multicast VLAN

5.5 Service Profile

Service profile is used to configure the UNI side services of ONU, such as Ethernet port, wifi, veip, and so on.

5.5.1 Service profile

Profile Configuration→Service Profile → Service Profile
The table displays service profile list. You can also do some operations, such as delete and modify.

Figure 5.5-1: Service Profile List

5.5.2 Add profile

Profile Configuration→Service Profile →Add Profile
Add a new service profile.

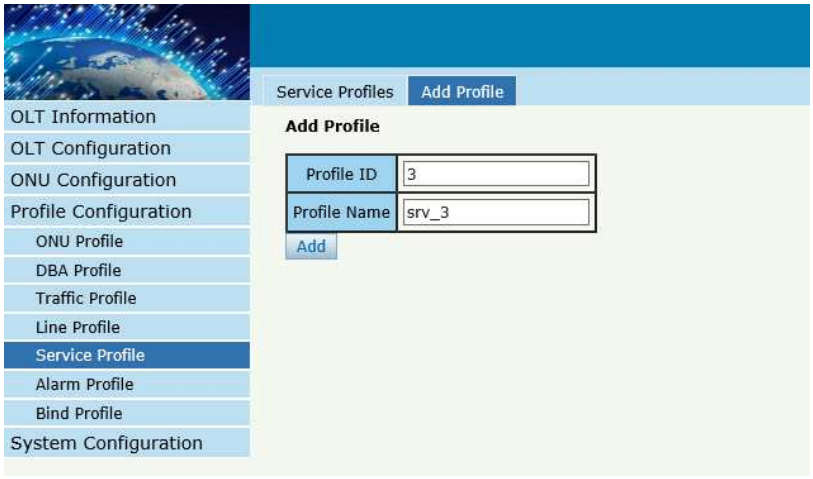


Figure 5.5-2: Add Service profile

Figure 5.5-3: Modify Service Profile

5.5.2.1 PortVlan

Set the VLAN mode of the ONU port. For HGU, need to configure veip 1 transparent; for SFU, configure Ethernet port directly.

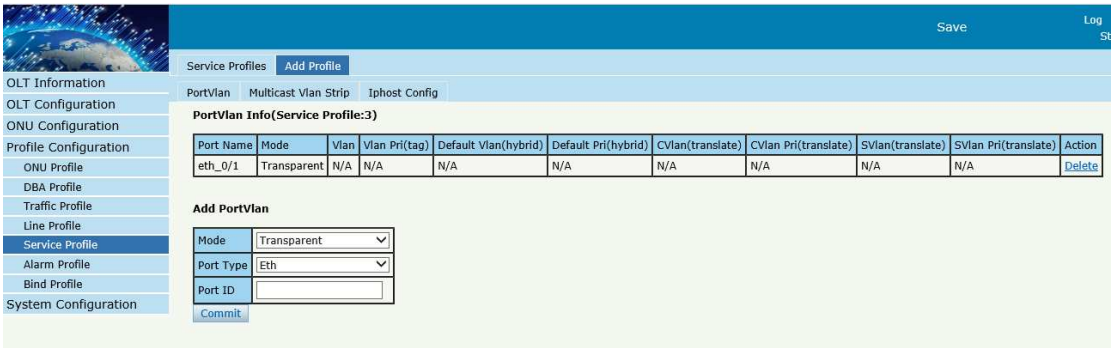


Figure 5.5-4: Port VLAN mode

5.5.2.2 Multicast VLAN Strip

Set the multicast VLAN mode of ONU's port.

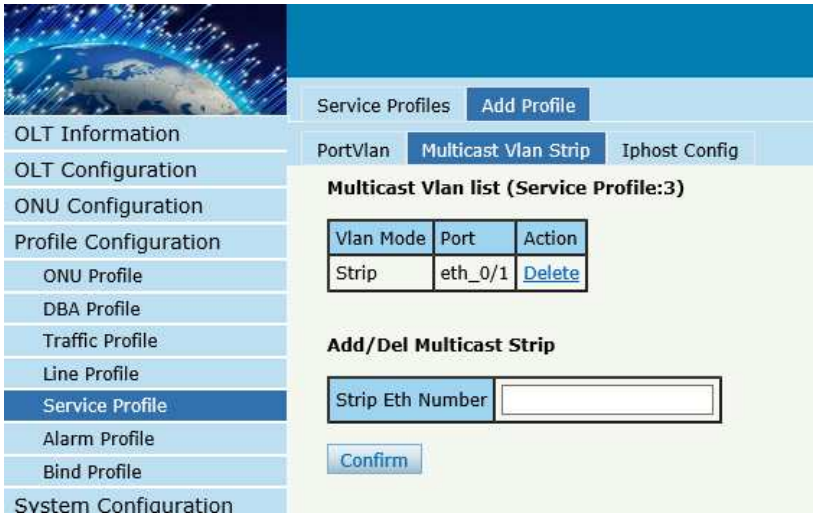


Figure 5.5-5: Port Multicast VLAN Mode

5.5.2.3 Iphost Config

Add Iphost for ONU wan connection. IPhost is used for ONU management.

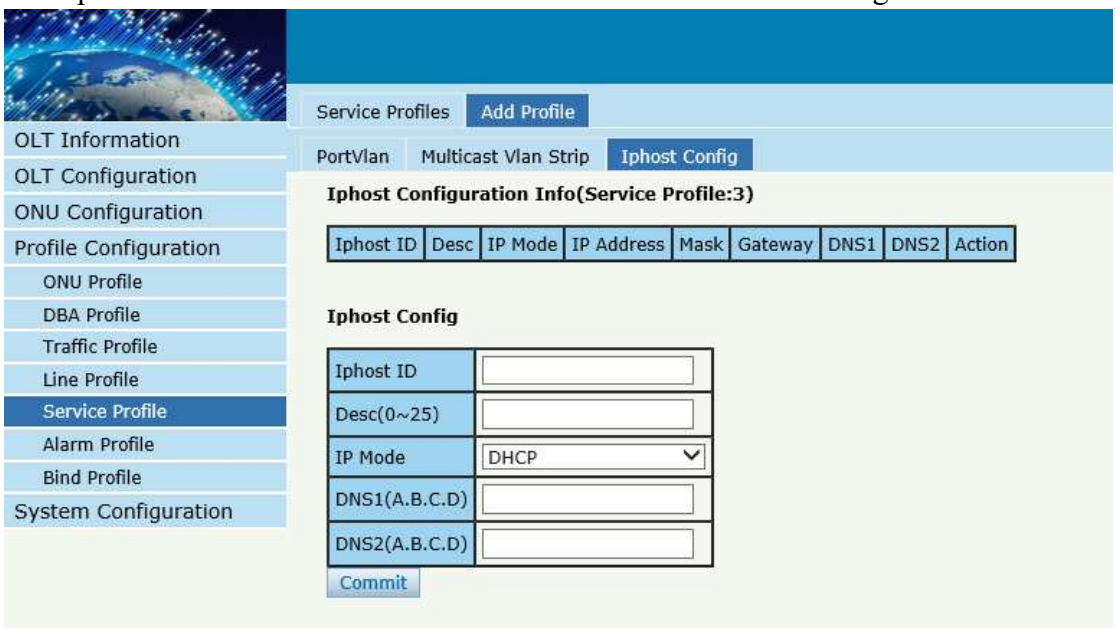


Figure 5.5-6: Add IPhost

5.6 Alarm Profile

Alarm profile is used to configure the parameters of ONU alarm.

5.6.1 Profile Info

Profile Configuration→Alarm Profile →profile info

The table displays alarm profile list.

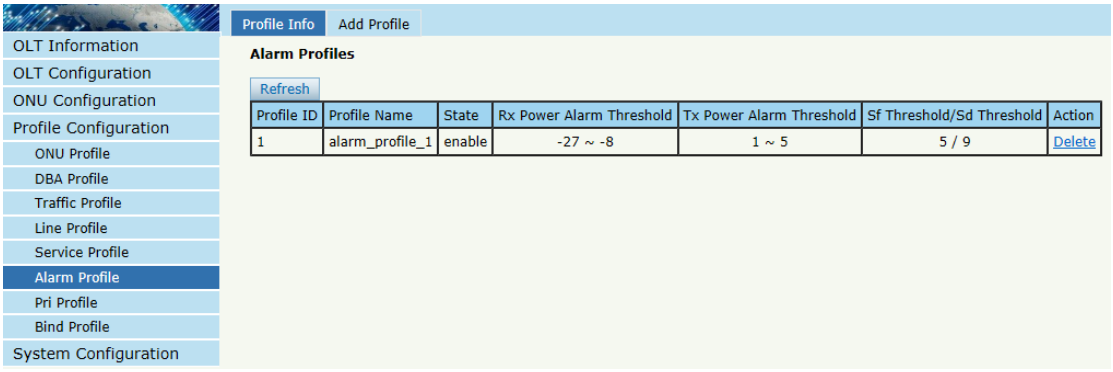


Figure 5.6-1: Alarm Profile List

5.6.2 Add Profile

Profile Configuration→Alarm Profile →Add profile

Add new alarm profile, set the threshold of alarm generation.

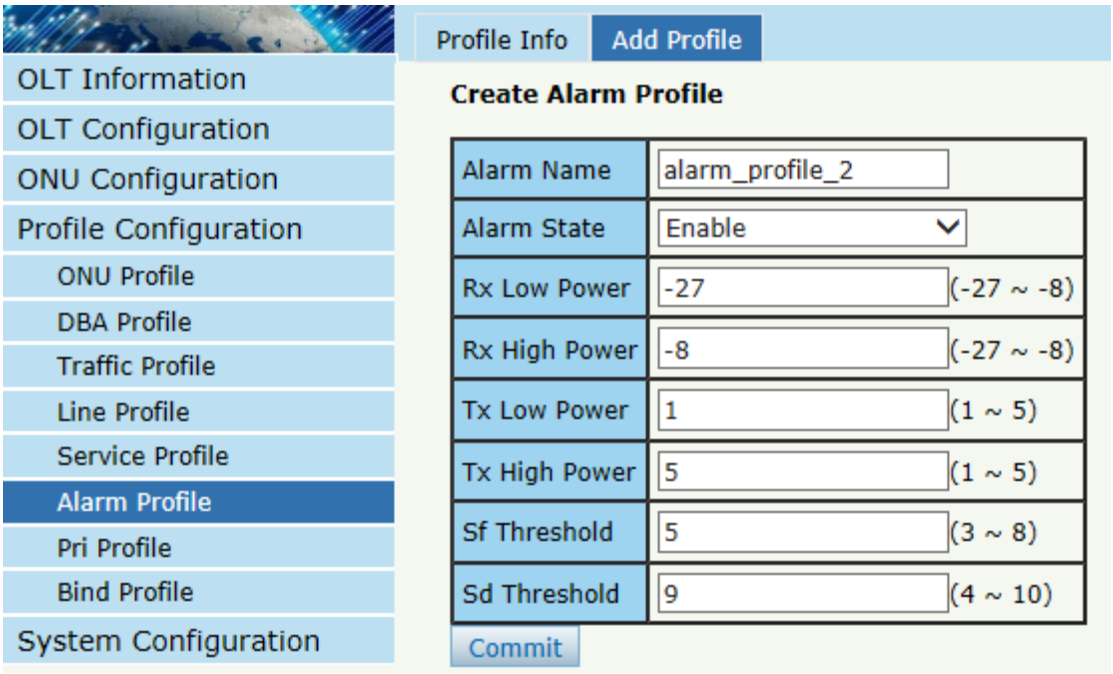


Figure 5.6-2: Add Alarm Profile

5.7 Pri Profile

Pri Profile is the profile which the parameters are configured by private OMCI, including WAN, SIP, WIFI, CATV, DHCP Server, and so on.

5.7.1 Pri Profile

Profile Configuration→Pri Profile

The table displays private profile list. You can also do some operations, such as delete and modify.

Figure 5.7-1: Pri Profile

5.7.2 Add Profile

Profile Configuration→Pri Profile →Add profile

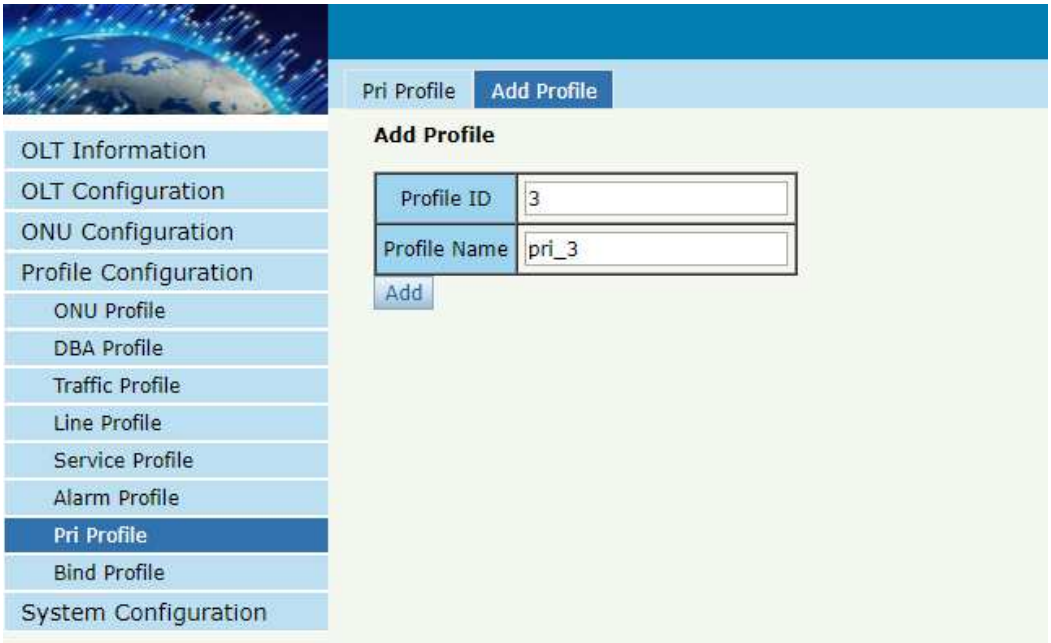


Figure 5.7-2: Add Private Profile

5.8 IGMP Profile

5.8.1 IGMP Profile

Profile Configuration→IGMP Profile →IGMP Profile

You can view the list of currently created IGMP profiles in this interface.

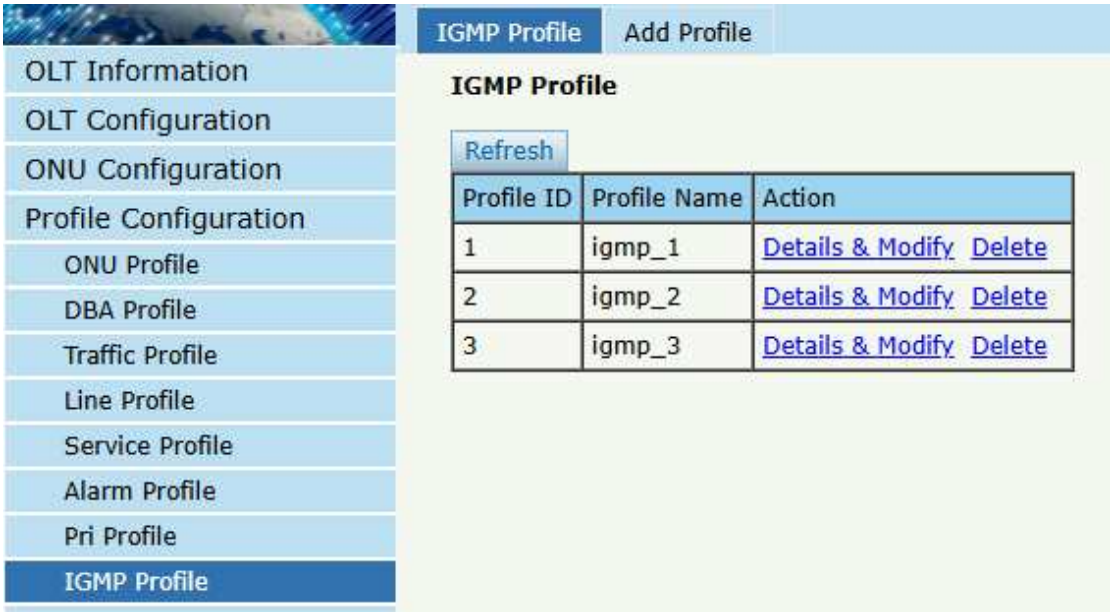


Figure 5.8-1: IGMP Profile List

Click "Detail & Modify" to configure the IGMP parameters in detail. Along with the ONU binding profile, these parameters will be sent to the ONU.

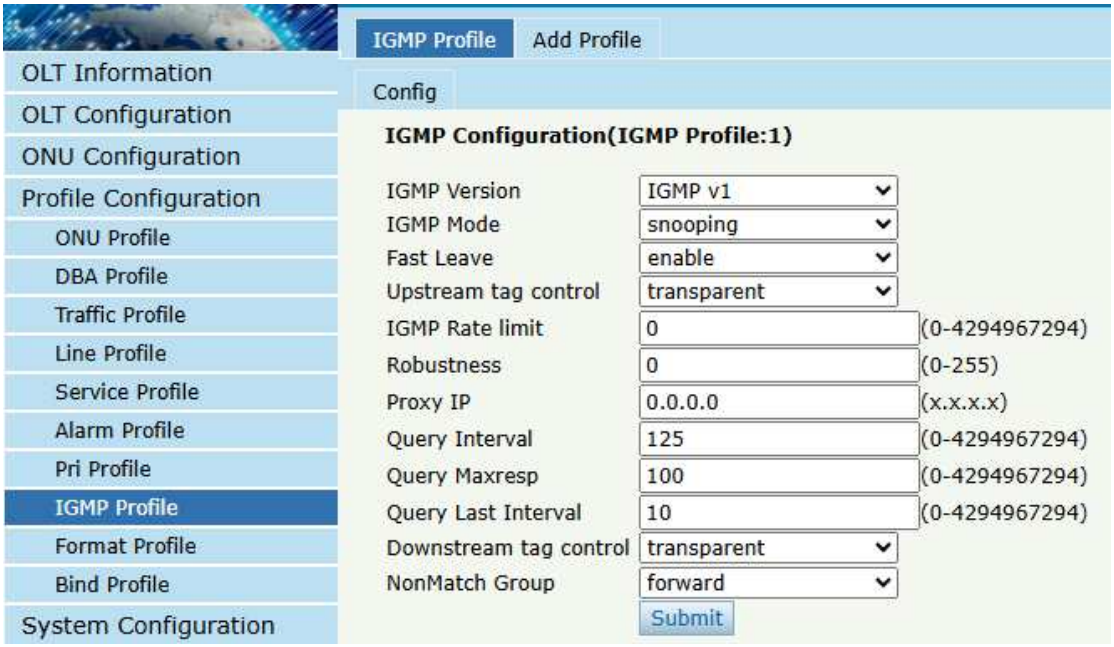


Figure 5.8-2: IGMP Profile Configuration

5.8.2 Add Profile

Profile Configuration→IGMP Profile →Add Profile

This interface is used to create new IGMP profiles.

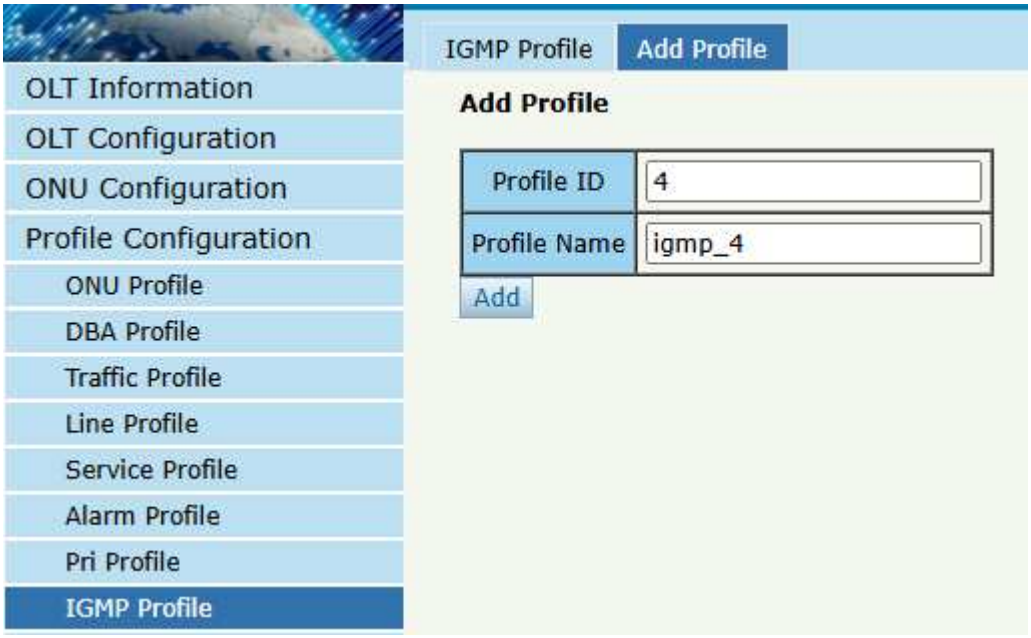


Figure 5.8-3: Add IGMP Profile

5.9 Format Profile

5.9.1 Format Profile

Profile Configuration→IGMP Profile →Format Profile

You can view the list of currently created Format profiles in this interface.

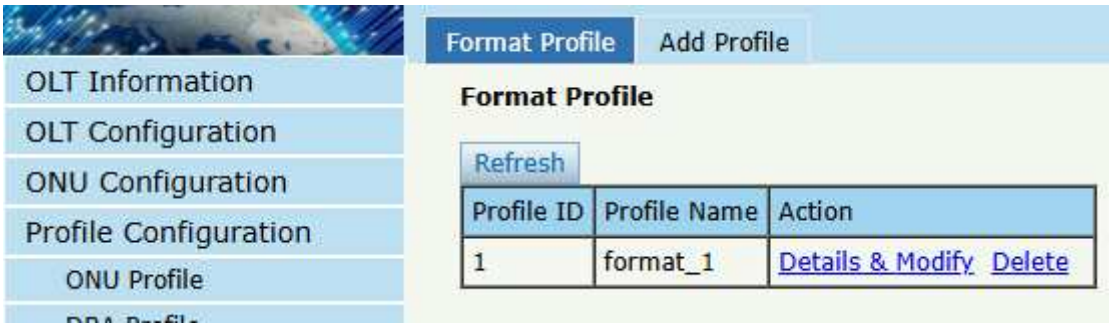


Figure 5.9-1: Format Profile List

Click "Detail & Modify" to configure the Format parameters in detail. It contains the switches of DHCP Option 82, DHCPv6 Option 18, Option 37 and PPPoE+. You can also configure the formats and carried parameters of Circuit ID and Remote ID, which are mainly used for DHCP Relay or DHCP Snooping.

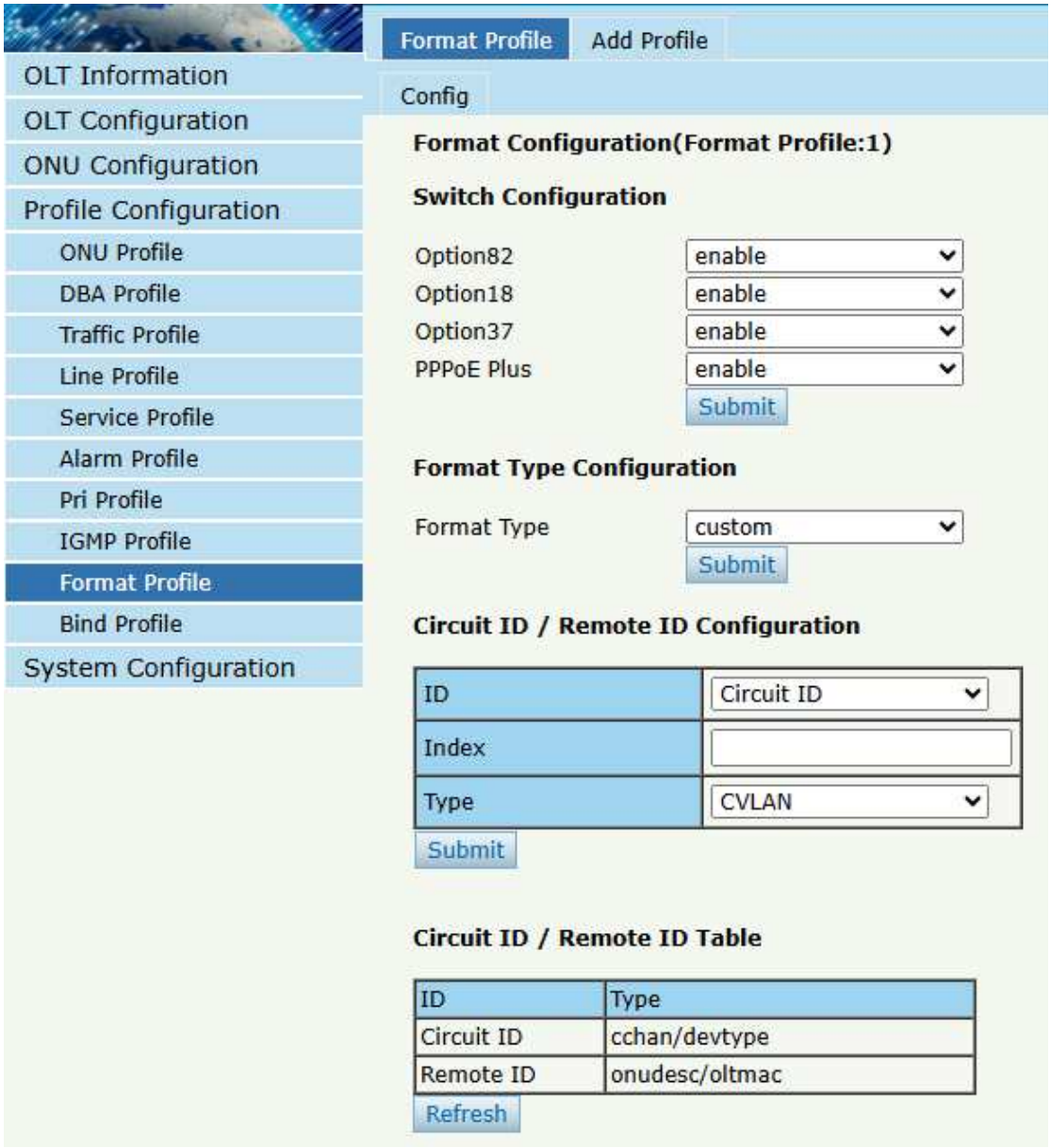


Figure 5.9-2: Format Profile Configure

5.9.2 Add Profile

Profile Configuration→IGMP Profile →Add Profile

This interface is used to create new Format profiles.

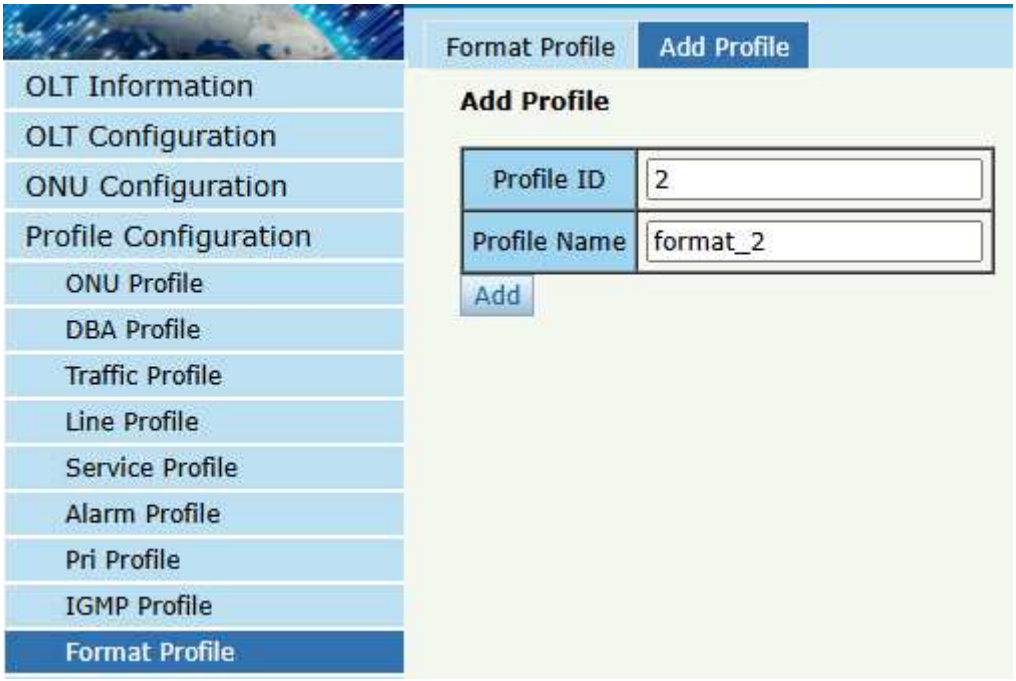


Figure 5.9-3: Add Format Profile

5.10 Bind Profile

After profile is configured, it is necessary to bind it to ONU.

Profile Configuration→Bind Profile

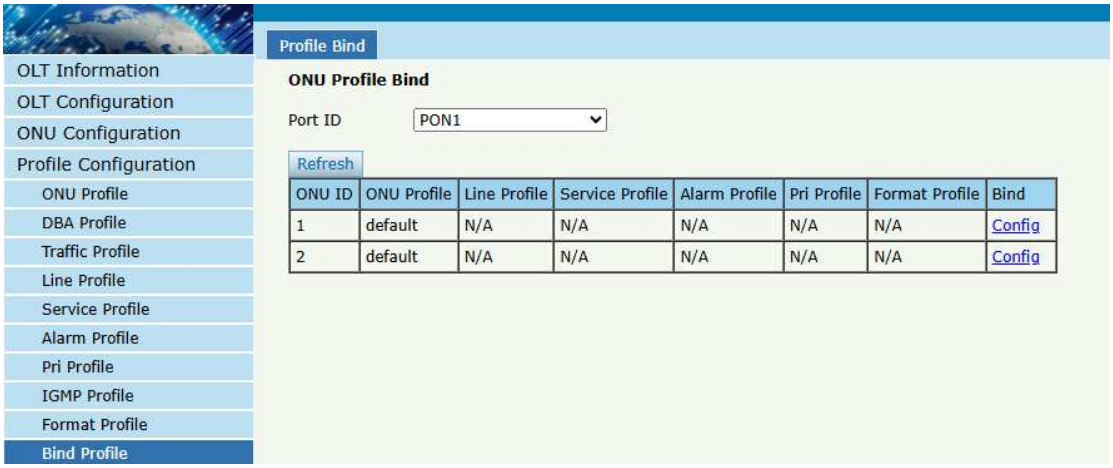


Figure 5.10-1: Bind profile

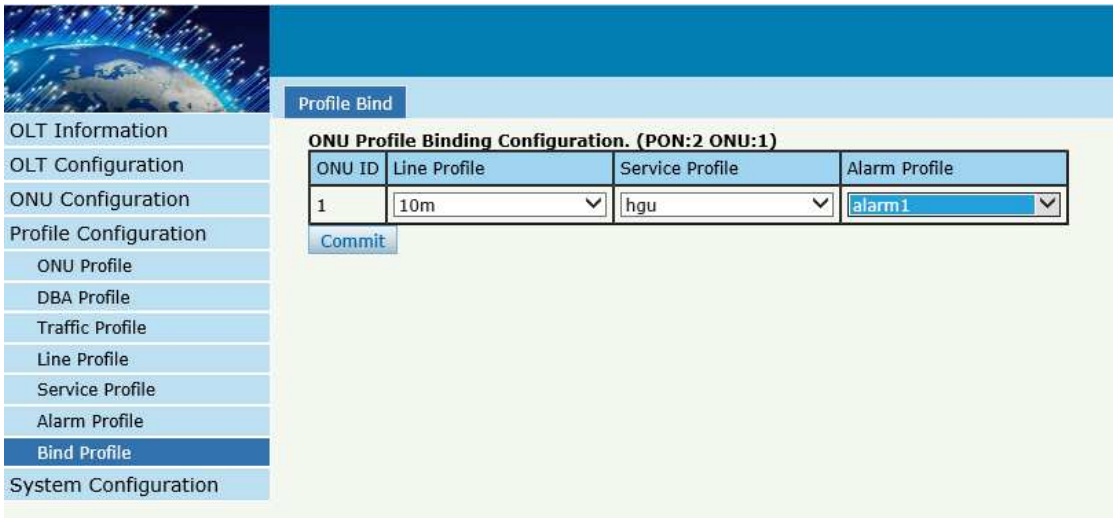


Figure 5.10-2: Select Profile

Chapter 6 System Configuration

This chapter is about the global management of OLT.

6.1 System Log

6.1.1 System Log

System Configuration→System Log
This page displays OLT system alarms and events.

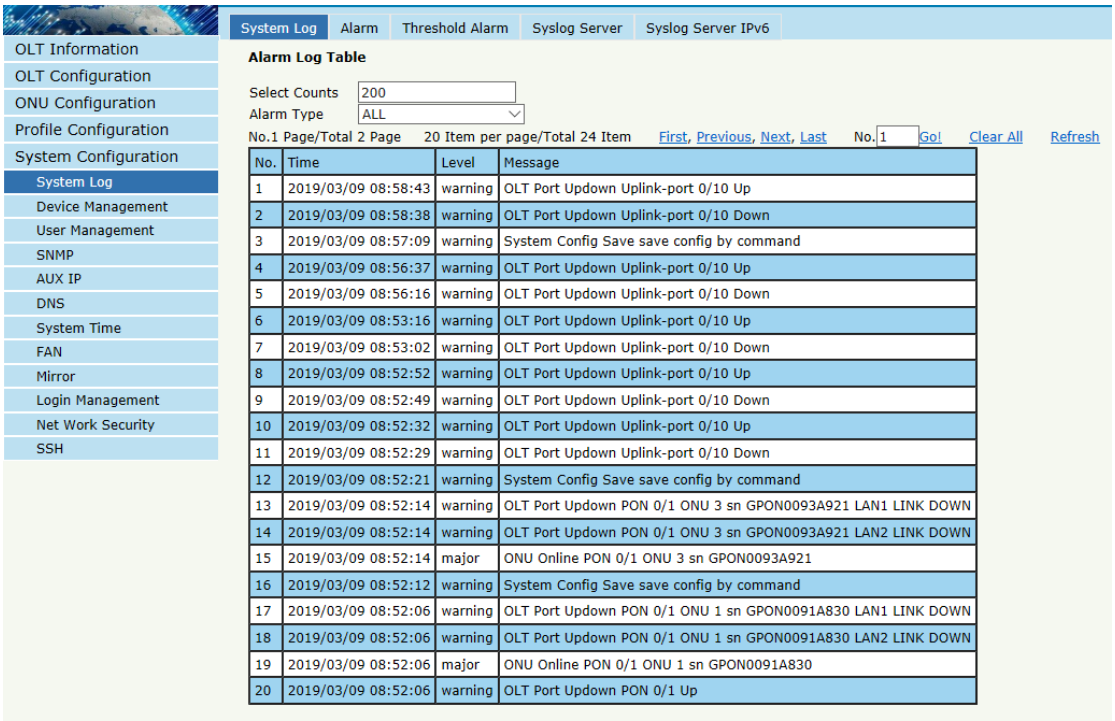


Figure 6.1-1: System Log

6.1.2 Alarm

System Configuration →System Log →Alarm
It contains all the alarms of OLT. User can choose the different alarms to "**Print**", "**Record**", "**Trap**" and "**Remote**".

Figure 6.1-2: Alarm

Options	Illustration
Print	Alarm and event show in console and telnet, but not show in syslog, EMS and remote log server.
Record	Alarm and event show in syslog, but not show in console, telnet, EMS and remote log server.
Trap	Alarm and event show in EMS, but not show in console, telnet, syslog and remote log server.
Remote	Alarm and event show in remote log server, but not show in console, telnet, syslog and EMS.

Table 6.1-1 Different Alarms

6.1.3 Threshold Alarm

System Configuration →System Log →Threshold Alarm

This page is used to configure OLT temperature threshold, CPU-usage threshold and memory- usage threshold, PON optical threshold.

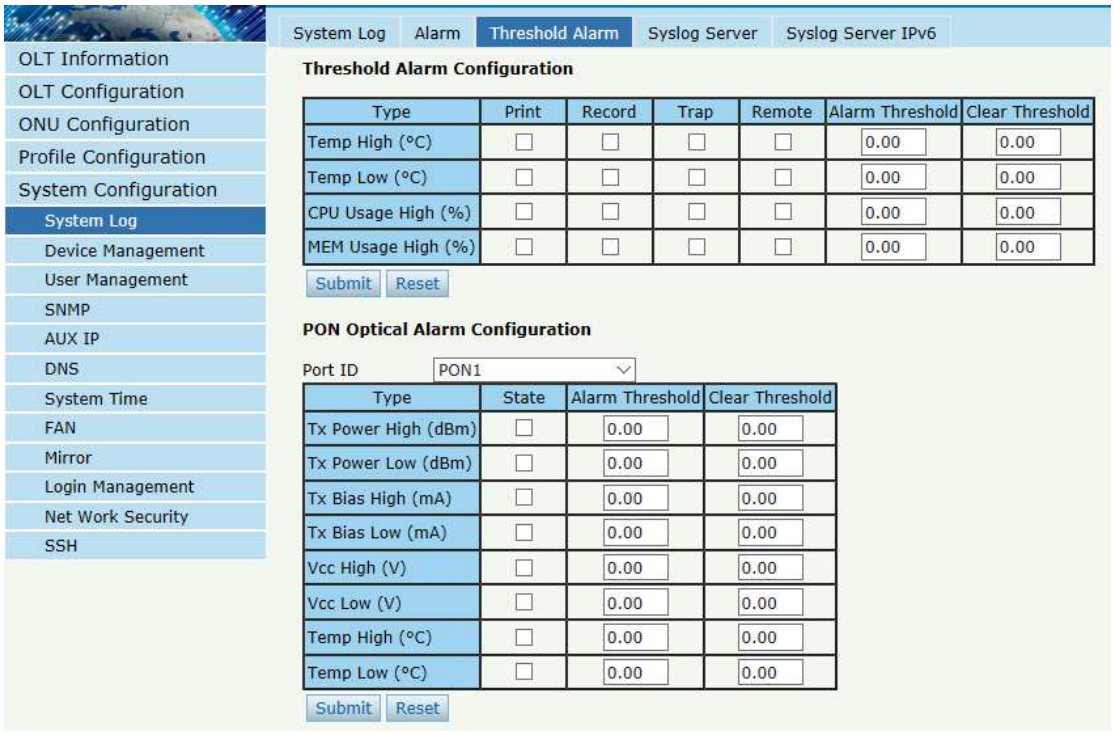


Figure 6.1-3: Threshold Alarm

6.1.4 Syslog Server

System Configuration→System Log →Syslog Server

This page is used to configure remote IPv4 server of OLT system log.

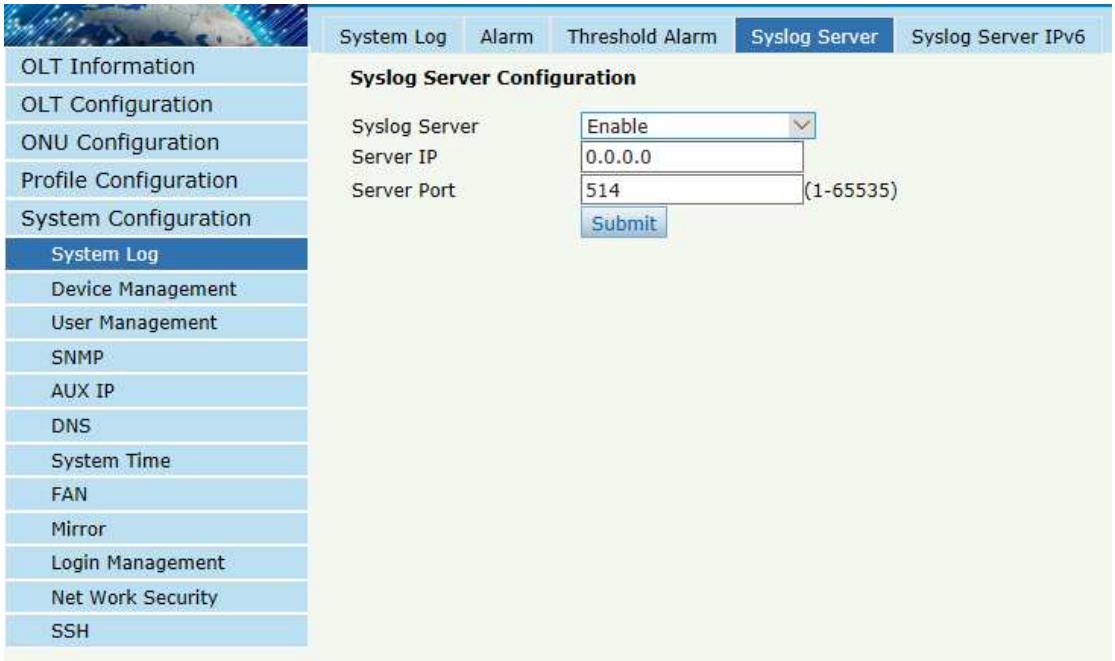


Figure 6.1-4: Syslog Server

6.1.5 Syslog Server IPv6

System Configuration→System Log →Syslog Server IPv6

This page is used to configure remote IPv6 server of OLT system log.

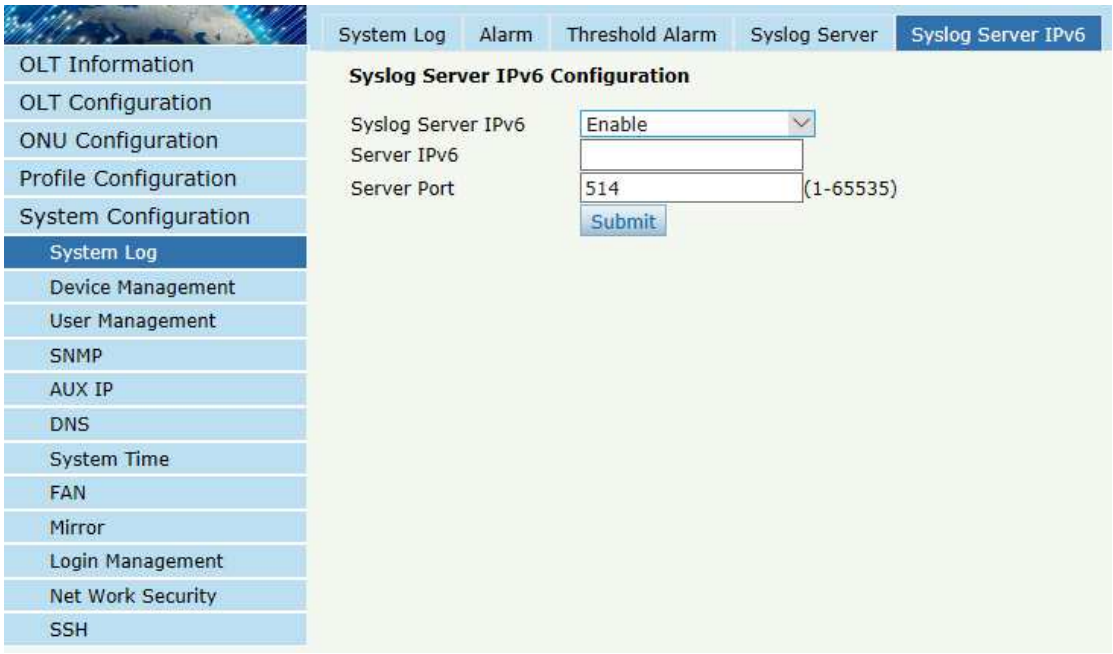


Figure 6.1-5: Syslog Server IPv6

6.2 Device Management

6.2.1 Firmware Upgrade

System Configuration→Device Management →Firmware Upgrade

You can upgrade the OLT firmware on this page. OLT will reboot automatically with the new firmware after upgraded.

Figure 6.2-1: Firmware Upgrade

6.2.2 Device Reboot

System Configuration→Device Management →Device Reboot

You can reboot the entire system on this page. Please do save the configuration before reboot.

Figure 6.2-2: Device Reboot

6.2.3 Config File

System Configuration→Device Management →Config File

You can backup configuration, restore configuration, restore factory defaults and save configuration on this page.

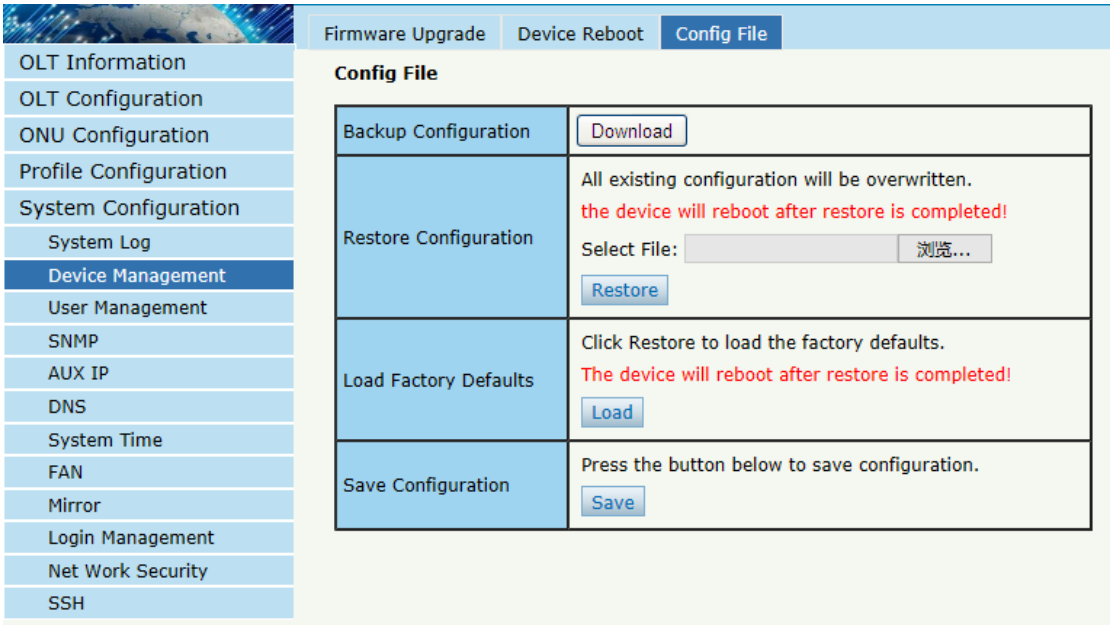


Figure 6.2-3: File Configuration

6.2.4 Advance Config File

System Configuration→Device Management →Advance Config File

The OLT supports the configuration of auto-save and backup functions, allowing users to schedule automatic configuration saving and backup tasks at specified times.

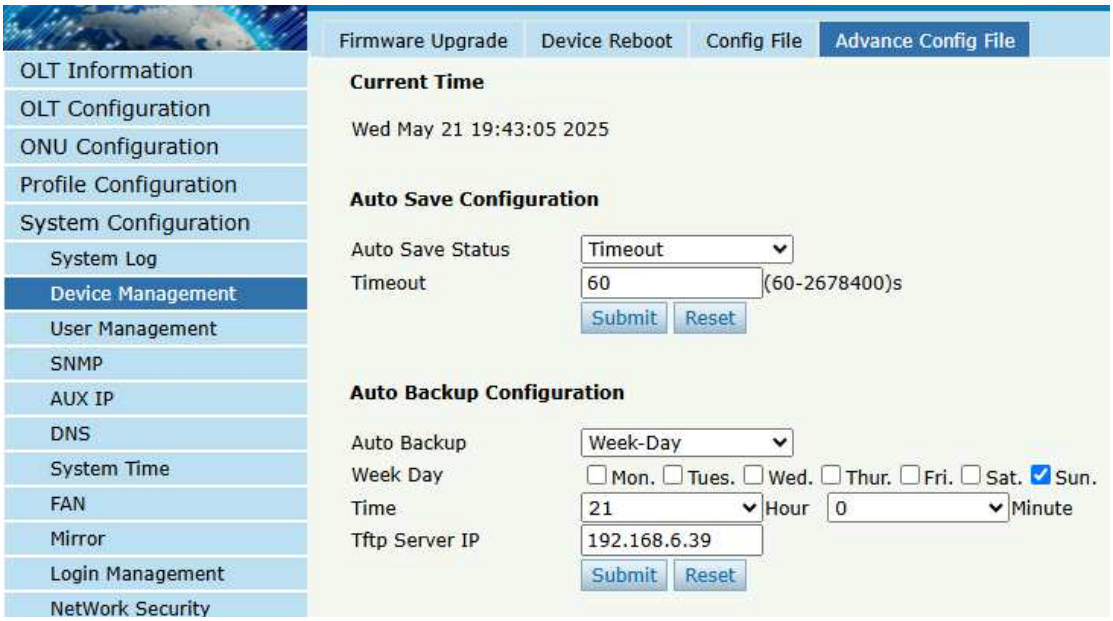


Figure 6.2-4: Advance Config File

6.3 User Management

6.3.1 User Manage

System Configuration→User management→User Manage

Two types of user have been defined, Normal and Admin. There are limitations to normal user, and Admin user has no limits to full function of OLT. The default account member is **Admin** level.

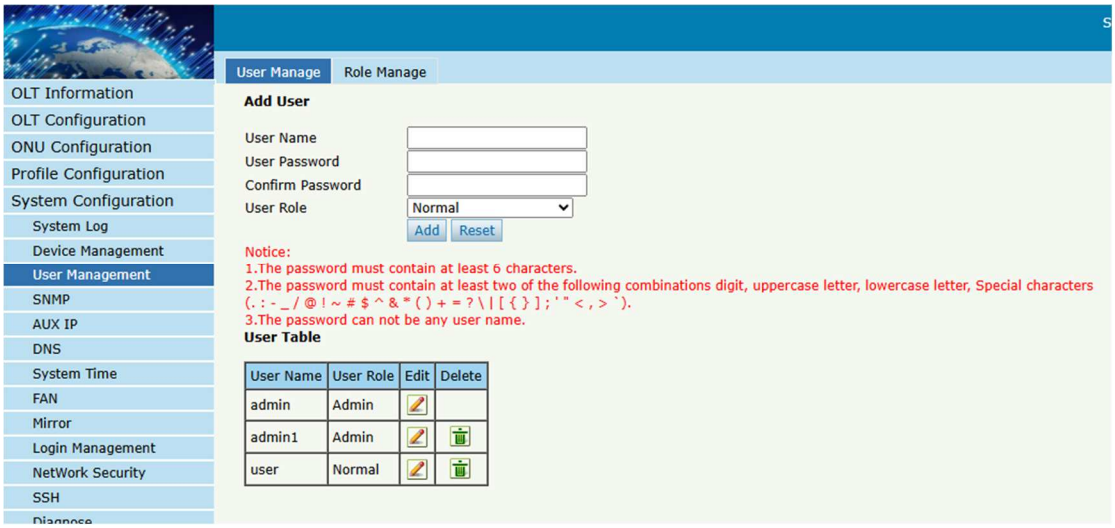


Figure6.3-1: User Manage

6.3.2 Role Manage

System Configuration→User management→Role manage

You can add roles and assign different permissions to different roles.

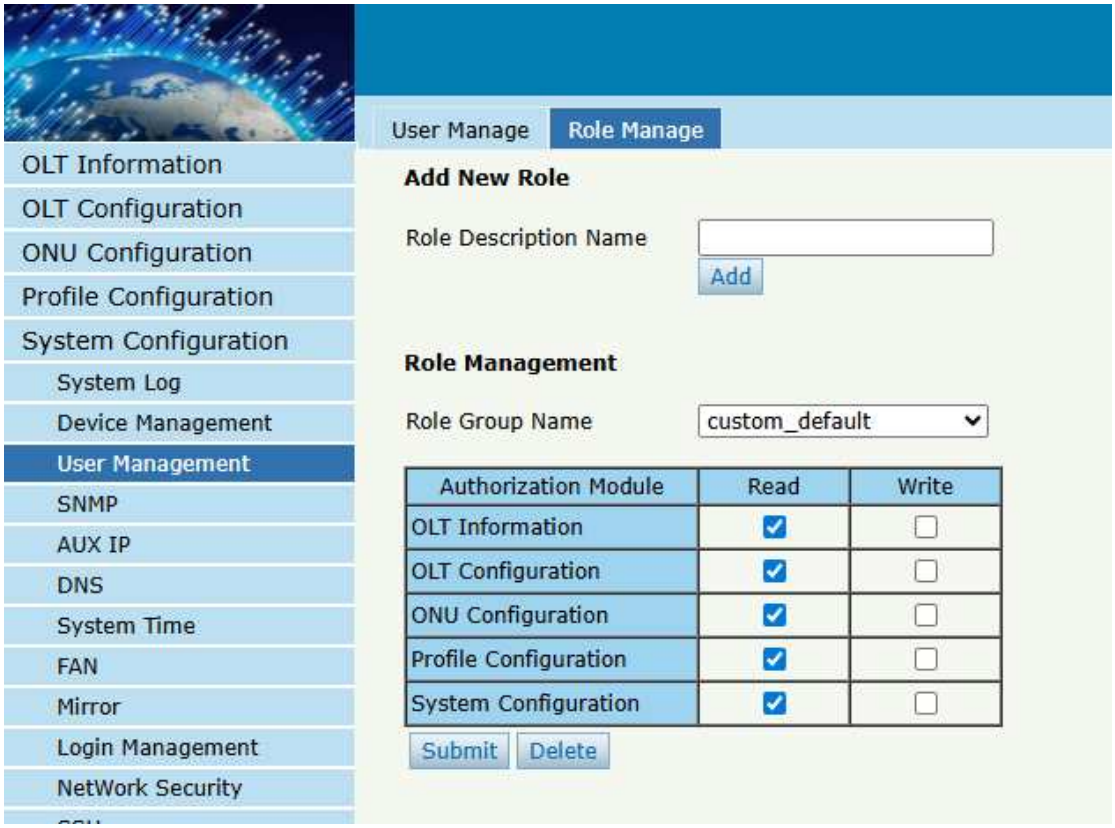


Figure6.3-2: Role Manage

6.4 SNMP

6.4.1 SNMP V1/V2

System Configuration → SNMP →SNMP V1/V2

This page is used to configure SNMP parameters of version 1 and version 2 for OLT management.

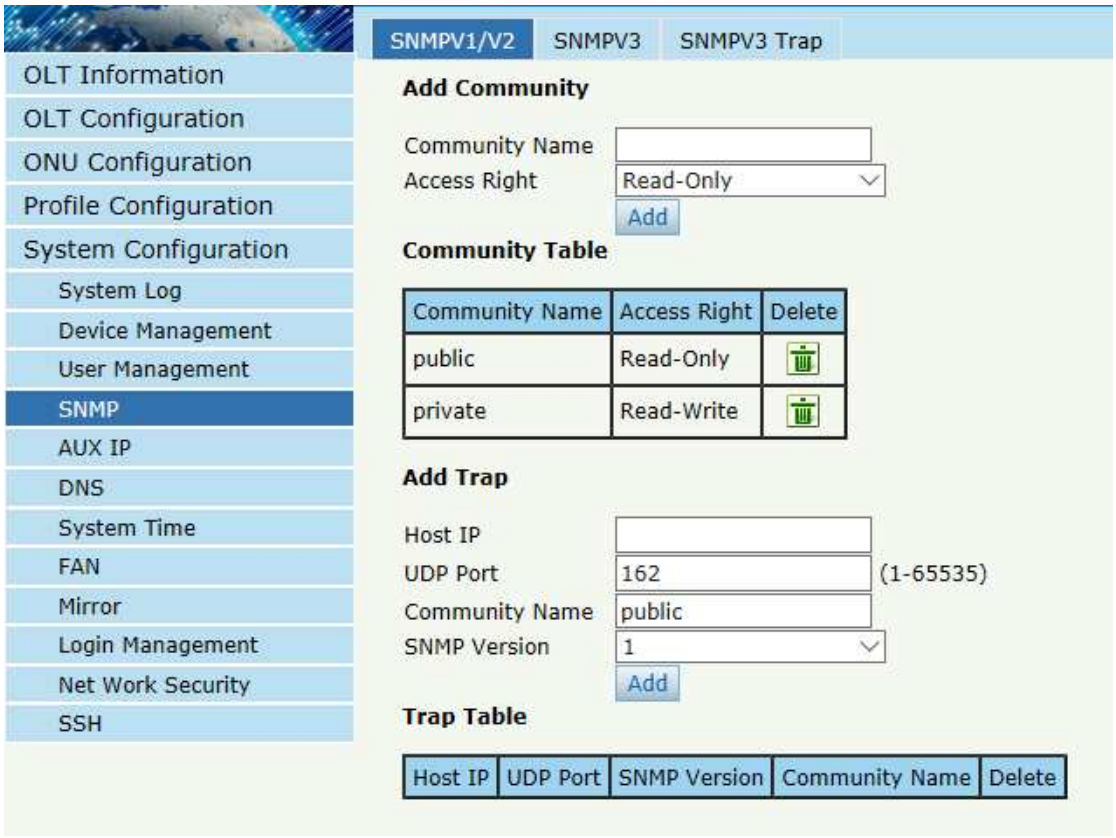


Figure6.4-1: SNMP V1/V2

6.4.2 SNMP V3

System Configuration → SNMP →SNMP V3

This page is used to configure SNMP parameters of version 3 for OLT management.

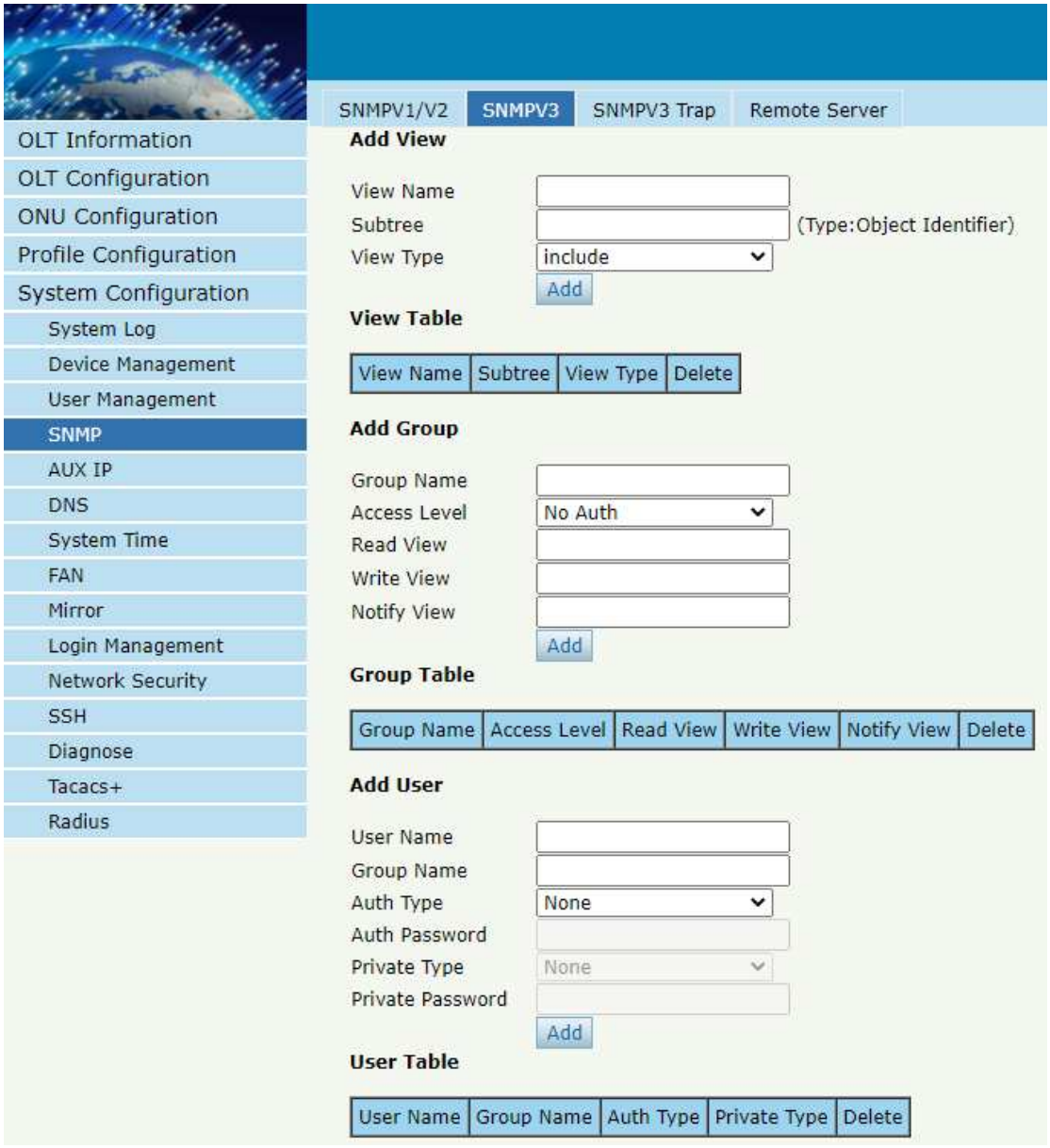


Figure6.4-2: SNMP V3

6.4.3 SMNP V3 Trap

System Configuration → SNMP →SNMP V3 Trap
Configure the target host IP address of trap messages.

Figure 6.4-3: SNMP V3 Trap

6.4.4 Remote Server

System Configuration → SNMP →Remote Server

Configure the IP address of your SNMP network management server.

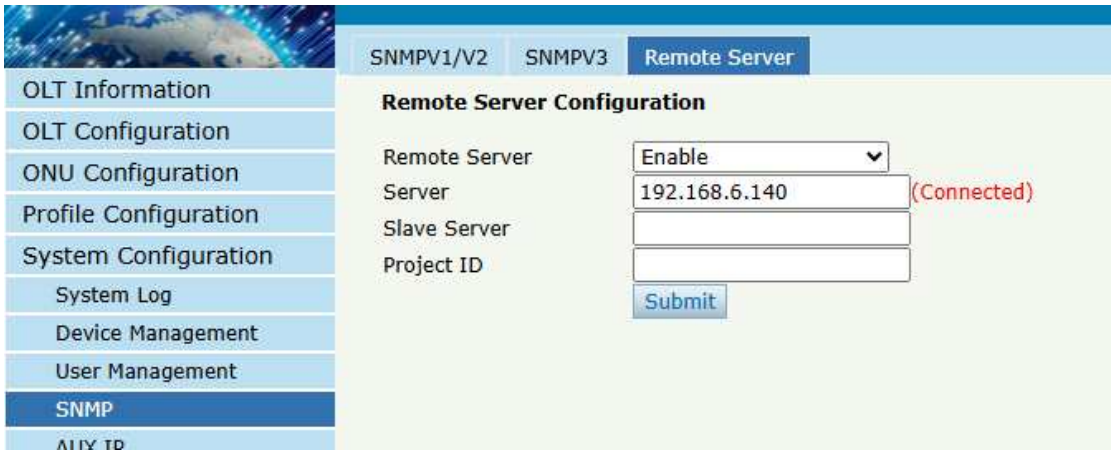


Figure 6.4-4: Remote Server

6.5 AUX IP

6.5.1 AUX IP

System Configuration → AUX IP→ AUX IP

AUX port is out band management port. The IPv4 address of aux port is out band management IP. Default IPv4 address is 192.168.8.200.

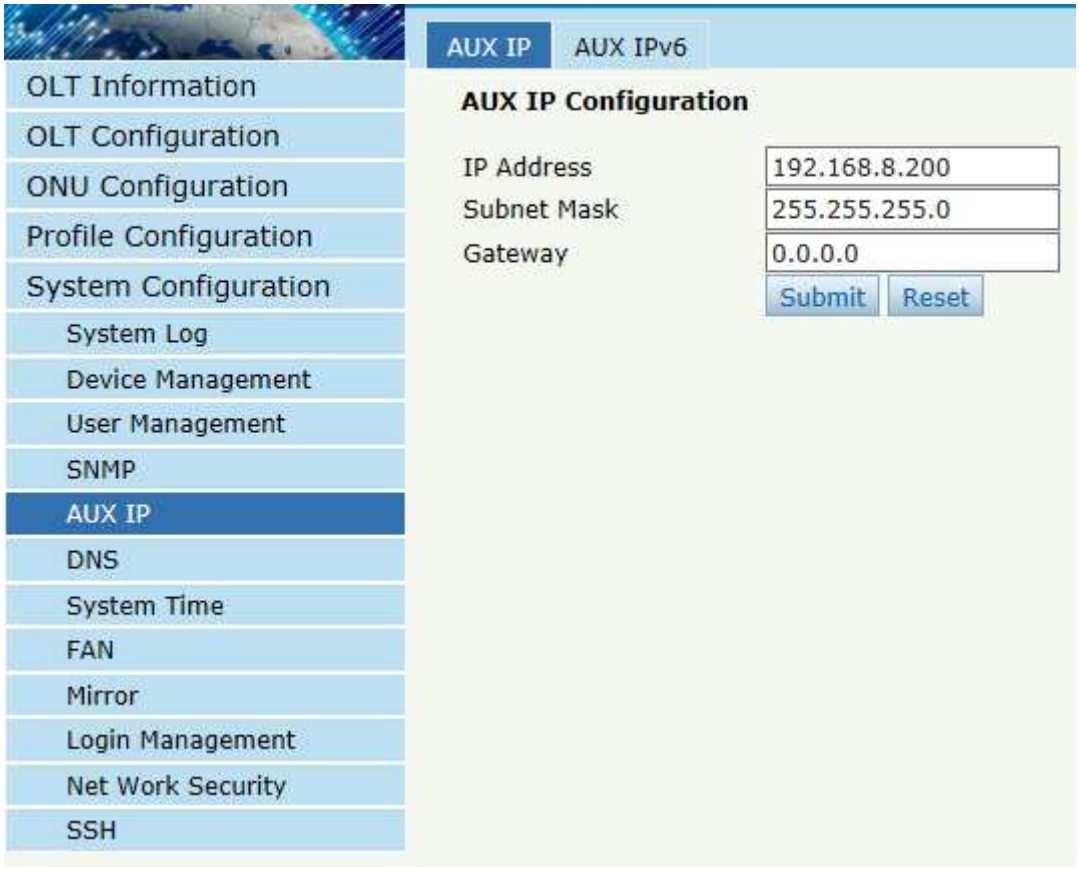


Figure 6.5-1: AUX IP

6.5.2 AUX IPv6

System Configuration → AUX IP → AUX IPv6

AUX port is out band management port. The IPv6 address of aux port is out band management IP. By default, there is a link local address.

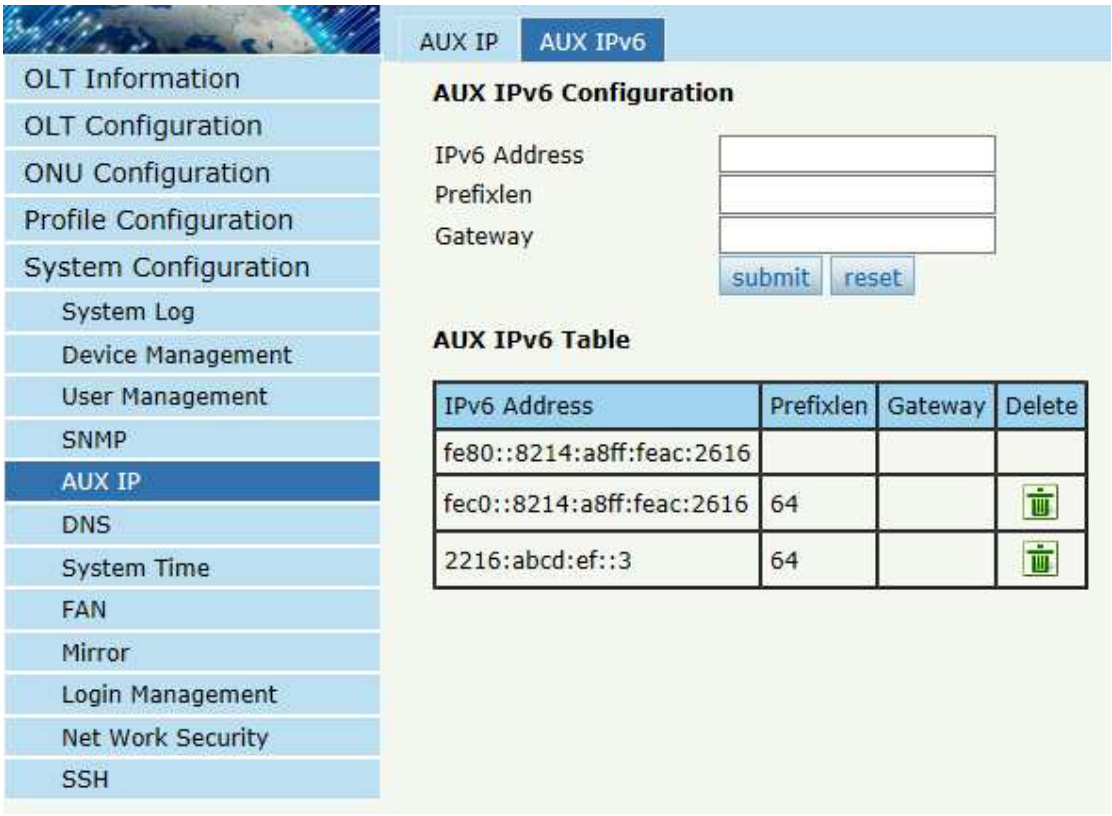


Figure 6.5-2: AUX IPv6

6. 6 DNS

DNS is used for domain name resolution. When OLT need to visit a site or a destination by domain, DNS is required, such as NTP server.

6.6.1 IPv4 DNS

System Configuration → DNS → IPv4 DNS
This page is used to configure IPv4 DNS.

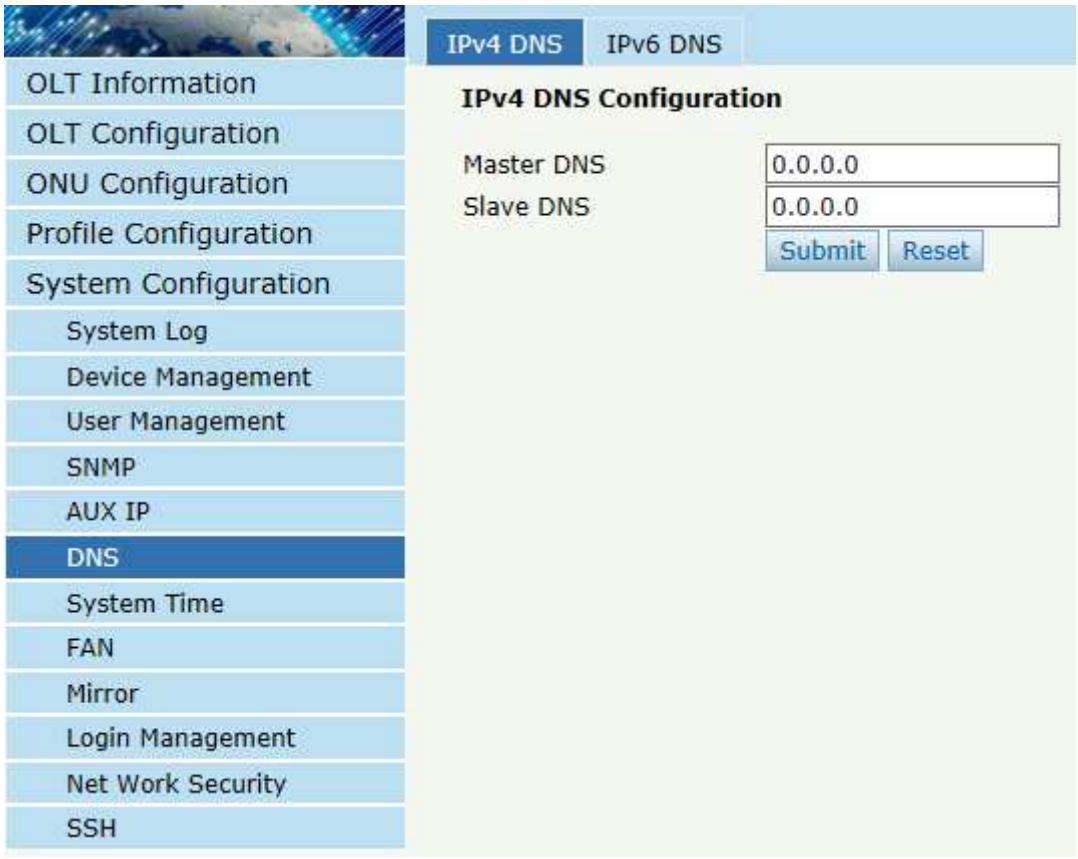


Figure 6.6-1: IPv4 DNS

6.6.2 IPv6 DNS

System Configuration → DNS → IPv6 DNS
This page is used to configure IPv6 DNS.

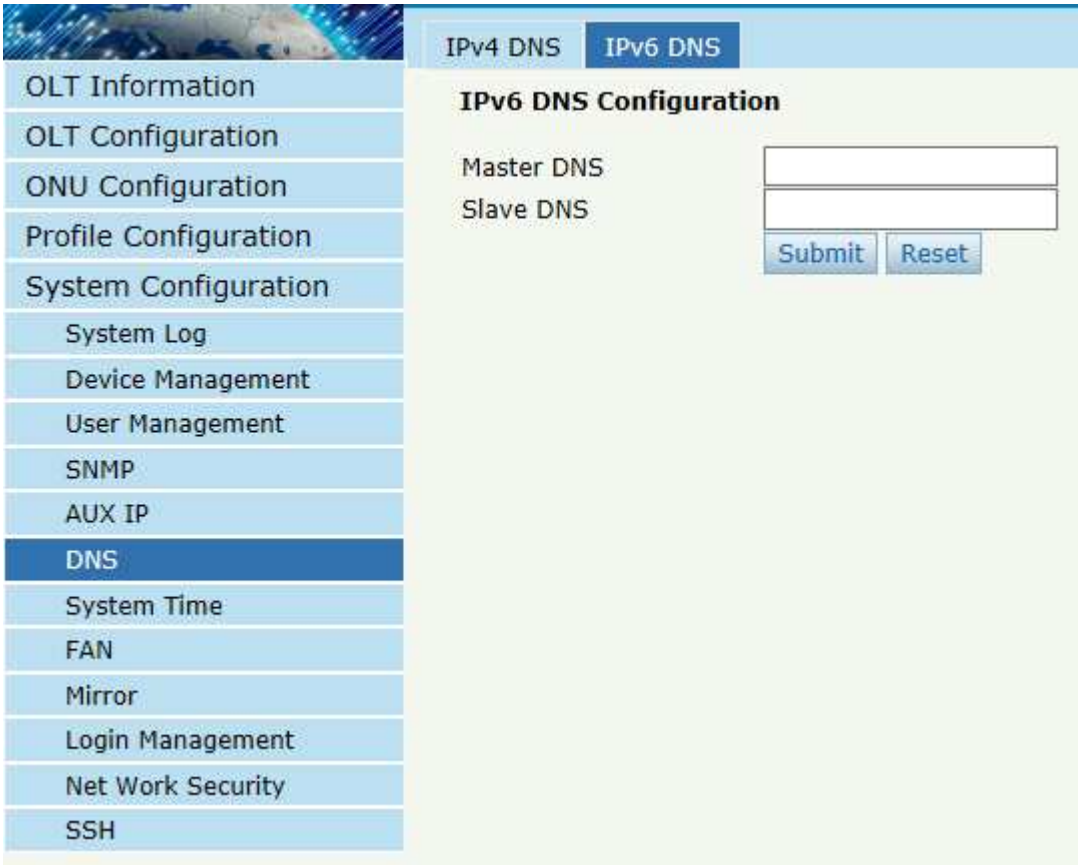


Figure 6.6-2: IPv6 DNS

6.7 System Time

6.7.1 RTC

System Configuration → System Time→RTC

This page is used to set OLT system time. RTC stands for Real-Time Clock, it provides clock signal to the system. There is no battery inside OLT, so the time will not be saved after powered off.

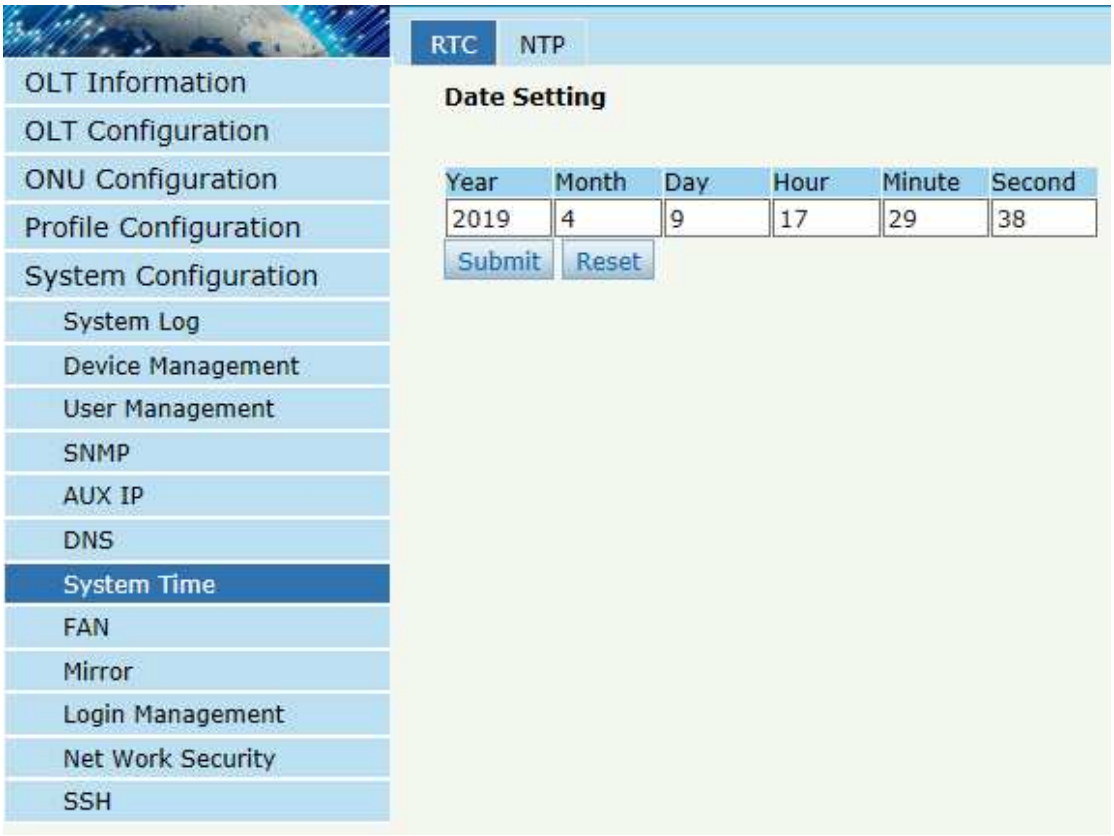


Figure 6.7-1: RTC Setting

6.7.2 NTP

System Configuration → System Time→NTP

This page is used to configure NTP server. OLT will synchronize time with the NTP server at a given time.

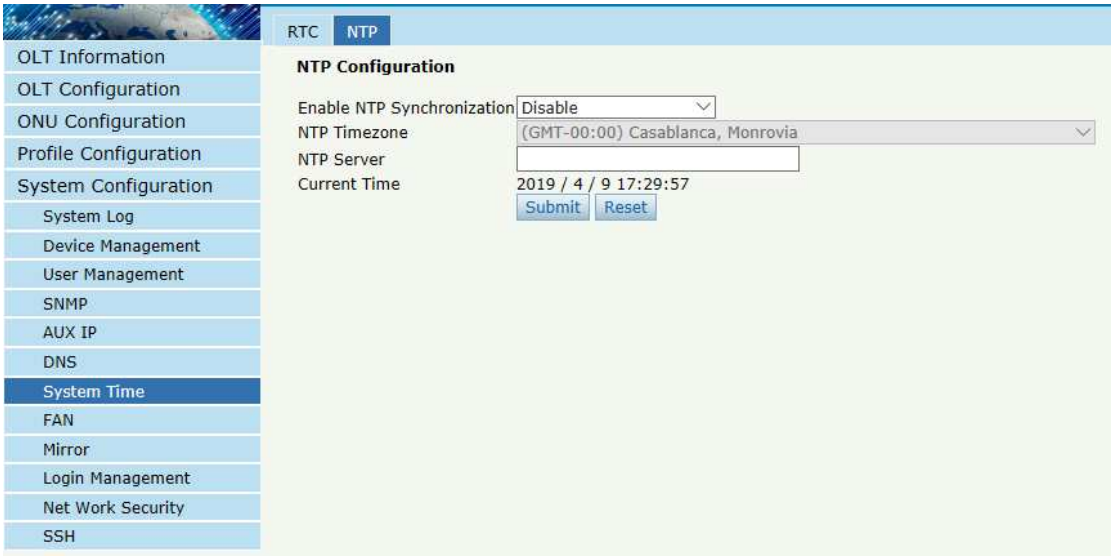


Figure 6.7-2: NTP Configuration

6.8 FAN

System Configuration → FAN

The fans can be turned on and turned off manually; and also can be turned on and off automatically according to the temperature of OLT main chip.

This configuration will not be saved after reboot.

Figure 6.8-1: FAN Configuration

6.9 Mirror

System Configuration → Mirror

Port mirror is usually used for troubleshooting. Each monitor session can be set with one destination port and up to 8 source ports.

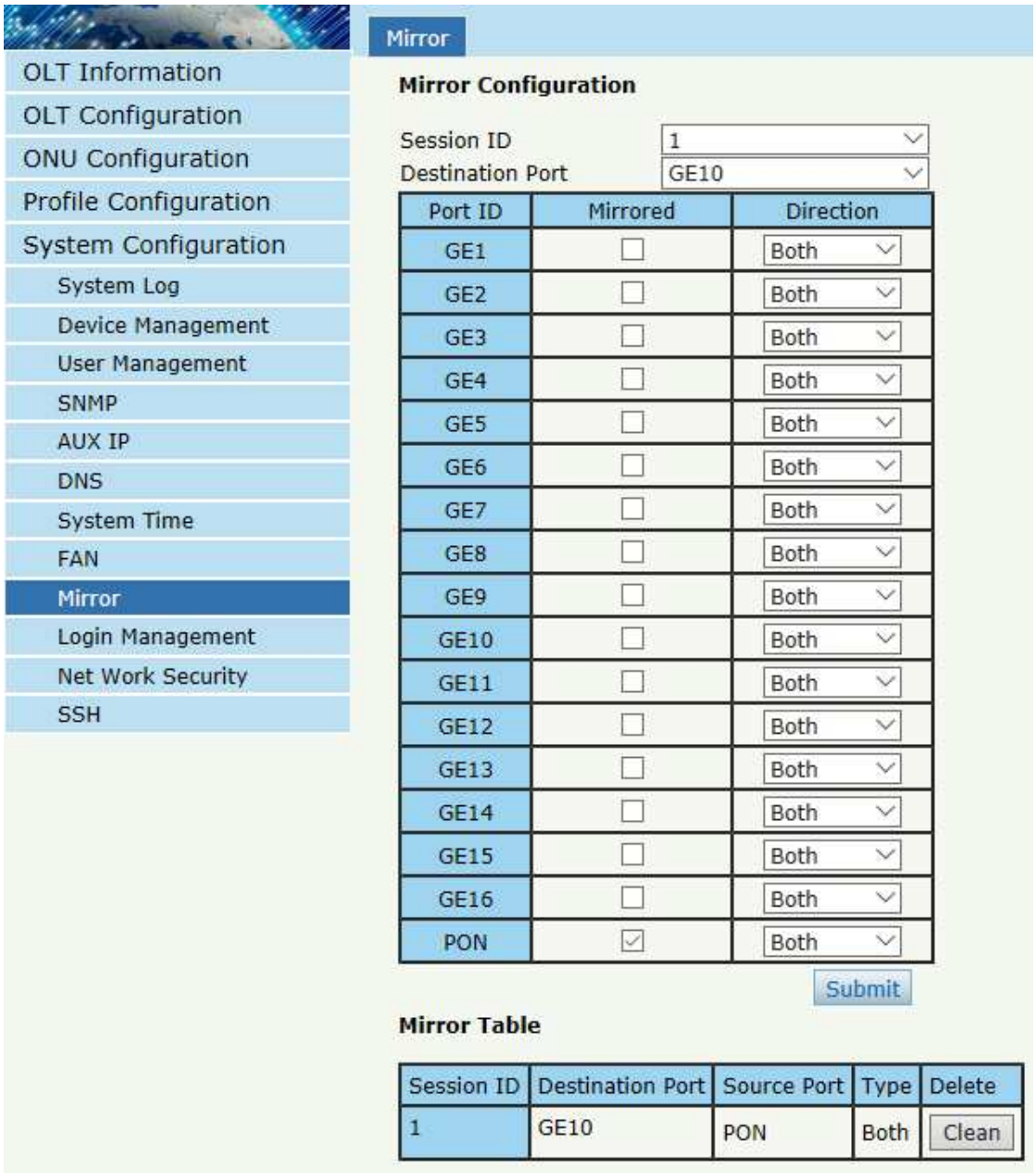


Figure 6.9-1: Mirror Configuration

6.10 Login Management

6.10.1 Login Access List

System Configuration → Login Management→ Login Access List

This page is used to configure access rights for management. You can configure access rights for telnet, web, SNMP, SSH according to source IP address.

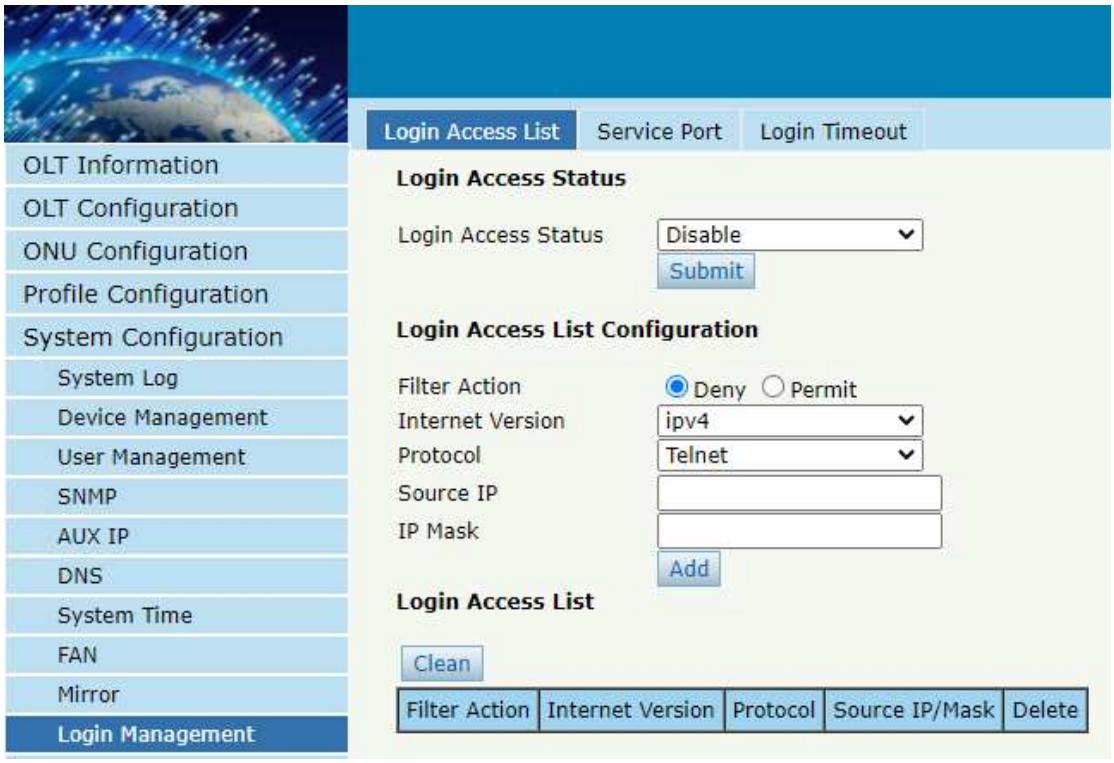


Figure 6.10-1: Login Access List Configuration

6.10.2 Service Port

System Configuration → Login Management→ Service Port

This user interface allows you to modify the default remote service port.

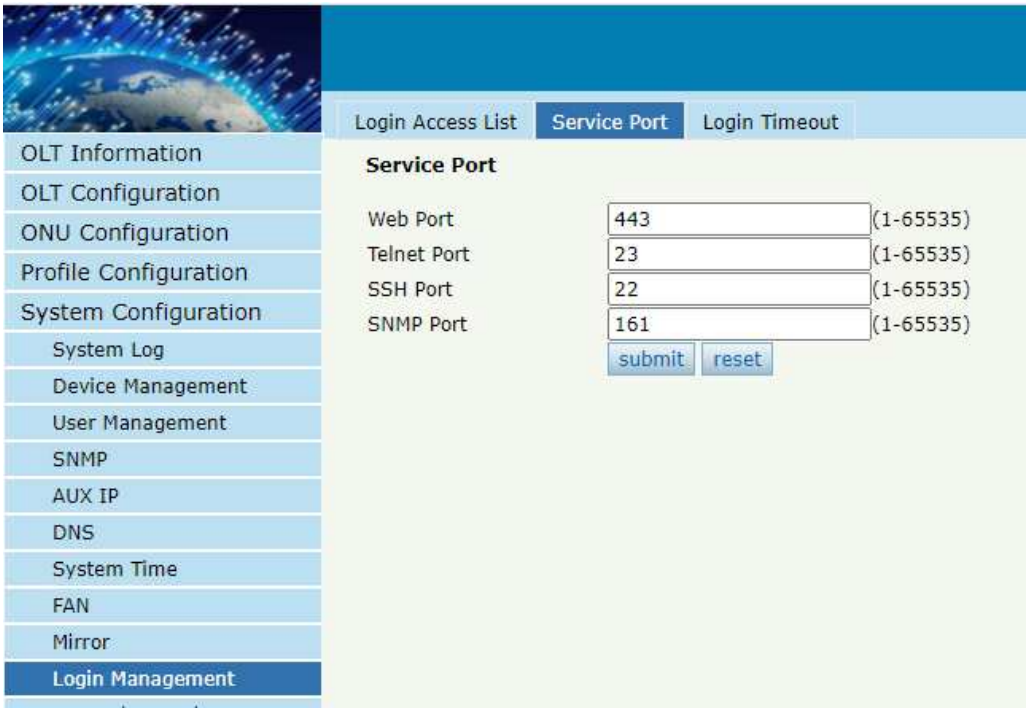


Figure 6.10-2: Service Port Configuration

6.10.3 Login Configuration

System Configuration → Login Management→ Login Configuration

This page is used to set web timeout.

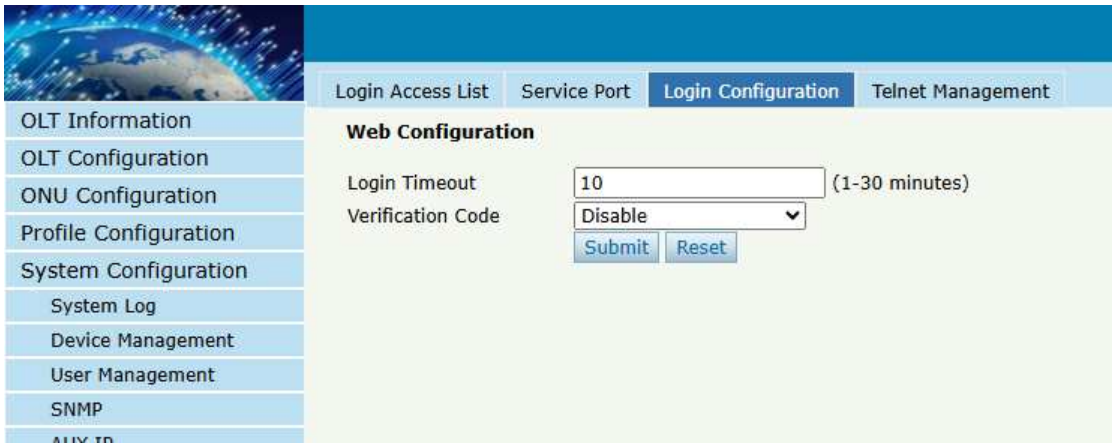


Figure 6.10-3: Login Timeout Configuration

6.10.4 Telnet Management

System Configuration → Login Management→Telnet Management

This interface displays the current session accessing the OLT via telnet. You can choose to terminate a certain session.

Figure 6.10-4: Telnet Management

6.11 Net Work Security

System Configuration → Net Work Security
This page is used to set up OLT' network security level.

Figure 6.11-1: Net Work Security Setting

6.12 SSH

SSH (Secure Shell) is a reliable protocol that provides security for remote login sessions and other network services. The SSH protocol can effectively prevent information leakage during remote management.

6.12.1 SSH Server State

System Configuration → SSH→ SSH Server State
This page displays current connections that have established by SSH protocol.

Figure 6.12-1: SSH Server State

6.12.2 SSH Enable

System Configuration → SSH→ SSH Enable

This page is used to configure SSH protocol related parameters.

Figure 6.12-2: SSH Global Configuration

6.13 Diagnose

6.13.1 Ping Diagnose

System Configuration → Diagnose→ Ping Diagnose
This interface is used to diagnose network connectivity.

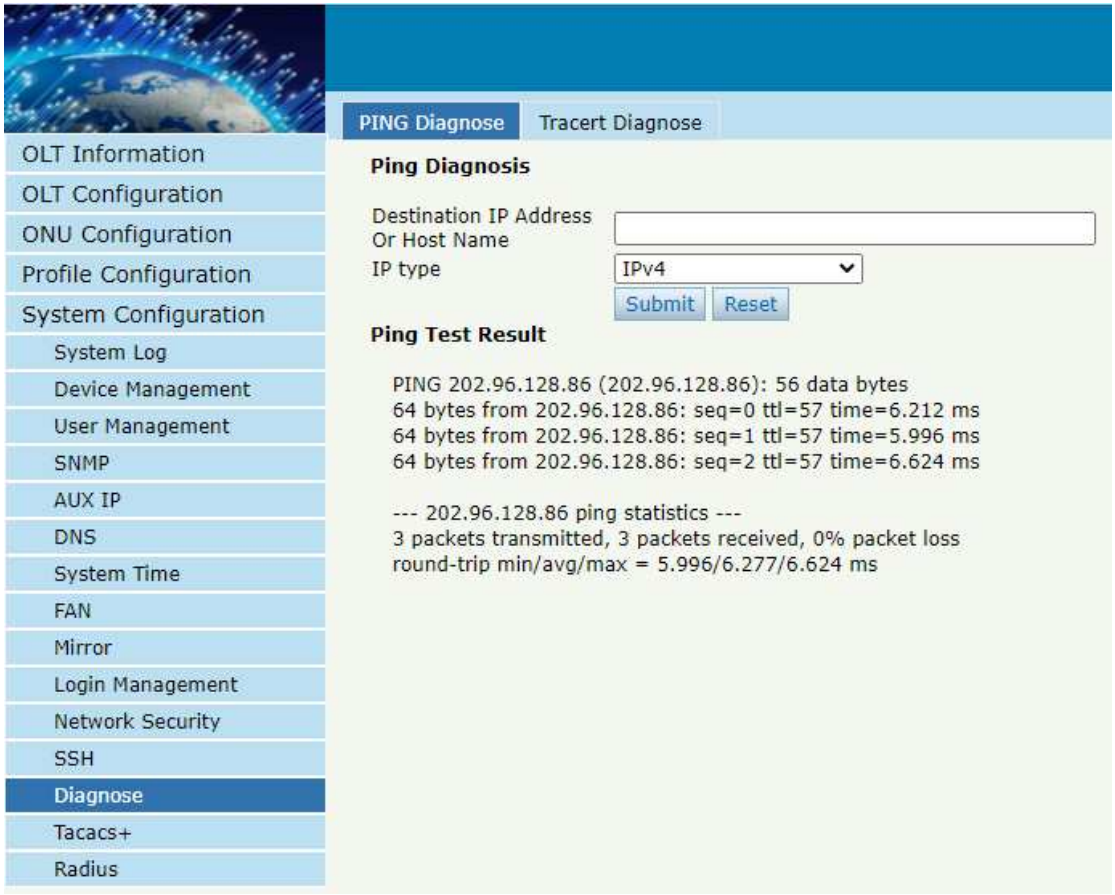


Figure 6.13-1: Ping Diagnose Configuration

6.13.2 Tracert Diagnose

System Configuration → Diagnose→ Tracert Diagnose
This interface is used to track and diagnose routing and forwarding.

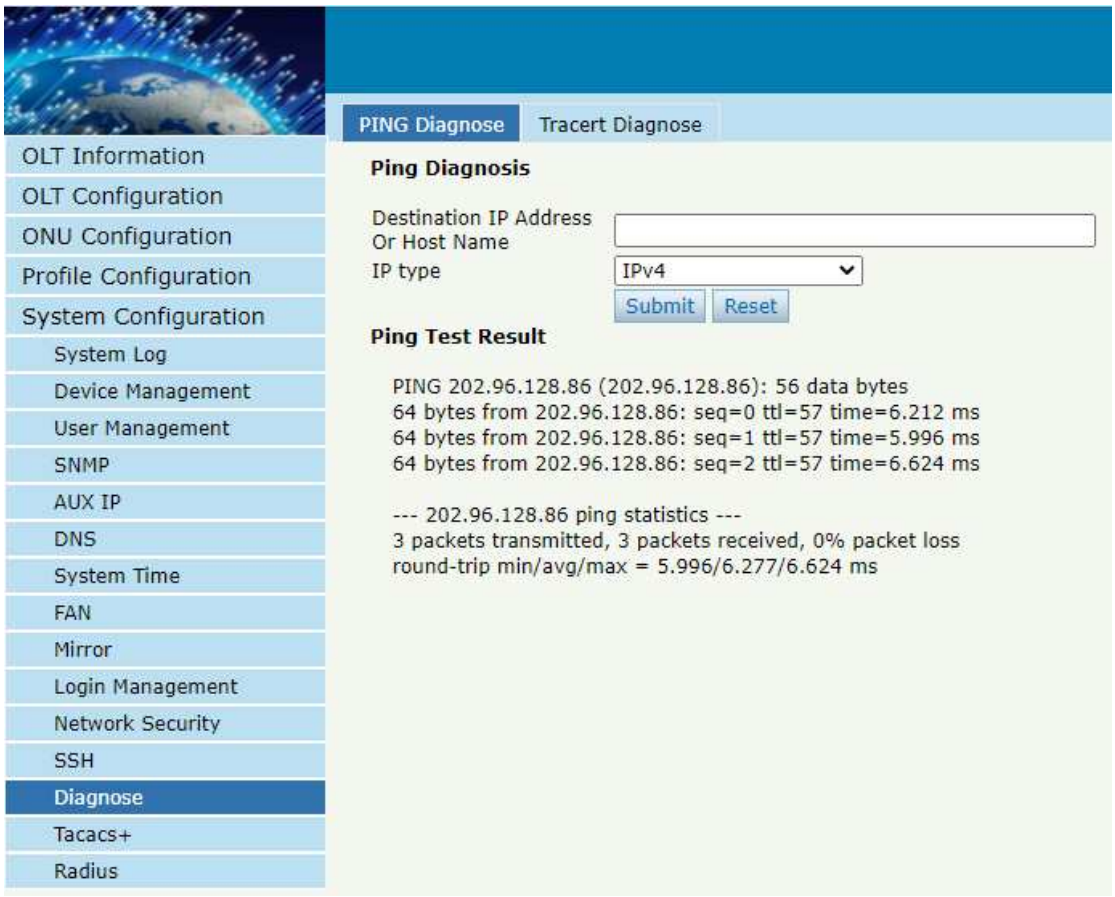


Figure 6.13-2: Tracert Diagnose Configuration

6.14 Tacacs+

Tacacs+ is a protocol that provides access control for routers, network access servers, and other interconnected computing devices through one or more centralized servers. Tacacs+ provides independent authentication, authorization, and billing services.This interface allows you to configure the Tacacs+ server IP address and other specific parameters.

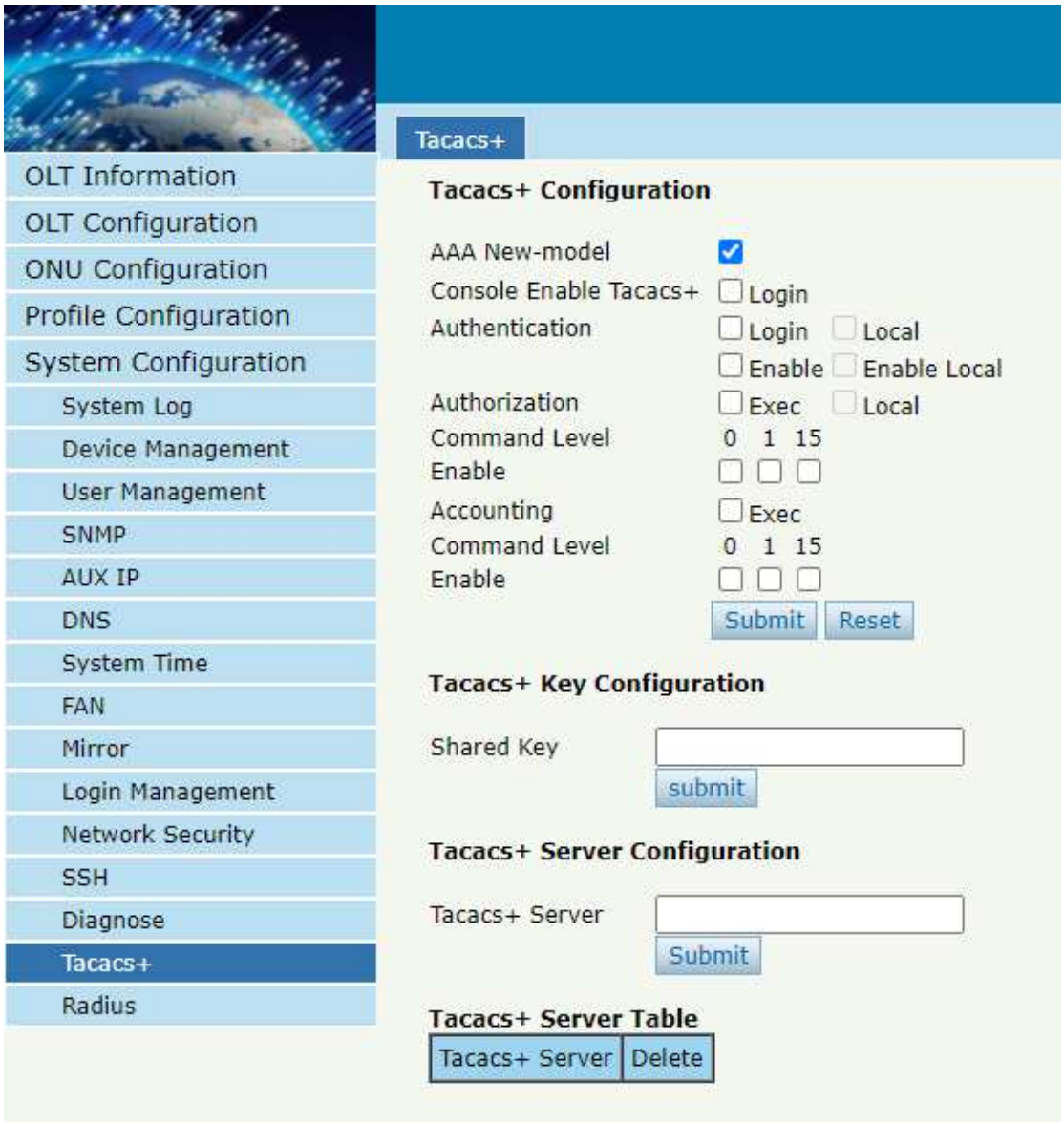


Figure 6.14-1: Tacacs+ Configuration

6.15 Radius

Radius is a protocol for authentication, authorization, and accounting information.The Radius server is responsible for receiving the user's connection request, authenticating the user, and then returning all the necessary configuration information to the client to send the service to the user.This interface allows you to configure the Radius server IP address and other parameters.

Figure 6.15-1: Radius Configuration

--------END--------