User Manual

TOLT-4422 Layer 3 GPON OLT - 4 GPON ports

Article				Article no.
TOLT-4422	Layer 3 GPON OLT – 4 GPON ports			308500
Version	V1.0	**Date**	2025/08	**EN**

triax.com

Table of content

1 Safety Instructions

Read these instructions carefully before connecting the unit

ATTENTION

- Failure to comply with the specified precautionary measures may cause serious injury to persons or damage to property.
- The assembly, installation, additional electrical wiring, servicing and commissioning may only be performed by suitably qualified persons, technicians or installers in compliance with safety regulations.
- Damage due to improper installation and commissioning, defective connectors on cables or any other incorrect handling will void the warranty.

CAUTION

- The safety requirements are according to the standards EN 62368-1 resp. EN 60728-11 and must be observed, especially concerning equipotential bonding and earthing.
- Observe the relevant country-specific standards, regulations and guidelines on the installation and operation of antenna systems.
- Before starting installation or service work disconnect the receiving system from mains.
- Installation or service work should NEVER be undertaken during electrical / thunderstorms.
- Avoid short circuits!
- To ensure electromagnetic compatibility, make sure all connections are tight and that the covers are screwed on securely.
- Take action to prevent static discharge when working on the device!
- Due to the risk of fires caused by lightning strikes, we recommend that all mechanical parts (e.g. distributor, equipotential bonding rail, etc.) be mounted on a non-combustible base. Wood panelling, wooden beams, plastic covered panels and plastic panels are all examples of combustible bases.

⚠ To prevent fire, short circuit or shock hazard:

- Do not expose the unit to rain or moisture.
- Install the unit in a dry location without infiltration or condensation of water.
- Do not expose it to dripping or splashing.
- Do not place objects filled with liquids, such as vases, on the apparatus.
- If any liquid should accidentally fall into the cabinet, disconnect the power plug.

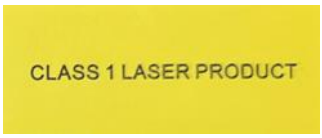
⚠ To avoid any risk of overheating:

- Install the unit in a well aired location and keep a minimum distance of 5 cm around the apparatus for sufficient ventilation.
- Do not place any items such as newspapers, tablecloths, curtains, on the unit that might cover the ventilation holes.
- Do not place any naked flame sources, such as lit candles, on the apparatus.
- Do not install the product in a dusty place.
- Use the apparatus only in moderate climates (not in tropical climates).
- Respect the minimum and maximum temperature specifications.

To avoid any risk of electrical shocks:

- Connect apparatus only to a power socket with a protective earth connection.
- The mains plug shall remain readily operable.
- Pull out power plug to make the different connections of cables.
- To avoid electrical shock, do not open the housing of the product.

Warning (if SFP module is instered)



To avoid exposure to laser radiation from optical fibre or active optical devices like transmitters or receivers which pose a hazard to your health, you should:

- Never look into an exposed end of an optical fibre or mirror surfaces that could reflect light from an open optical fibre.
- Never look into an optical fibre connected with the radiation source with optical instruments (magnifying glass, microscope, etc...).
- Use an approved fibre optic cable to maintain conformity with applicable laser safety requirements.

Concerning fibre optic cables:

- Wearing protective goggles is recommended.
- You should handle fibre optic cables with extreme caution, particularly when unbundling or terminating a cable. The internal glass core of a fibre optic cable is brittle when the shielding and buffer material is removed. It will easily disintegrate into small pieces which may cause injury to the human body.
- Remove all filings immediately using tweezers, place them in a tightly sealed dustbin and dispose in accordance with local regulations.

Maintenance

Only use a dry soft cloth to clean the cabinet.

Do not use solvent.

For repairing and servicing, refer to qualified personnel.

Dispose according to your local authority's recycling processes

Electronic devices should never be disposed of in the household rubbish. In accordance with directive 2002/96/EC of the European Parliament and the European Council from January 27, 2003 which addresses old electronic and electrical devices, such devices must be disposed of at a designated collection facility. At the end of its service life, please take your device to one of these public collection facilities for proper disposal.

2 Introduction

2.1 Product description

The TOLT-4422 is a 19” rack mount GPON OLT with 4 PON ports that provides flexible and fast FTTx access, suiting scenarios such as sparsely populated or remote areas, industrial parks, commercial buildings and other MDU settings including hospitality.

2.2 Detailed features

- Compact design, meets various application scenarios:
  - Supports deployment in diverse scenarios including low density areas, remote/sparsely populated areas and industrial parks
  - Supports FTTM and sharing site/rack with wireless base stations
- Small size and lightweight, easier to transport and install:
  - Supports multiple installation modes, e.g, limited room space, basement and small rack or cabinet
- Carrier-class security protection, supports dynamic routing protocol RIP&OSPF, ensures the safe operation of the network:
  - Supports uplink redundancy protection including LACP STP, RSTP and MSTP
  - Supports RIP & OSPF protocol
  - Supports link protection
- Lower TCO:
  - Dramatically saves on investment fees in trunk fibres, pipe engineering and facilities.
  - Effectively reduce CapEx and OpEx

2.3 Installation

Preparation before installation:

- **Observe instructions given at chapter 1**
- Install the unit in a well aired location and keep a minimum distance of 5 cm around the TOLT for sufficient ventilation. Please don’t block the cooling holes of the device
- Connect the OLT only to a power socket with a protective earth connection
- Please make sure the power supply button on the rear panel is turned to OFF before the power supply cable is connected
- Please ensure the interface of the fibre is clean before connecting the fibre (if SFP module is inserted)
- If needed clean the fibre connector with the correct tool (if SFP module is inserted)

2.4 Front panel

2.5 Rear panel

2.6 Interfaces

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

2.7 Supported functions

2.7.1 MANAGEMENT

- SNMP, Telnet, CLI, WEB, SSH v2
- Fan Group Control
- Port status monitoring and configuration management
- Online ONT configuration and management
- User management
- Alarm management

2.7.2 LAYER 2 SWITCH

- 32K Mac address
- Supports 4096 VLANs
- Supports port VLAN
- Supports VLAN tag/Un-tag, VLAN transparent transmission
- Supports VLAN translation and QinQ
- Supports storm control based on port
- Supports port isolation
- Supports port rate limitation
- Supports 802.1D and 802.1W
- Supports static LACP, Dynamic LACP
- QoS based on port, VID, TOS and MAC address
- Access control list
- IEEE802.x flow control
- Port stability statistic and monitoring

2.7.3 MULTICAST

- IGMP snooping
- 2048 IP Multicast Groups

2.7.4 DHCP

- DHCP server, DHCP relay, DHCP snooping
- DHCP option82

2.7.5 LAYER 3 ROUTE

- ARP proxy
- 4096 hardware Host Routes, 512 hardware Subnet Routes
- Supports Radius, TACACS+
- Supports IP source guard
- Supports static route, dynamic route RIP v1/v2, RIPng and OSPF v2/v3

2.7.6 IPV6

- Supports NDP
- Supports IPv6 Ping, IPv6 Telnet, IPv6 routing
- Supports ACL based on source IPv6 address, destination IPv6 address, L4 port, protocol type, etc…
- Supports MLD v1/v2 snooping (Multicast Listener Discovery snooping)

2.7.7 GPON FUNCTION

- T-CONT DBA
- Gemport traffic
- Is compliant with ITU-T984.x standard
- Up to 20KM transmission distance
- Supports data encryption, multicast, port VLAN separation, RSTP, etc…
- Supports ONT auto-discovery/link detection/remote upgrade of software
- Supports VLAN division and user separation to avoid broadcast storm
- Supports power-off alarm function, for easy link problem detection
- Supports broadcasting storm resistance function
- Supports port isolation between different ports
- Supports ACL and SNMP to configure data packet filter
- Specialised design for system breakdown prevention to maintain a stable system
- Supports RSTP

2.7.8 Various

- Power consumption: 35W
- Working temperature: -20°C ~+60°C
- Storage temperature: -40~+70°C
- Relative humidity: 5~95% (non-condensing)
- Dimension (L*W*H): 442mm * 229mm * 43.6mm
- Weight
    - Net weight of single power: 2.95kg
    - Gross weight of single power: 4.15kg

2.8 Login to the OLT

Follow the steps to login:

- The device default IP address is 192.168.8.200
- Open your web browser, type the device IP in address bar
- Entry of the username and password will be prompted. Enter the default login Username and Password as per the Product label

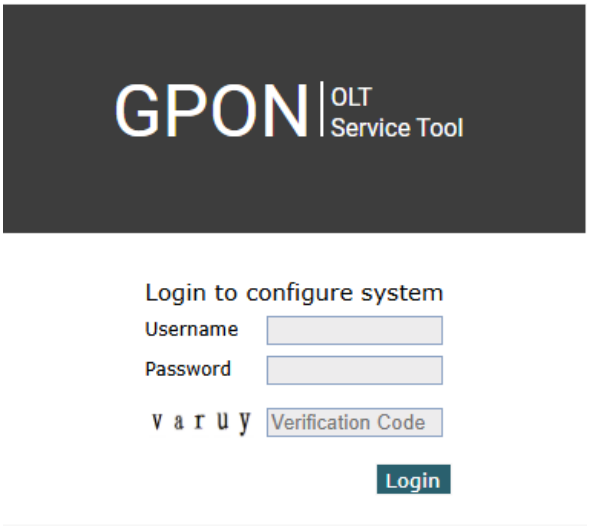


Figure 2.7: Login

2.9 Device Information

The OLT ports connection status is 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.

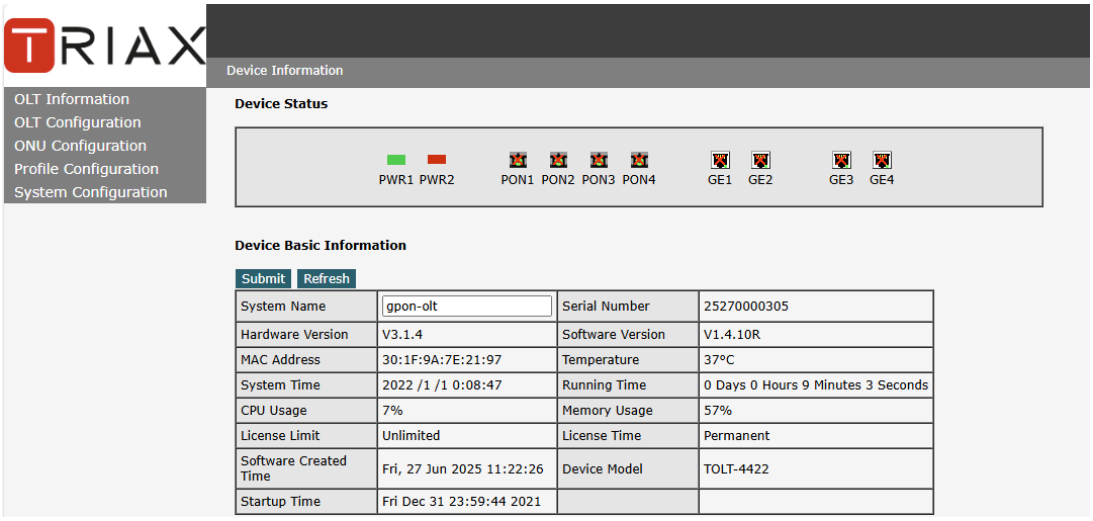


Figure 2.8: Device Information

3 OLT configuration

This section is about the basic service of OLT configuration.

3.1 VLAN

OLT equipment switch engine 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 1~4095.

All switch ports, including uplink ports and downlink ports, support VLAN partition.

VLAN 1 is the system reserved VLAN, it includes all switch ports which are UNTAG mode.

3.1.1 Create VLAN

OLT Configuration→VLAN

In this user interface, you can create new VLAN.

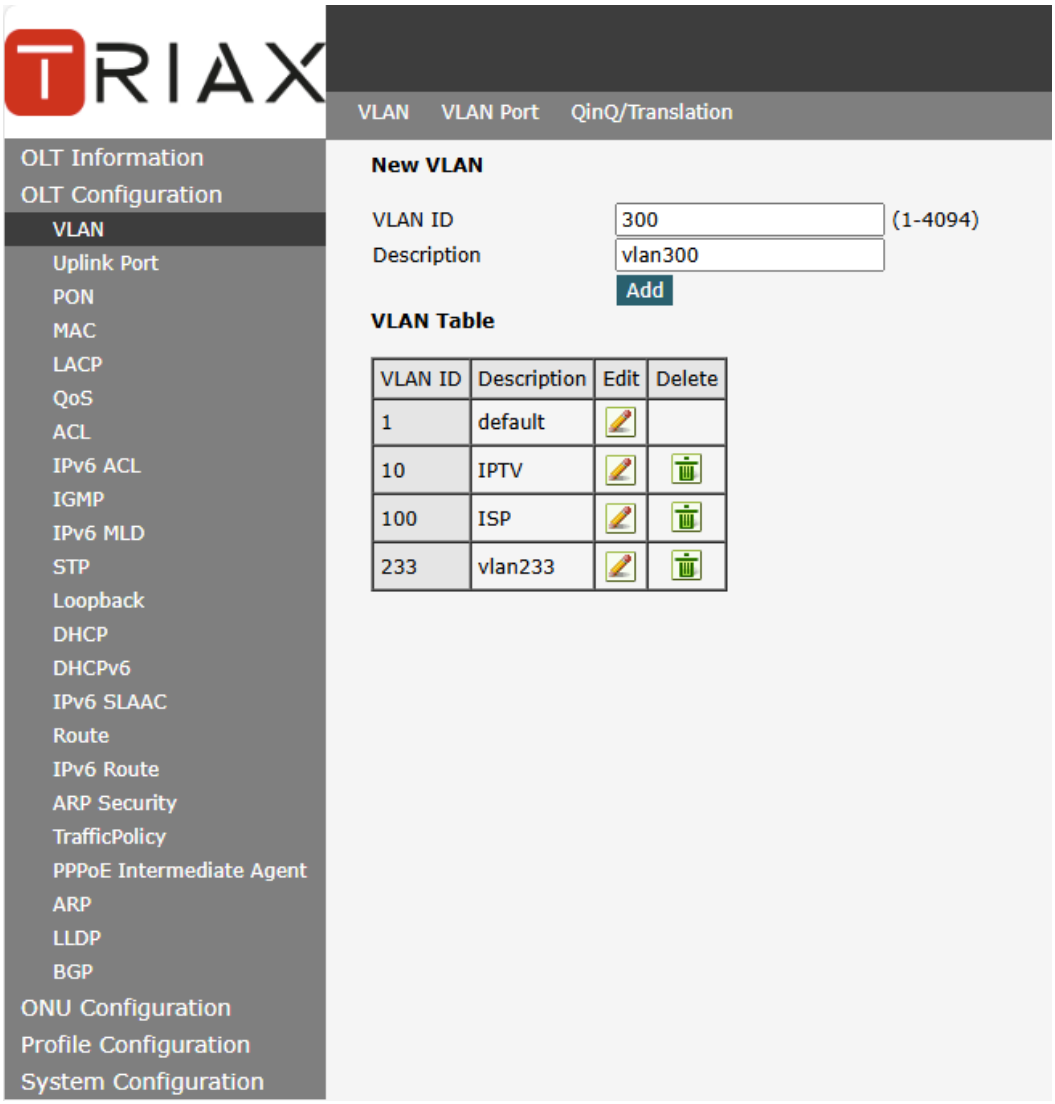


Figure 3.1-1: Create New VLAN

3.1.2 VLAN Port

OLT Configuration→VLAN→VALN Port

Assign the ports to the VLANs that have been created. You can choose the tag or untag VLAN mode.

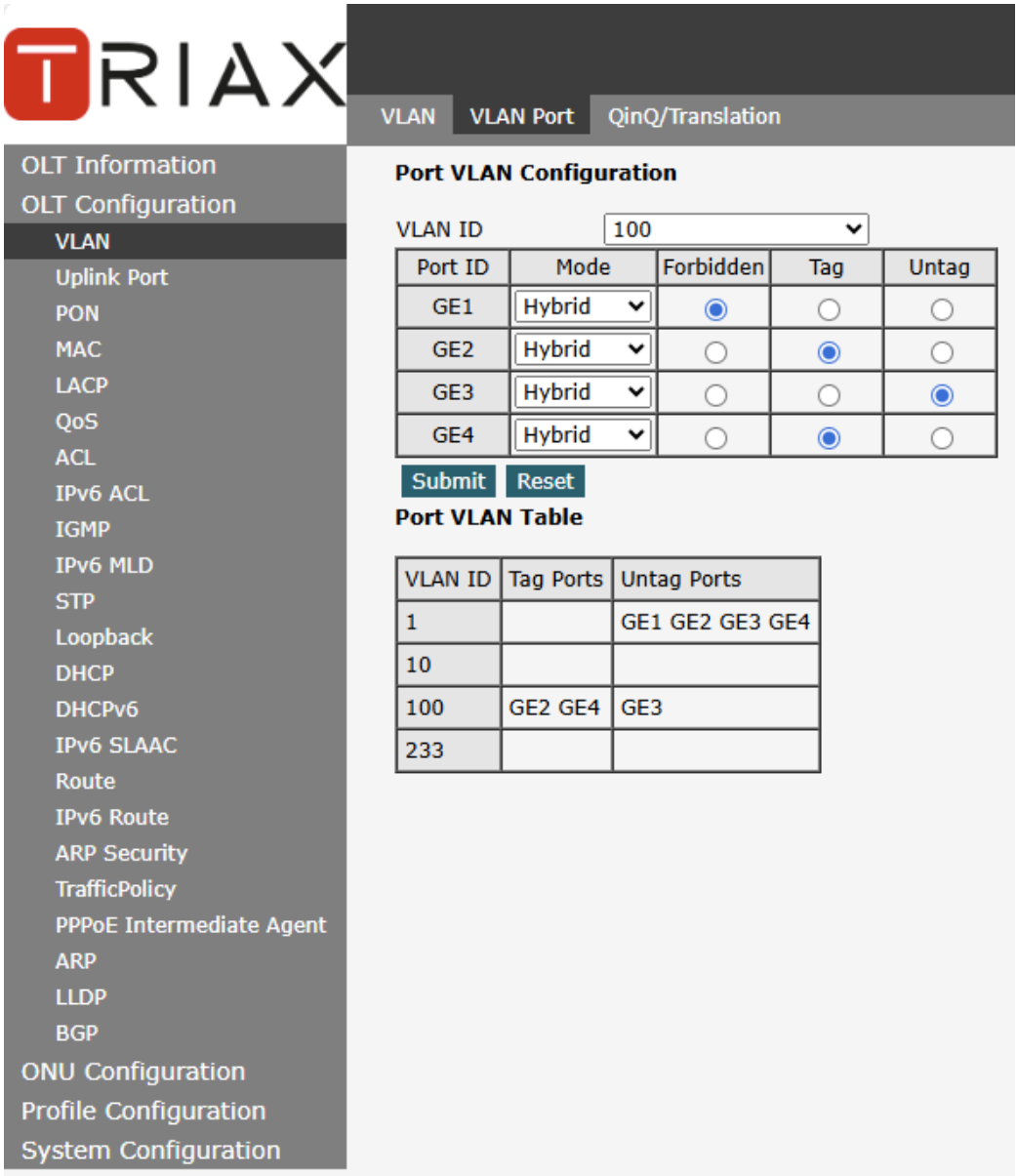


Figure 3.1-2: Add VLAN Port

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.

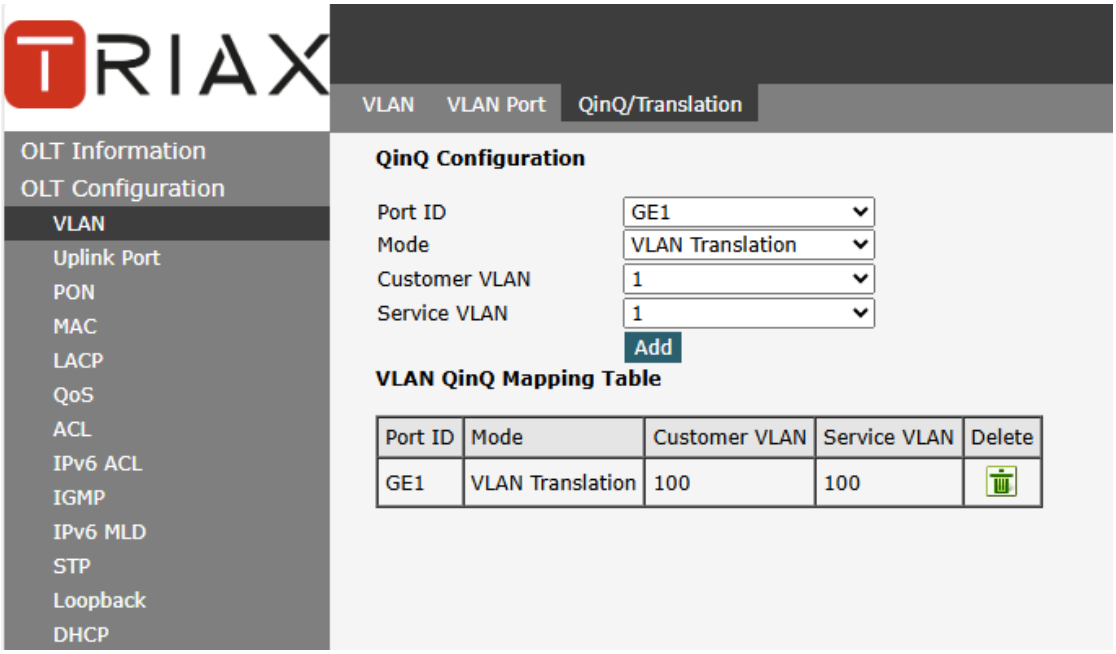


Figure 3.1-3: QinQ/Translation Configuration

3.1.4 P2P

OLT Configuration→PON→Configuration

The use of P2P enables ONU to communicate with each other under PON ports.

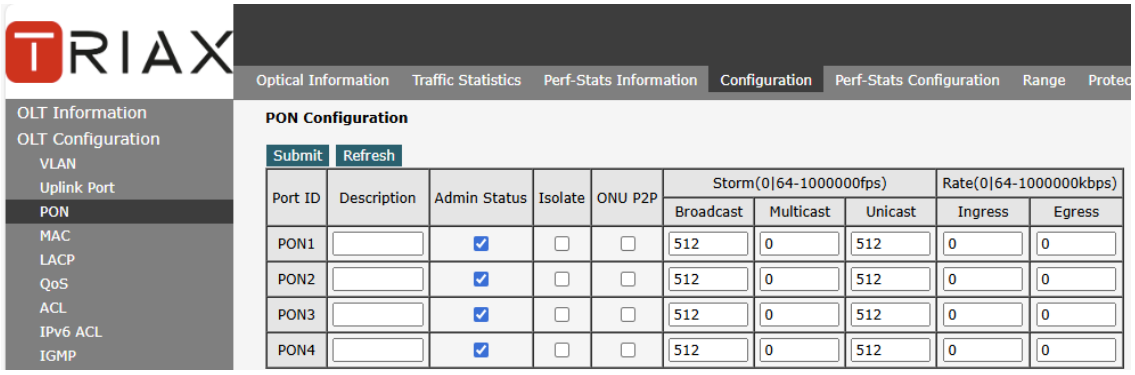


Figure 3.1-5: P2P Configuration

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 of uplink ports.

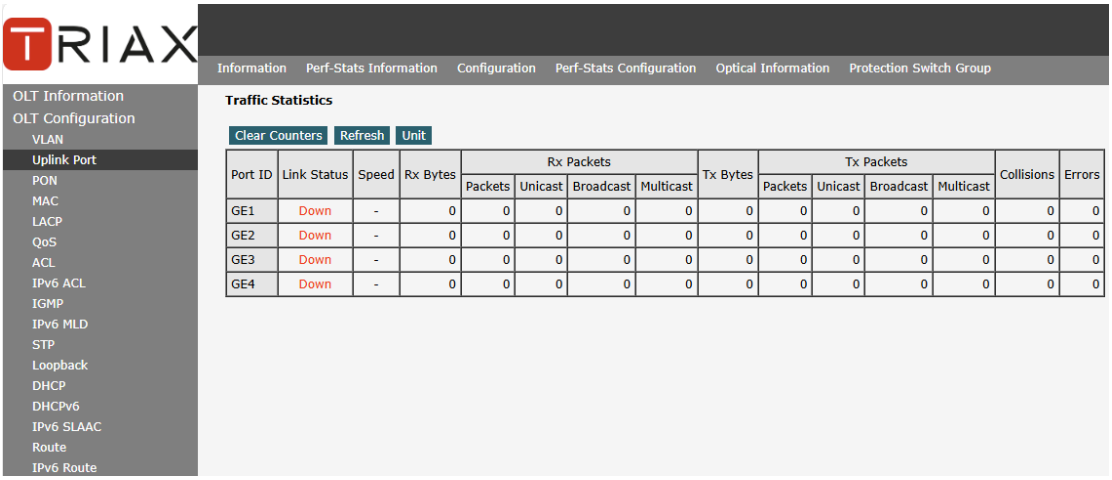


Figure 3.2-1: GE Traffic Statistics

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.

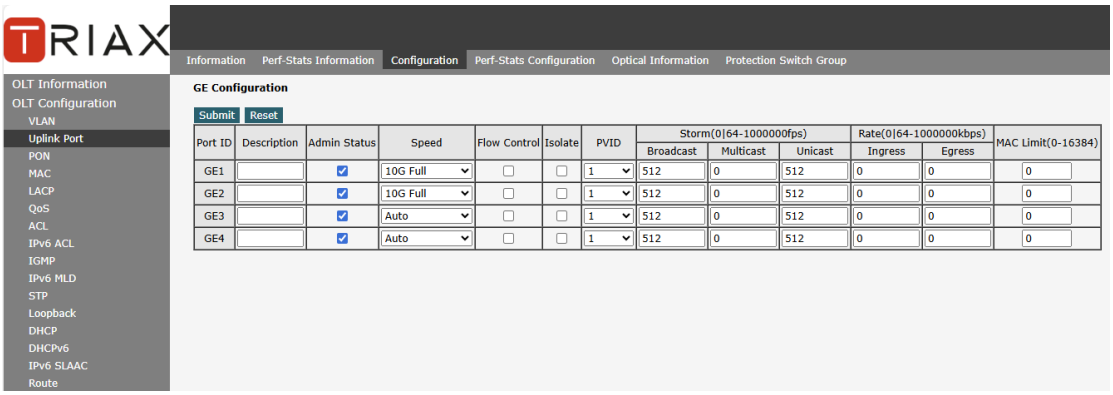


Figure 3.2-2: Uplink Ports Configuration

Illustrations of each parameter:

Parameters	Illustration
Port ID	GE port has two types, fibre SFP (GE1 to GE8) and copper (GE9 to GE16).
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. Disabled by default.
Isolate	Port isolation with each other.
PVID	Default VLAN ID of the port.
Broadcast	Broadcast storm inhibition.
Multicast	Multicast storm inhibition.
Unknown Unicast	Unknown unicast storm inhibition.
Ingress Rate	Port ingress rate.
Egress Rate	Port egress rate.
MAC limit	Number of MAC address can be learnt in the port.

3.3 PON

3.3.1 Information

OLT Configuration→PON→Information

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

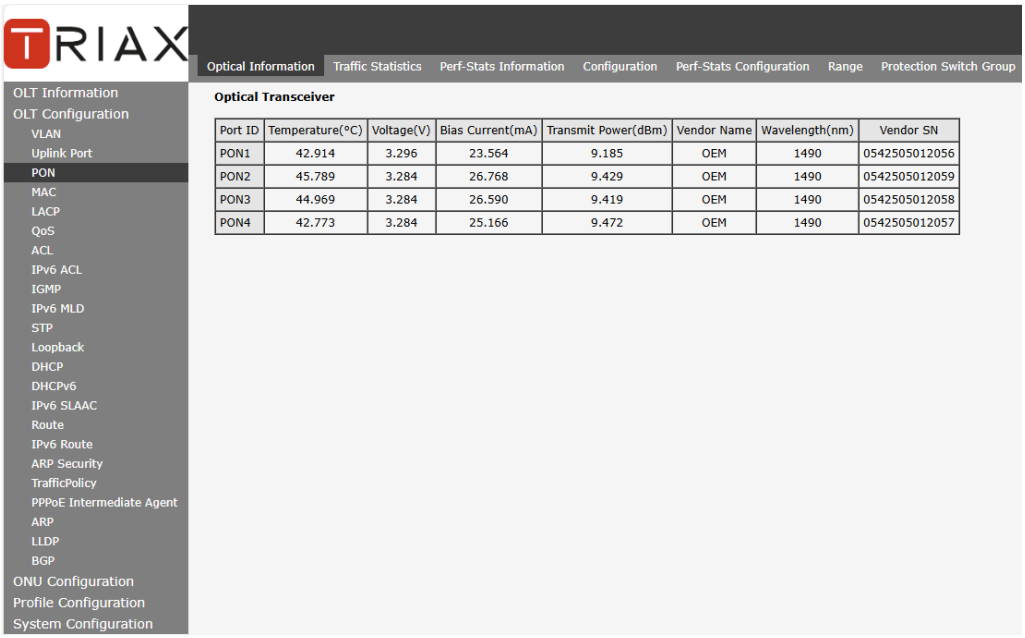


Figure 3.3-1: PON Information

3.3.2 Traffic Statistics

OLT Configuration→PON→Traffic Statistics

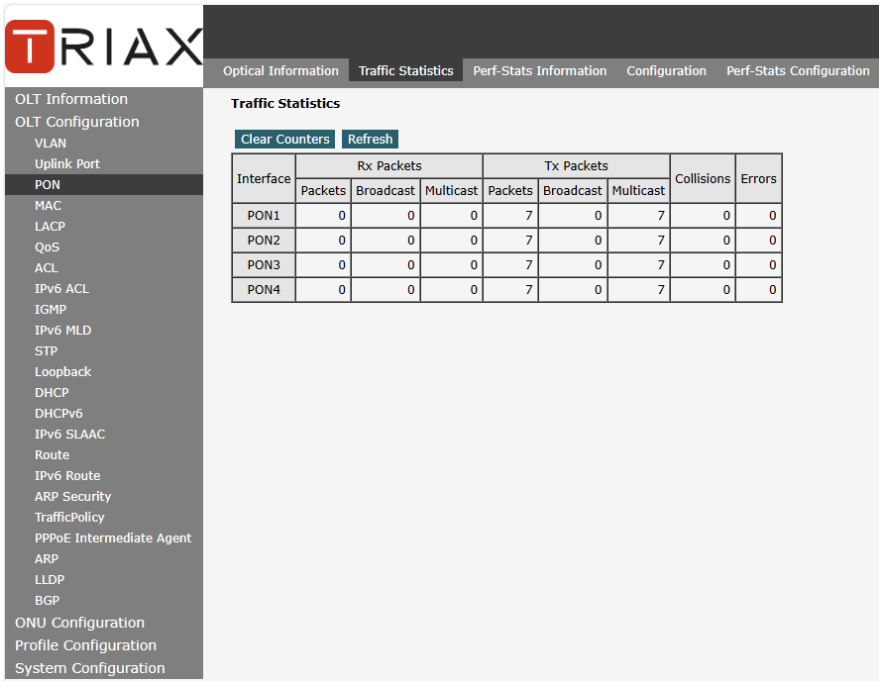


Figure 3.3-2: Traffic Statistics

3.3.3 Configuration

OLT Configuration→PON→Configuration

This user interface is used to configure port status.

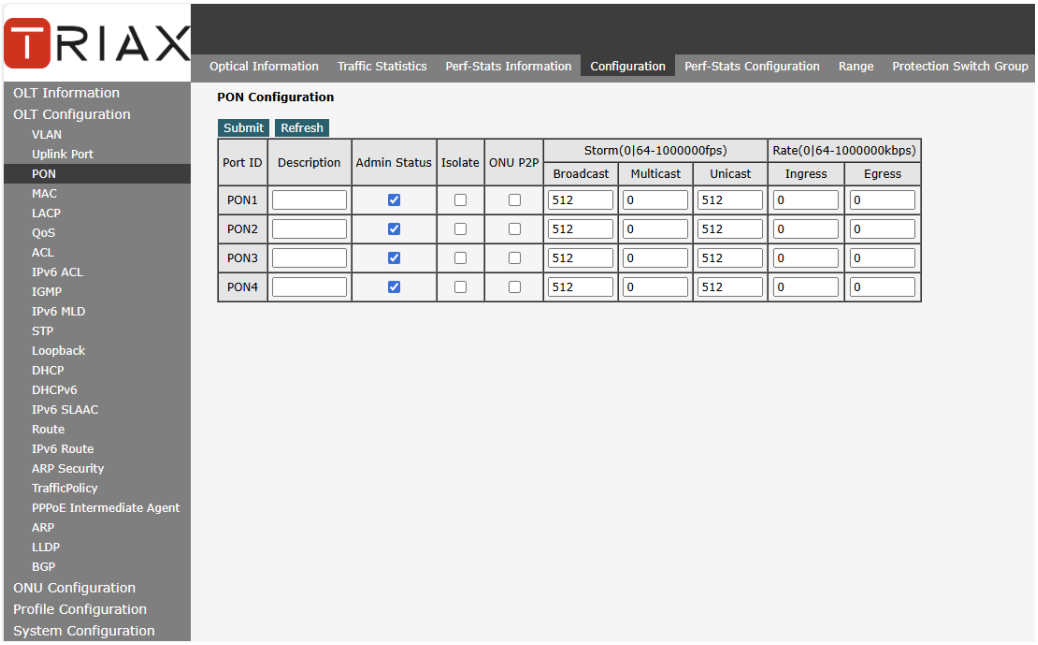


Figure 3.3-3: PON configuration

3.3.4 Range

OLT Configuration→PON→Range

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

For example, ONU is 25km away from OLT, the minimum is 50 and the maximum is 250.

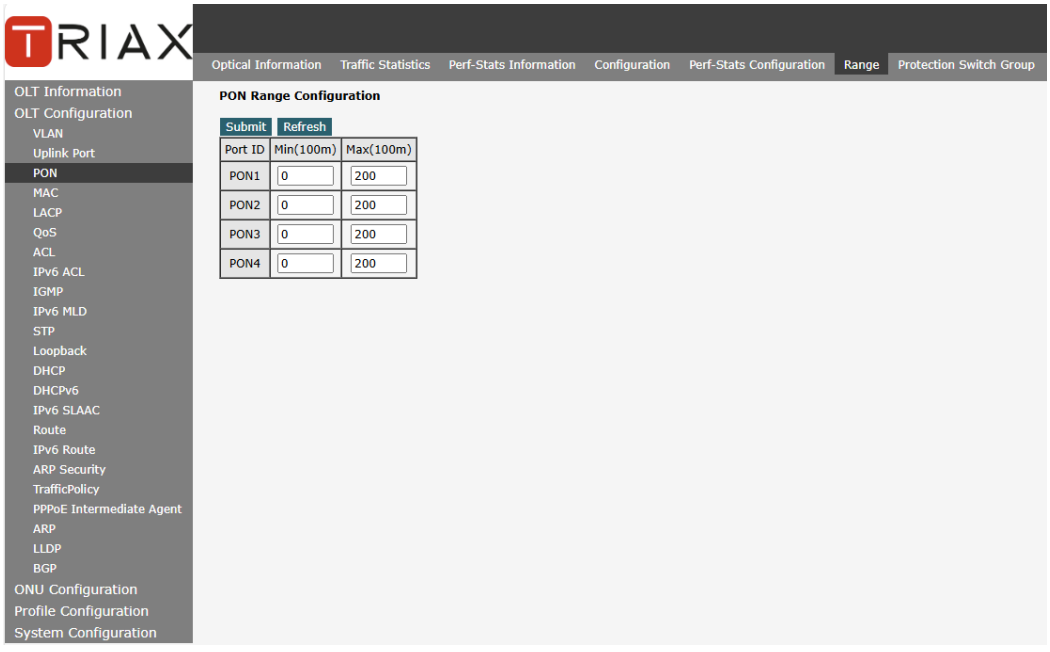


Figure 3.3-4: PON Range Configuration

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.

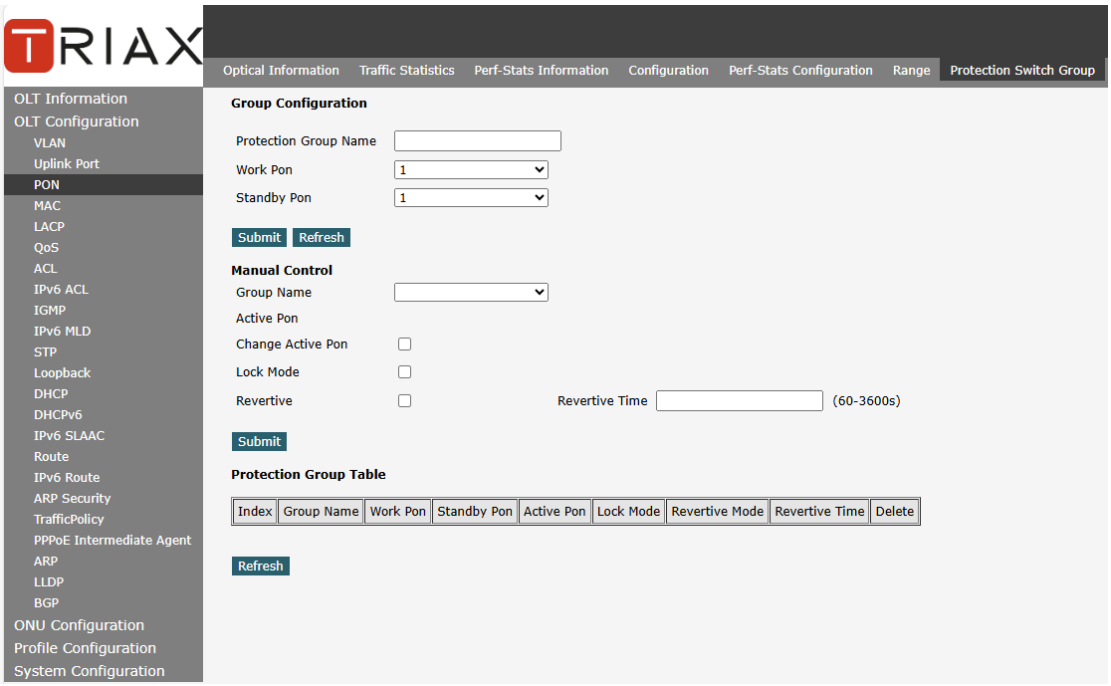


Figure 3.3-5: PON Protection Switch Group Configuration

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 learnt at PON ports and GE ports.

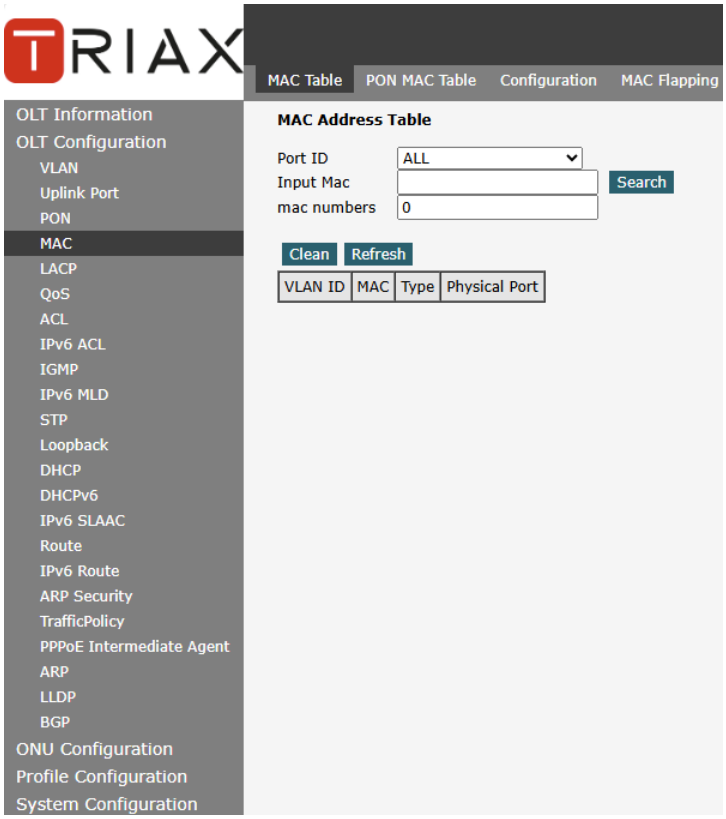


Figure 3.4-1: MAC Address Table

3.4.2 PON MAC Table

OLT Configuration→MAC→PON MAC Table

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

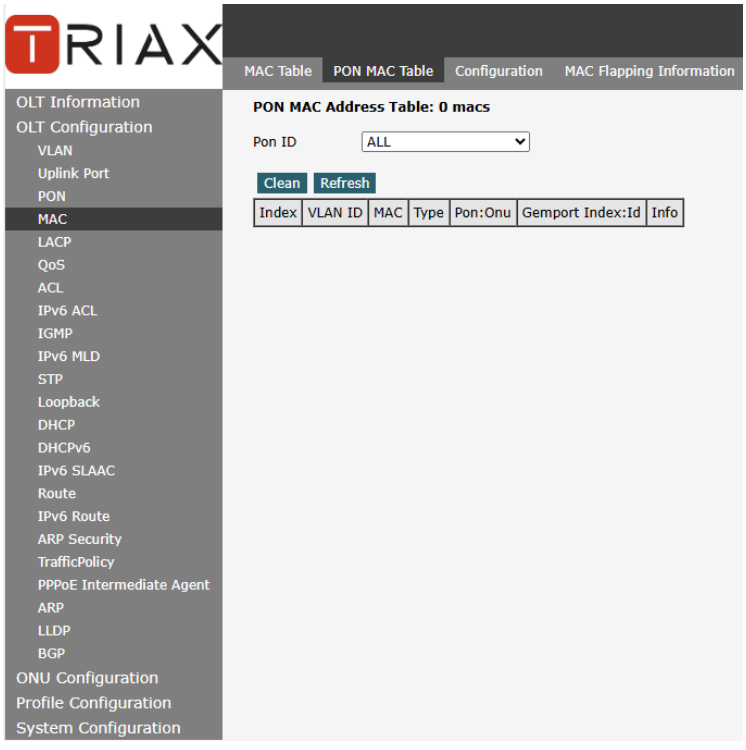


Figure 3.4-2: PON MAC Table

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.

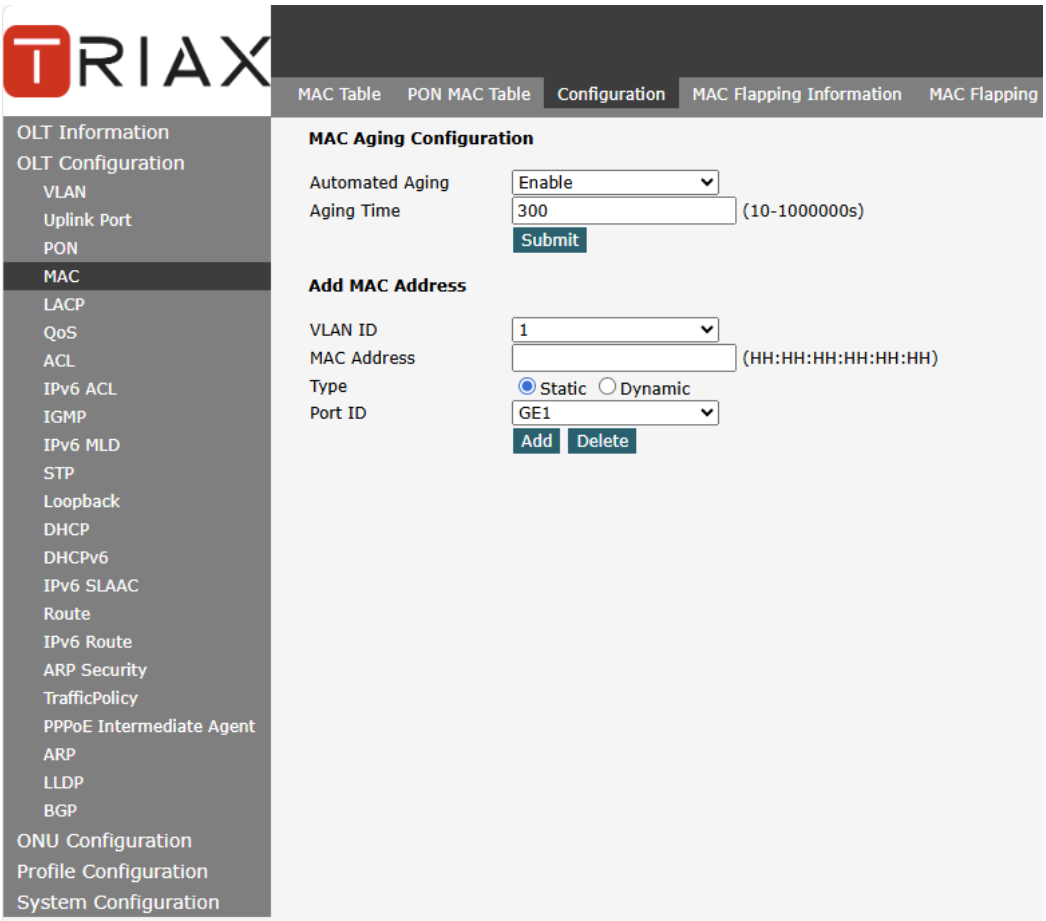


Figure 3.4-3: MAC Configuration

3.4.4 MAC Flapping Information

This interface displays information learned on multiple ports for the same MAC if you enable MAC Flapping switch.

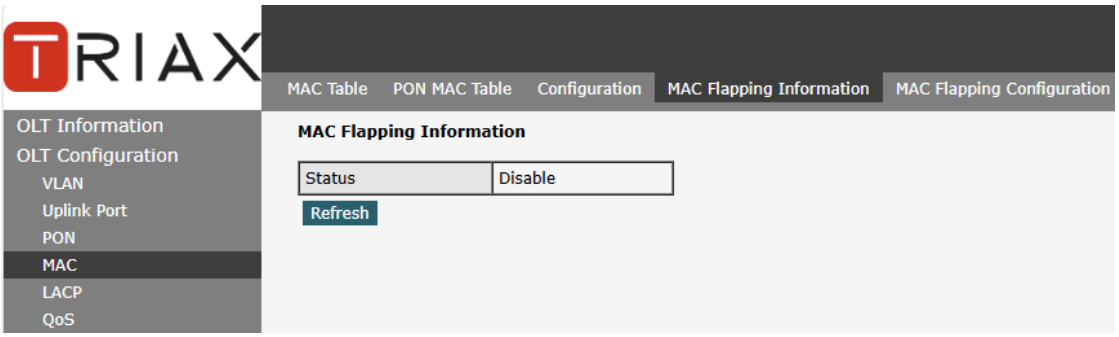


Figure 3.4-4: MAC Flapping Information

3.4.5 MAC Flapping Configuration

You can enable MAC Flapping Configuration in this interface.

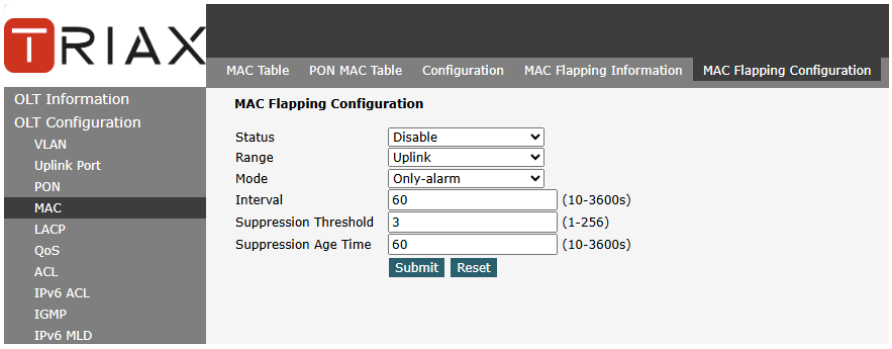


Figure 3.4-5: MAC Flapping Configuration

3.4.6 MAC Flapping Port Configuration

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

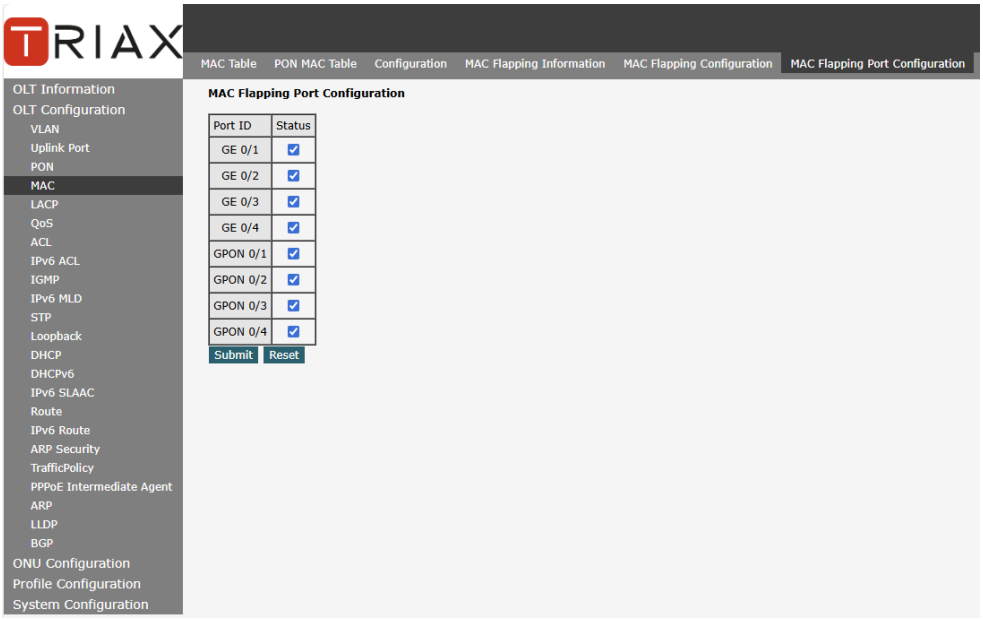


Figure 3.4-6: MAC Flapping Port Configuration

3.5 LACP

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.

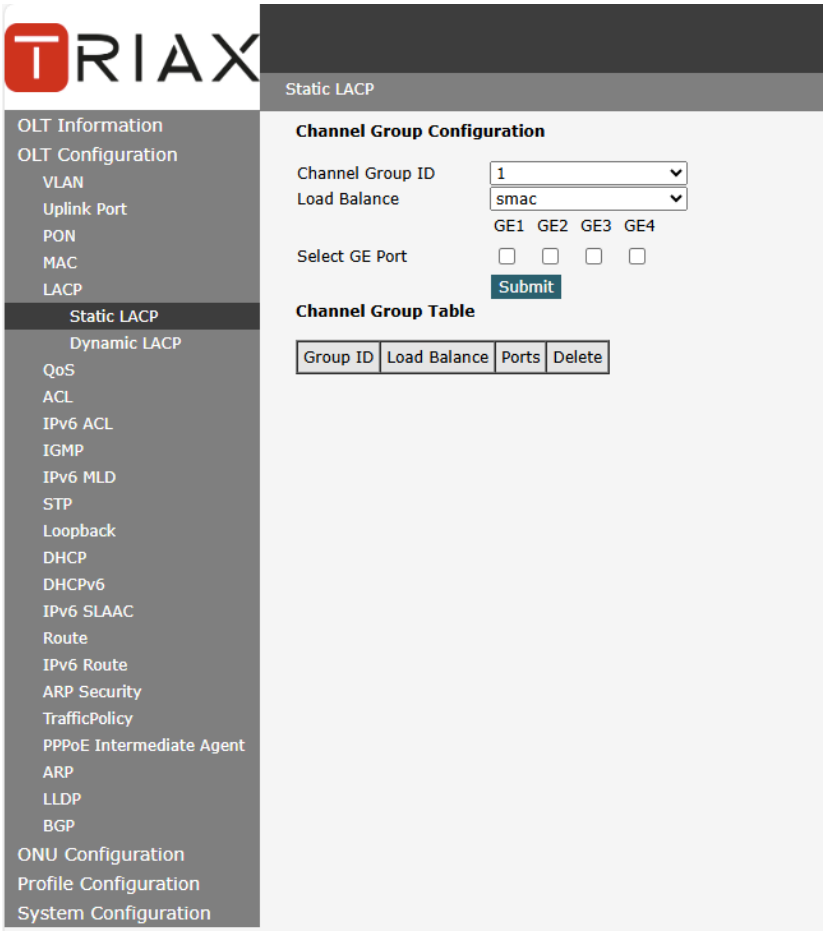


Figure 3.5-1: Create Static LACP

3.5.2 Dynamic LACP

OLT Configuration→LACP→Dynamic LACP

This page displays dynamic LACP information. Only the port which is linkup can be shown in the table. OLT can detect how many devices the uplink ports connected to. If the ports are connected to the same device, they will be in a channel group, otherwise in different channel group.

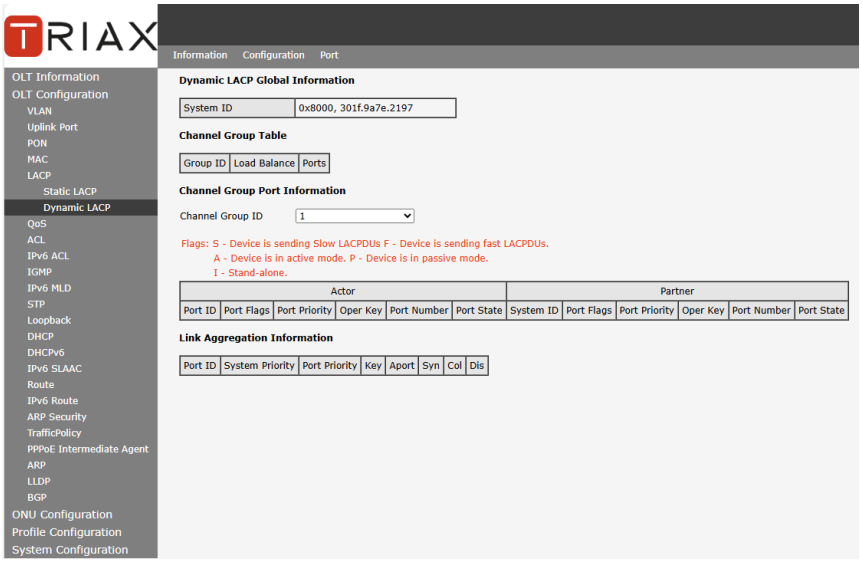


Figure 3.5-2: Dynamic LACP Information

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.

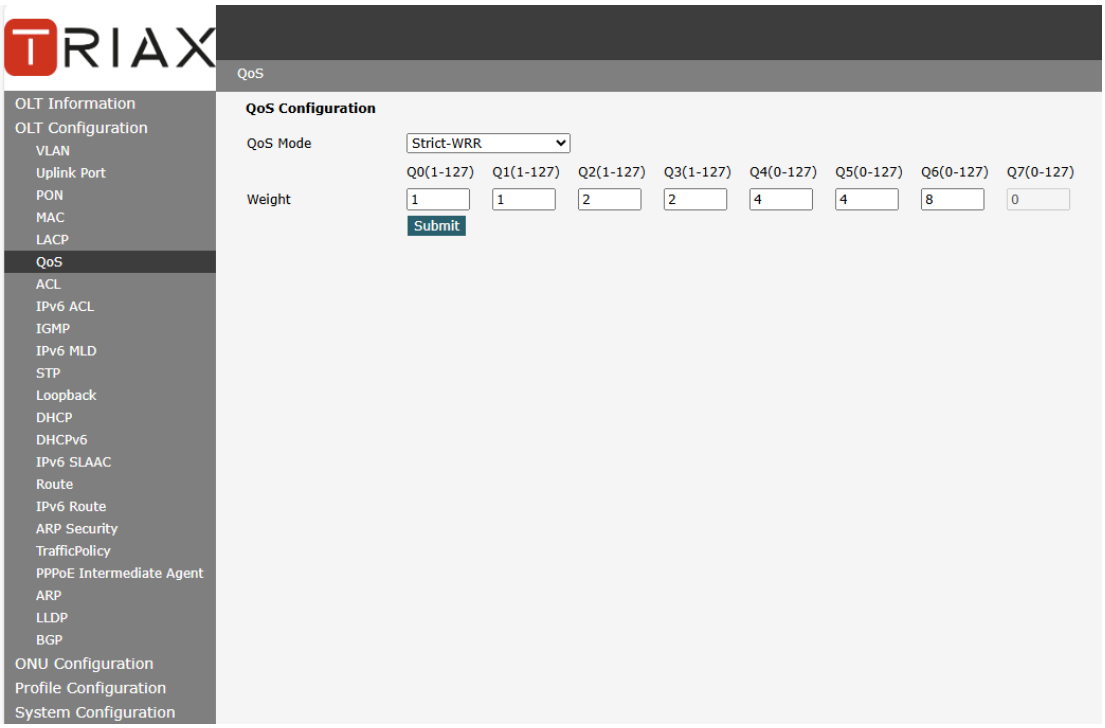


Figure 3.6-1: QOS Configuration

3.7 ACL

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

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.

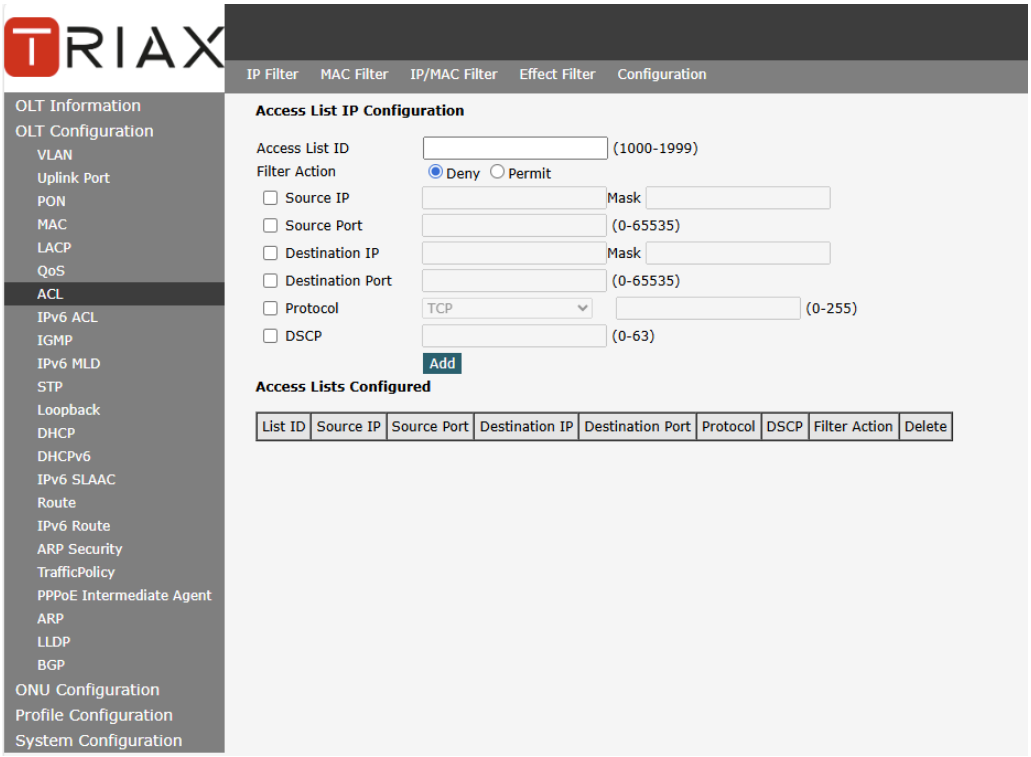


Figure 3.7-1: IP Filter

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.

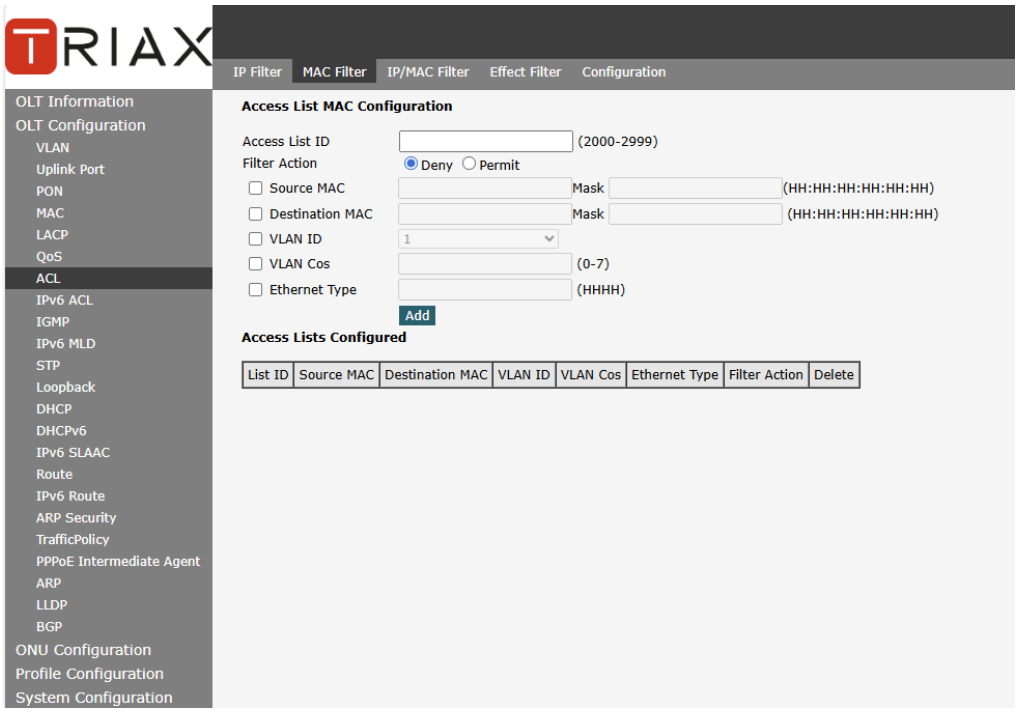


Figure 3.7-2: MAC Filter

3.7.3 IP/MAC Filter

OLT Configuration→ACL→IP/MAC Filter

This filter mixes the IP address and MAC address, include source MAC address and destination MAC address, source IP address and destination IP address.

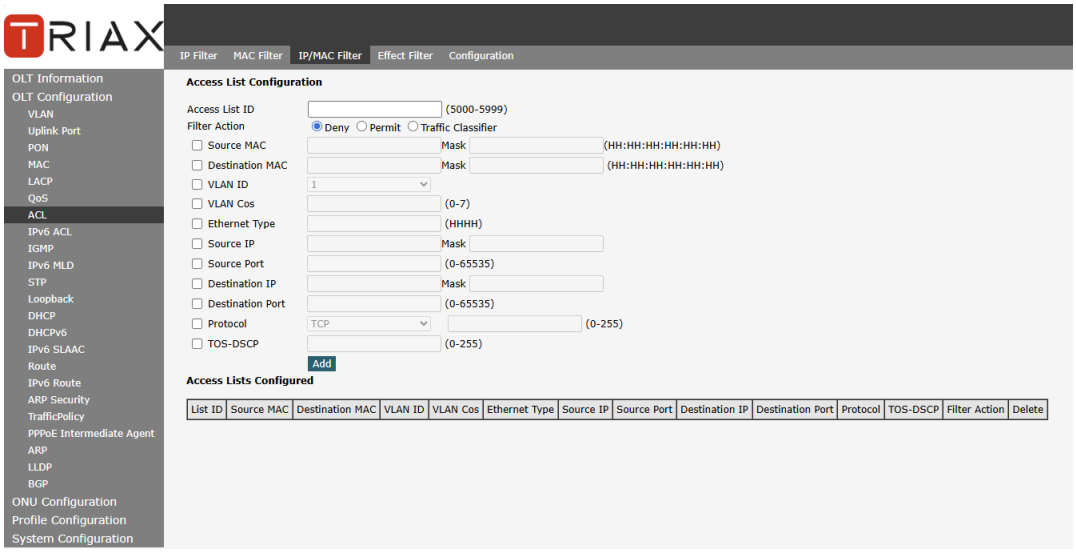


Figure 3.7-3: IP/MAC Filter

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.

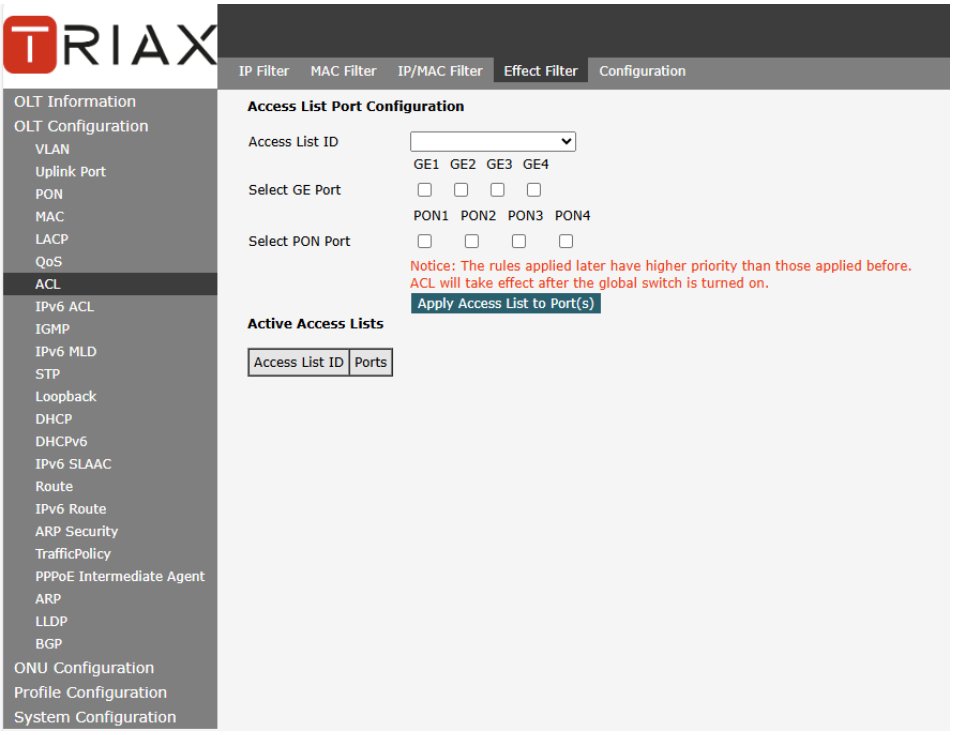


Figure 3.7-4: Bind Security Filter

3.8 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.

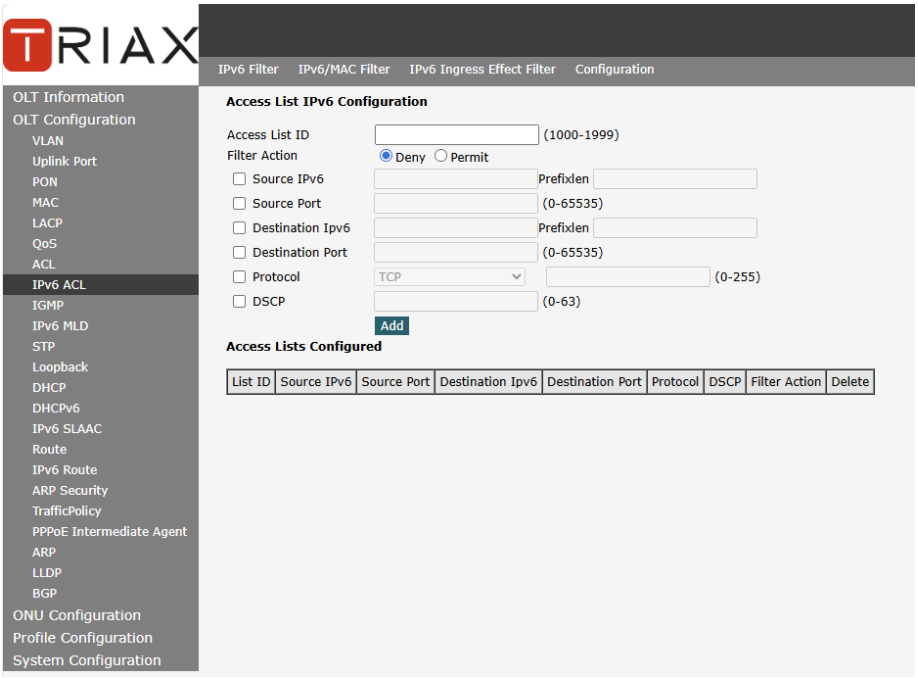


Figure 3.8-1: IPv6 Filter

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.

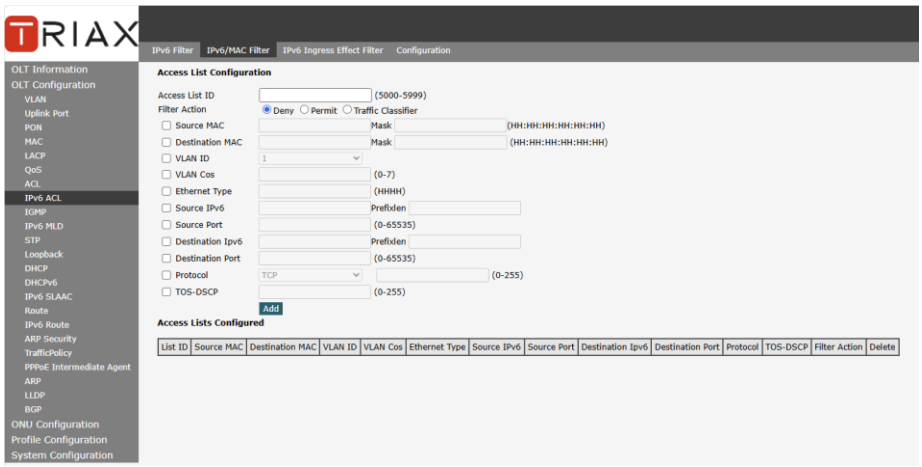


Figure 3.8-2: IPv6/MAC Filter

3.8.3 IPv6 Effect Filter

OLT Configuration → IPv6 ACL →IPv6 Effect Filter

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

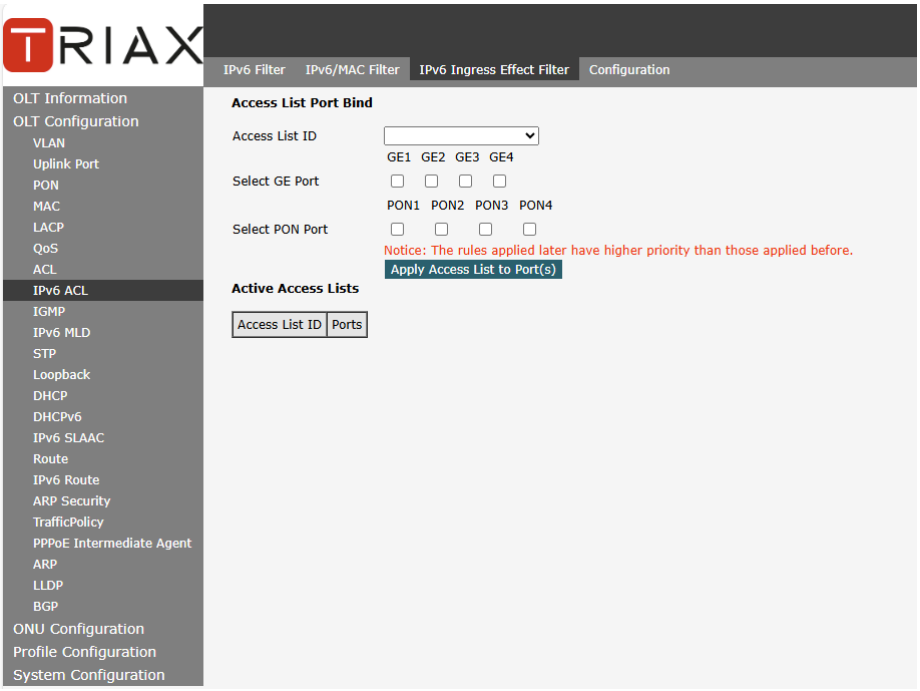


Figure 3.8-3: Bind IPv6 Security Filter

3.9 IGMP

3.9.1 Group Member

OLT Configuration→IGMP→Group Member

When there is a multicast group produced, the group will display in this table.

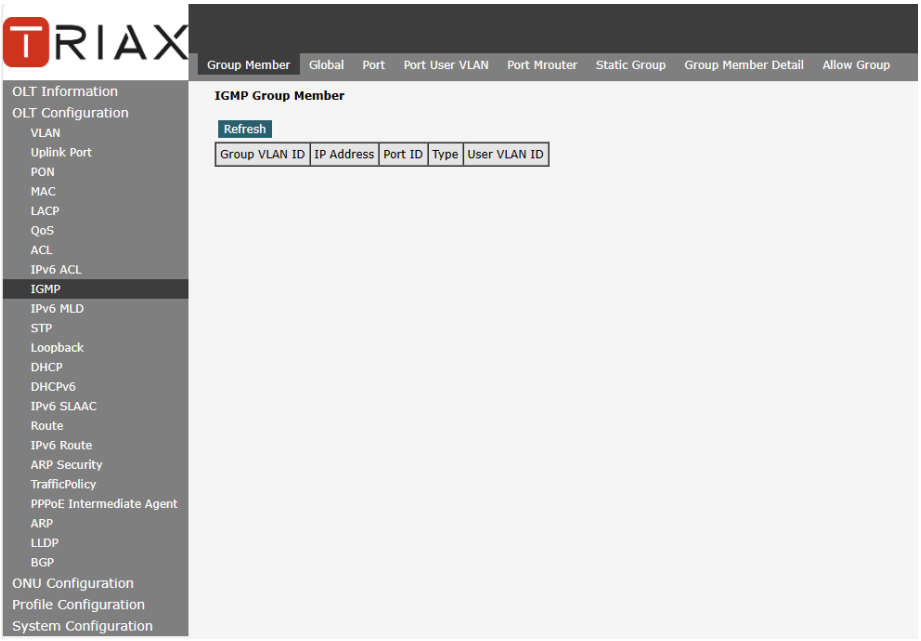


Figure 3.9-1: Group Member

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. Multicasts 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.

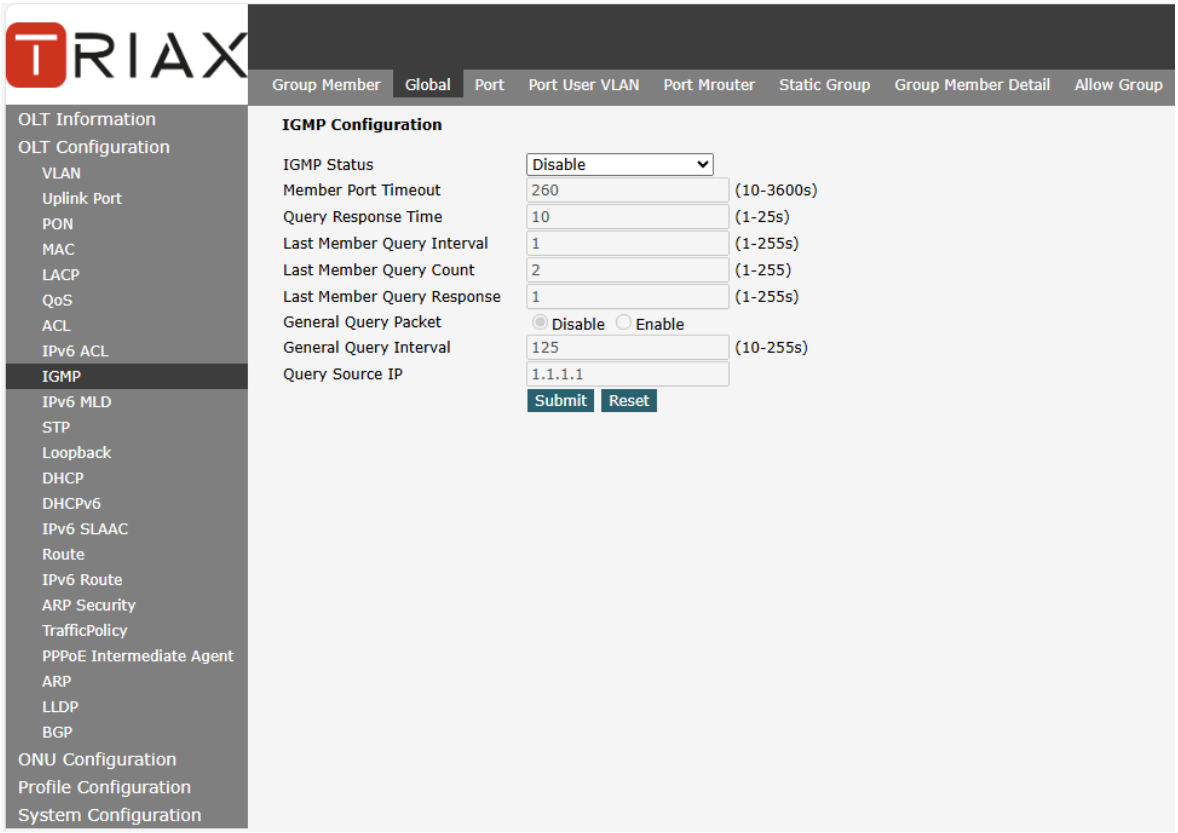


Figure 3.9-2: IGMP Global

3.9.3 Port

OLT Configuration →IGMP→Port

This configuration is used to set the maximum number of multicast groups, filter and fast leave mode.

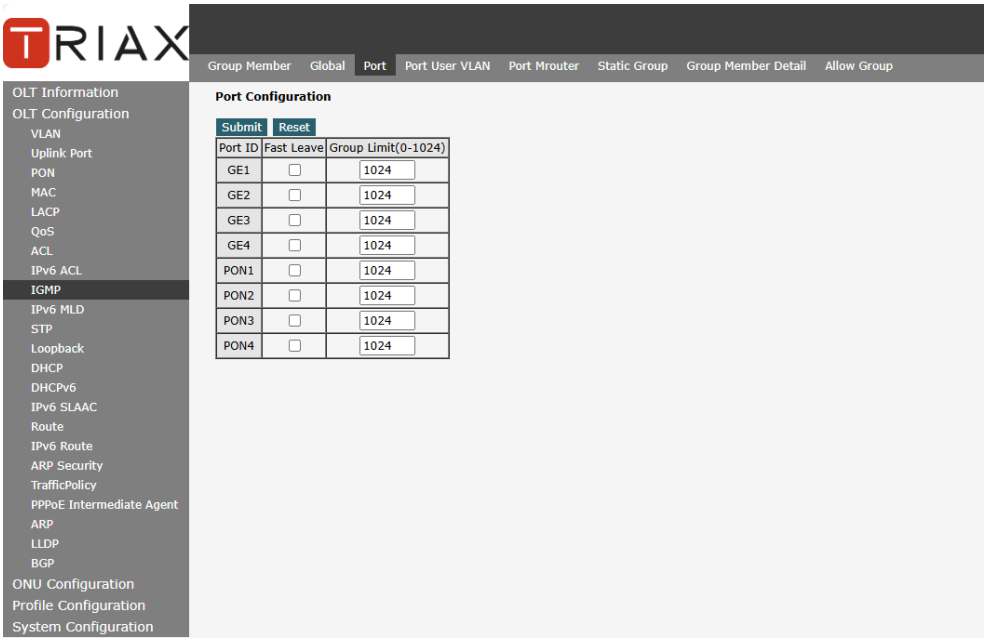


Figure 3.9-3: IGMP Port

3.9.4 Port User VLAN

OLT Configuration →IGMP→Port User VLAN

This configuration is used to configure IGMP VLAN for OLT. 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.

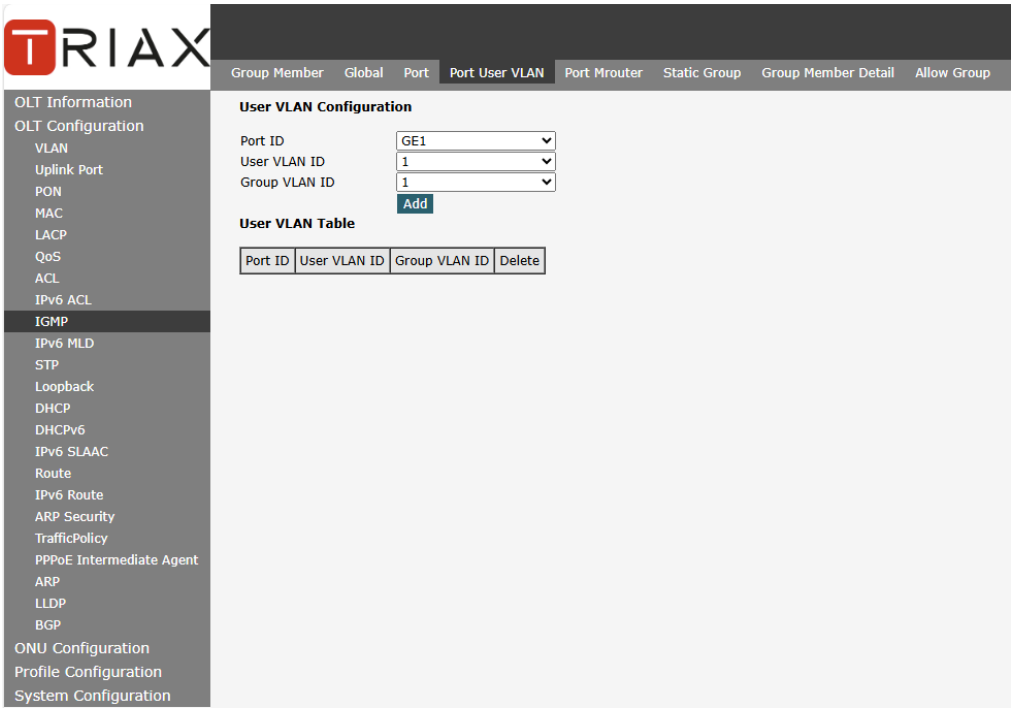


Figure 3.9-4: IGMP Port User VLAN

3.9.5 Port Mrouter

OLT Configuration →IGMP→Port Mrouter

Multicast router port is used to transmit IGMP signal messages. Generally, OLT uplink ports should be set as multicast router ports.

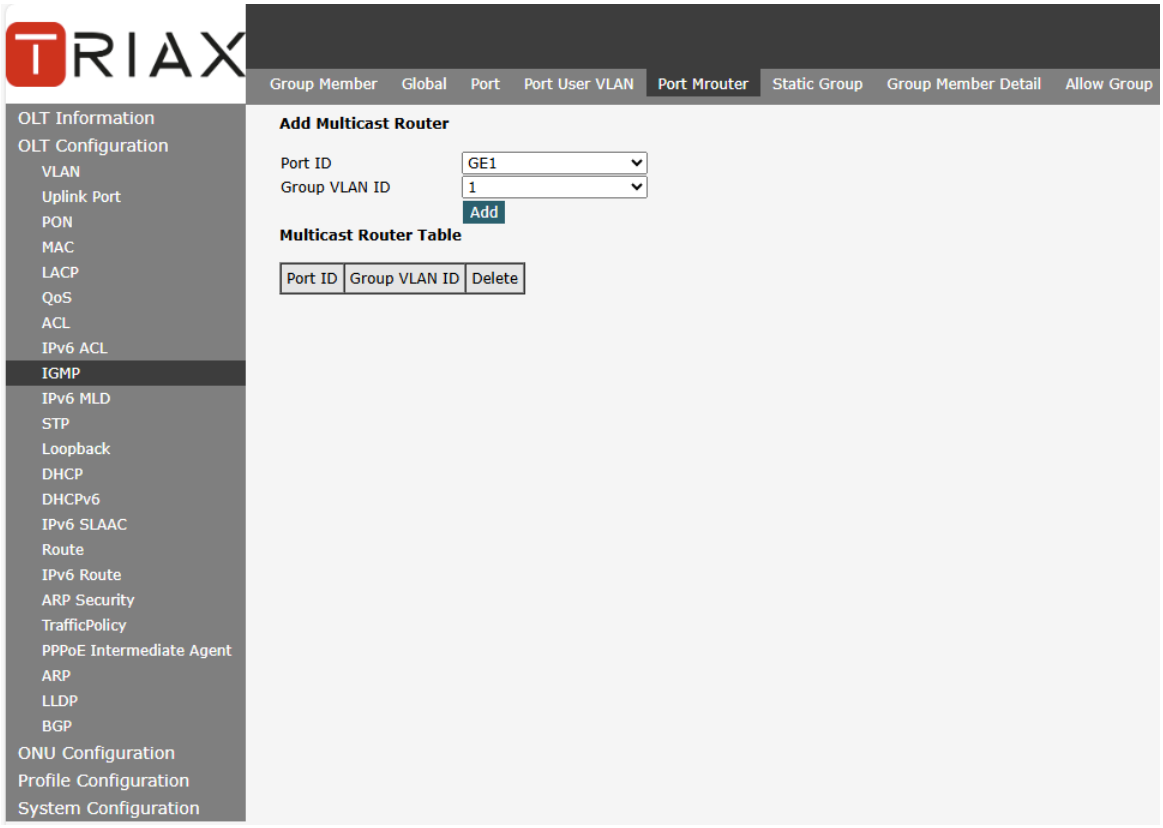


Figure 3.9-5: IGMP Port Mroute

3.9.6 Mvlan

OLT Configuration →IGMP→Mvlan

This configuration is used to configure multicast VLAN and its mode. No Mvlan configuration is required for this OLTs.

IGMP mode	Unknown multicast	Igmp packet
Snooping	drop	trap –to -cpu
Disable(transparent)	forward	forward

3.9.7 Static Group

OLT Configuration →IGMP→Static Group

This configuration is used to bind multicast IP address and VLAN ID.

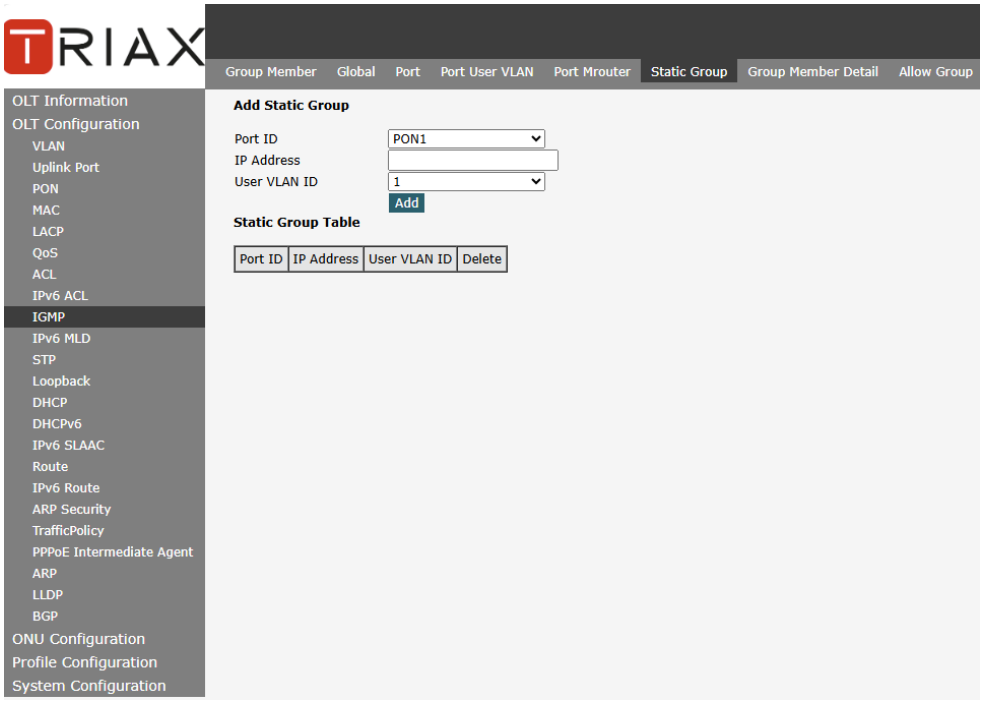


Figure 3.9-7: IGMP Static Group

3.10 IPv6 MLD

3.10.1 Group Member

OLT Configuration → IPv6 MLD → Group Member

This page displays IPv6 multicast group member ports.

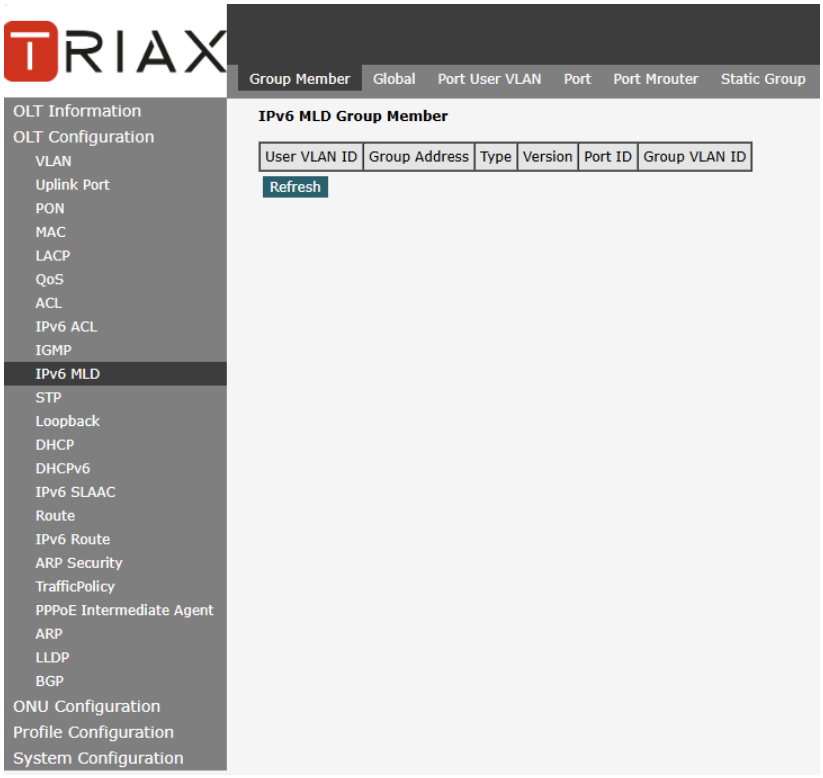


Figure 3.10-1: IPv6 MLD Group Member

3.10.2 Global

OLT Configuration → IPv6 MLD → Global

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

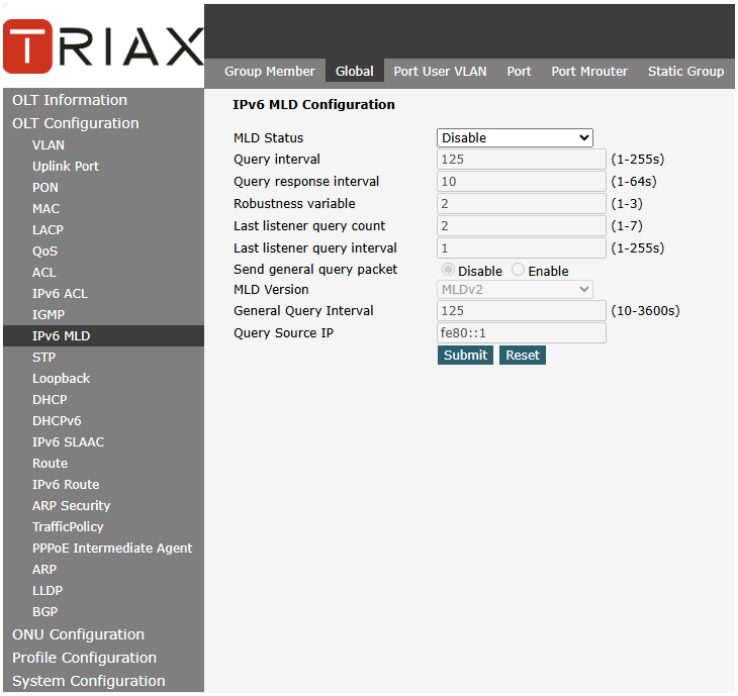


Figure 3.10-2: IPv6 MLD Global

3.10.3 Port User VLAN

OLT Configuration→IPv6 MLD→Port User VLAN

This page is used to configure IGMP VLAN for OLT.

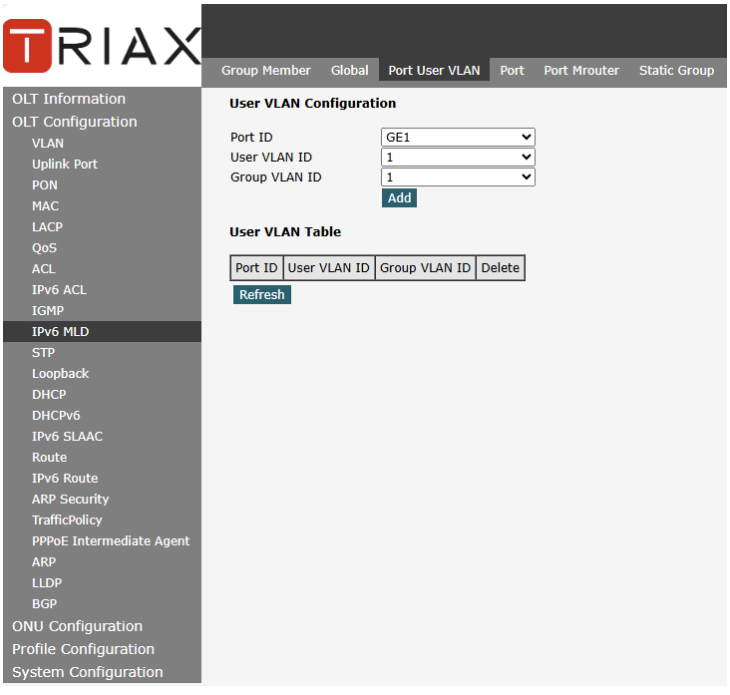


Figure 3.10-3: IPv6 Port User VLAN

3.10.4 Port

OLT Configuration → IPv6 MLD → Port

This page is used to configure group limit value, fast leave for each port.

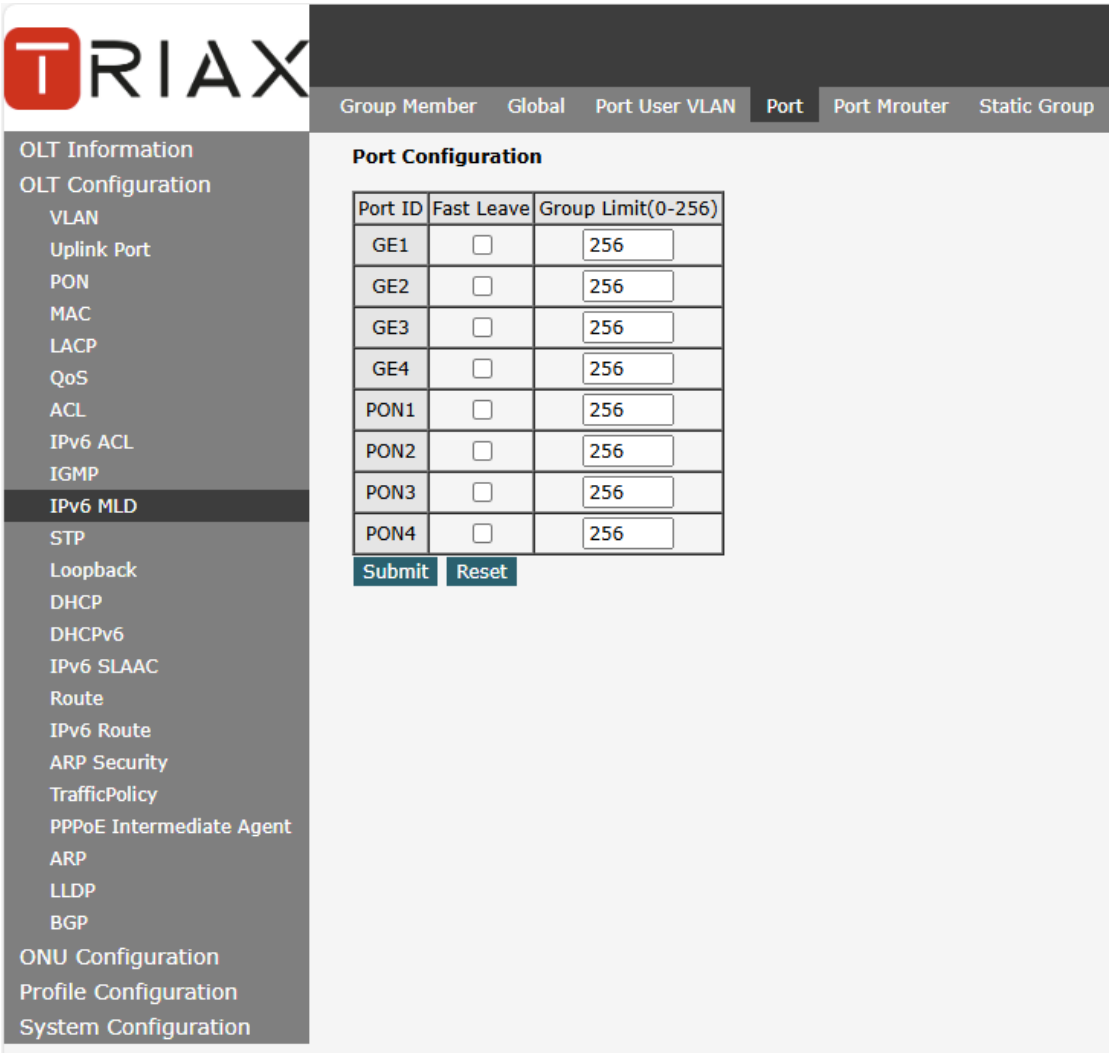


Figure 3.10-4: IPv6 MLD Port

3.10.5 Port Mrouter

OLT Configuration → IPv6 MLD → Port Mrouter

This page is used to set a port as IPv6 multicast router port.

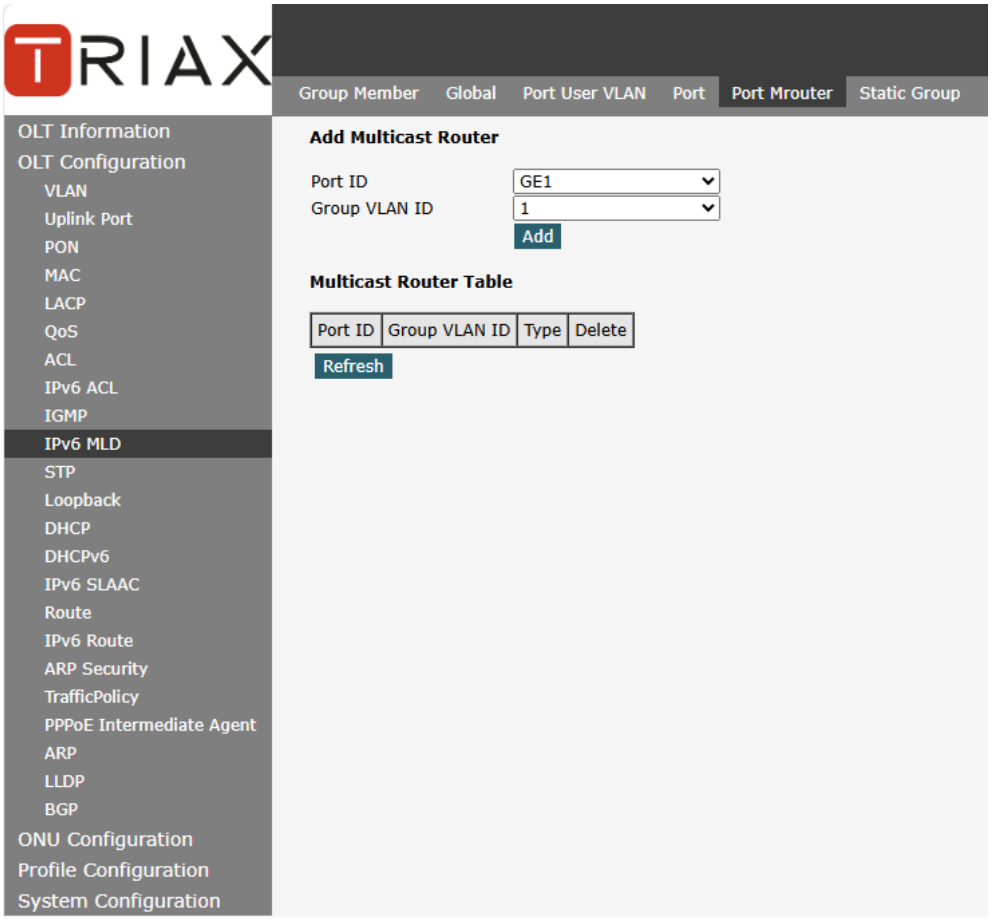


Figure 3.10-5: IPv6 MLD Port Mrouter

3.11 STP

Spanning Tree Protocol is layer2 protocol, which is used to eliminate network loop by blocking network redundant links selectively. It has the feature of link backup as well.

3.11.1 RSTP Information

OLT Configuration→STP→RSTP→Information

Global information mainly displays RSTP parameters of root bridge device.

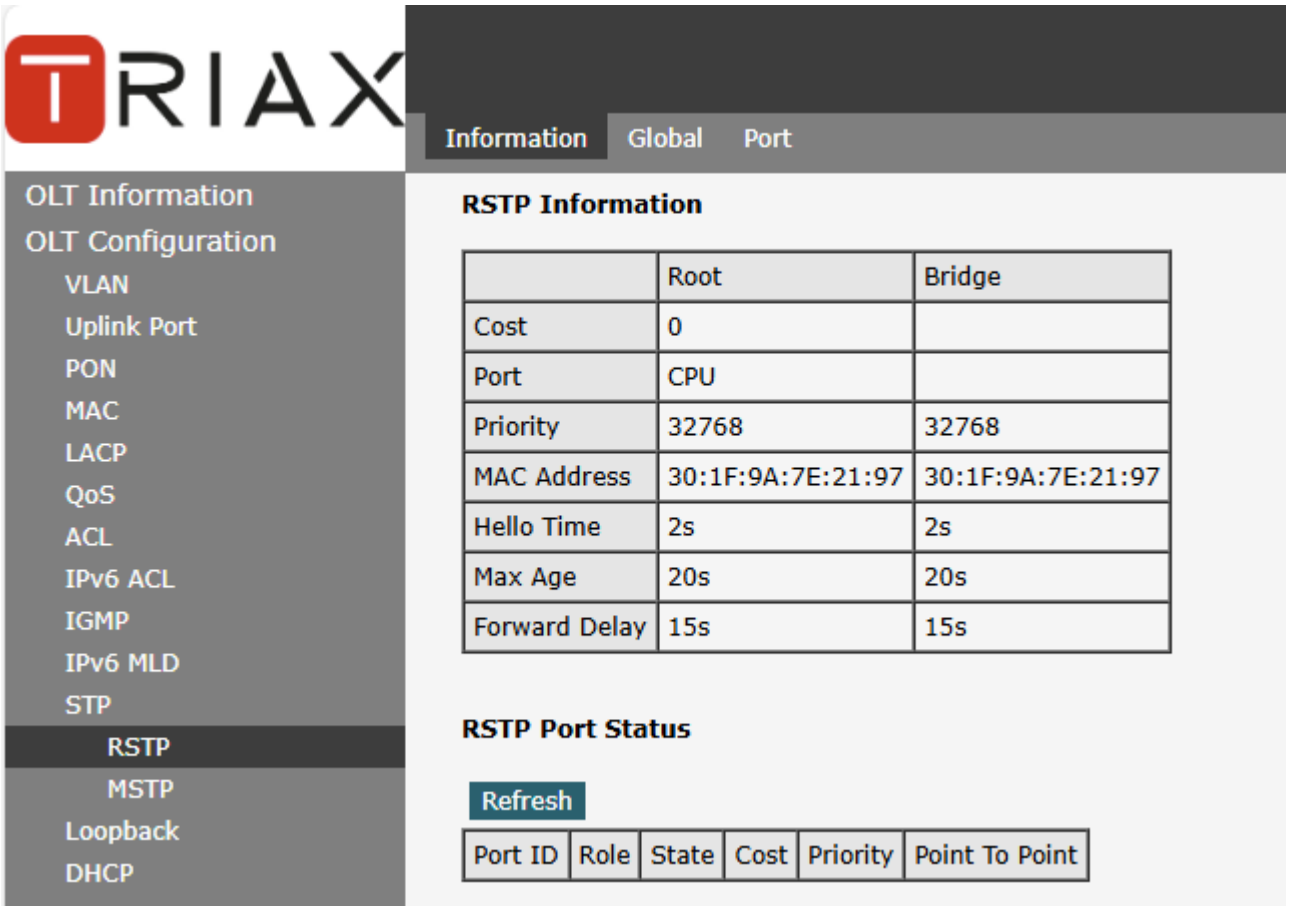


Figure 3.11-1: RSTP Information

3.11.2 Global

OLT Configuration→STP→RSTP →Global

This configuration is used to set RSTP parameters of the device, which contains RSTP switch, priority, hello time, max age, forward delay and MAC address.

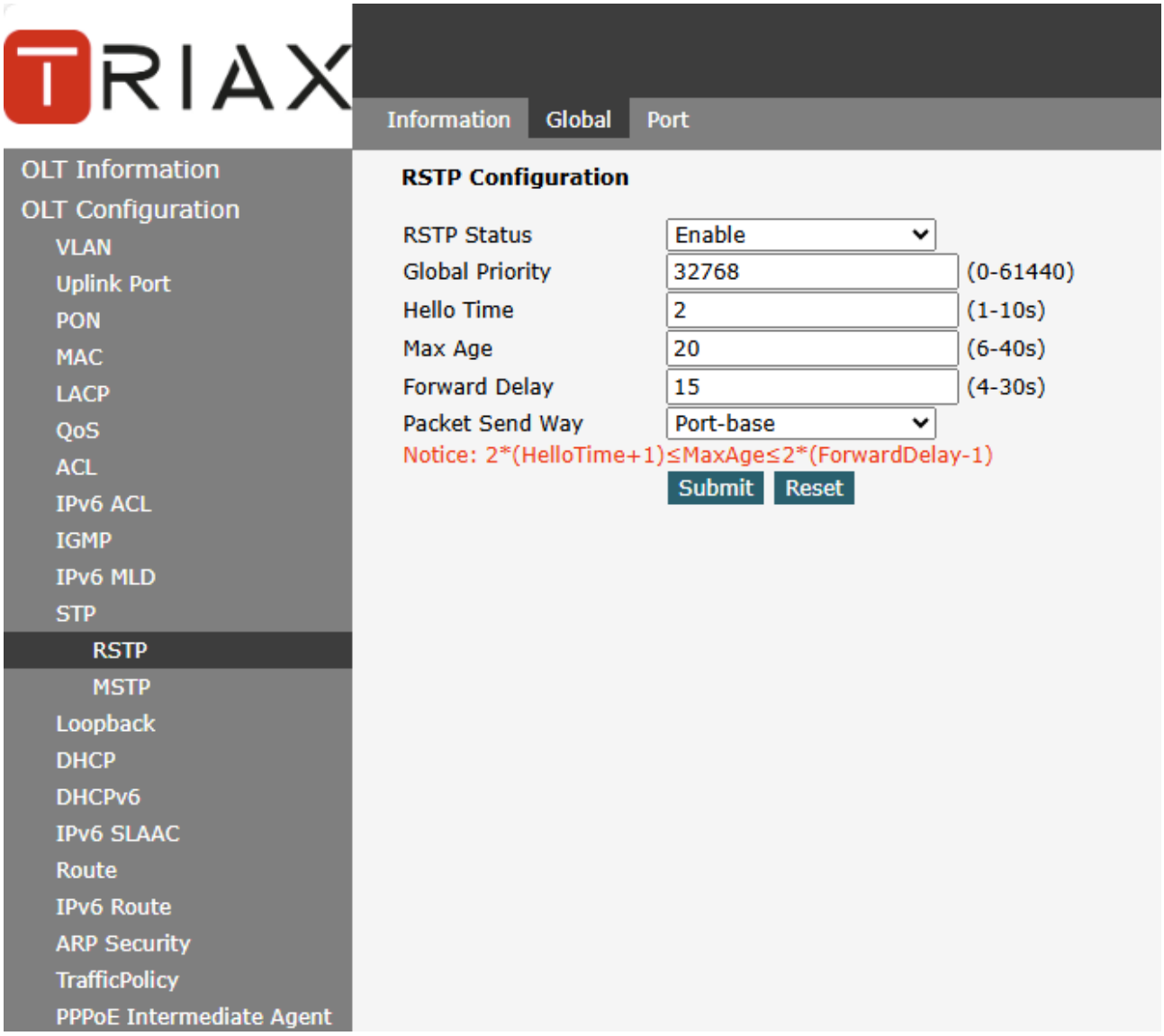


Figure 3.11-2: RSTP Global Setup

3.11.3 Port

OLT Configuration→STP→RSTP →Port

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

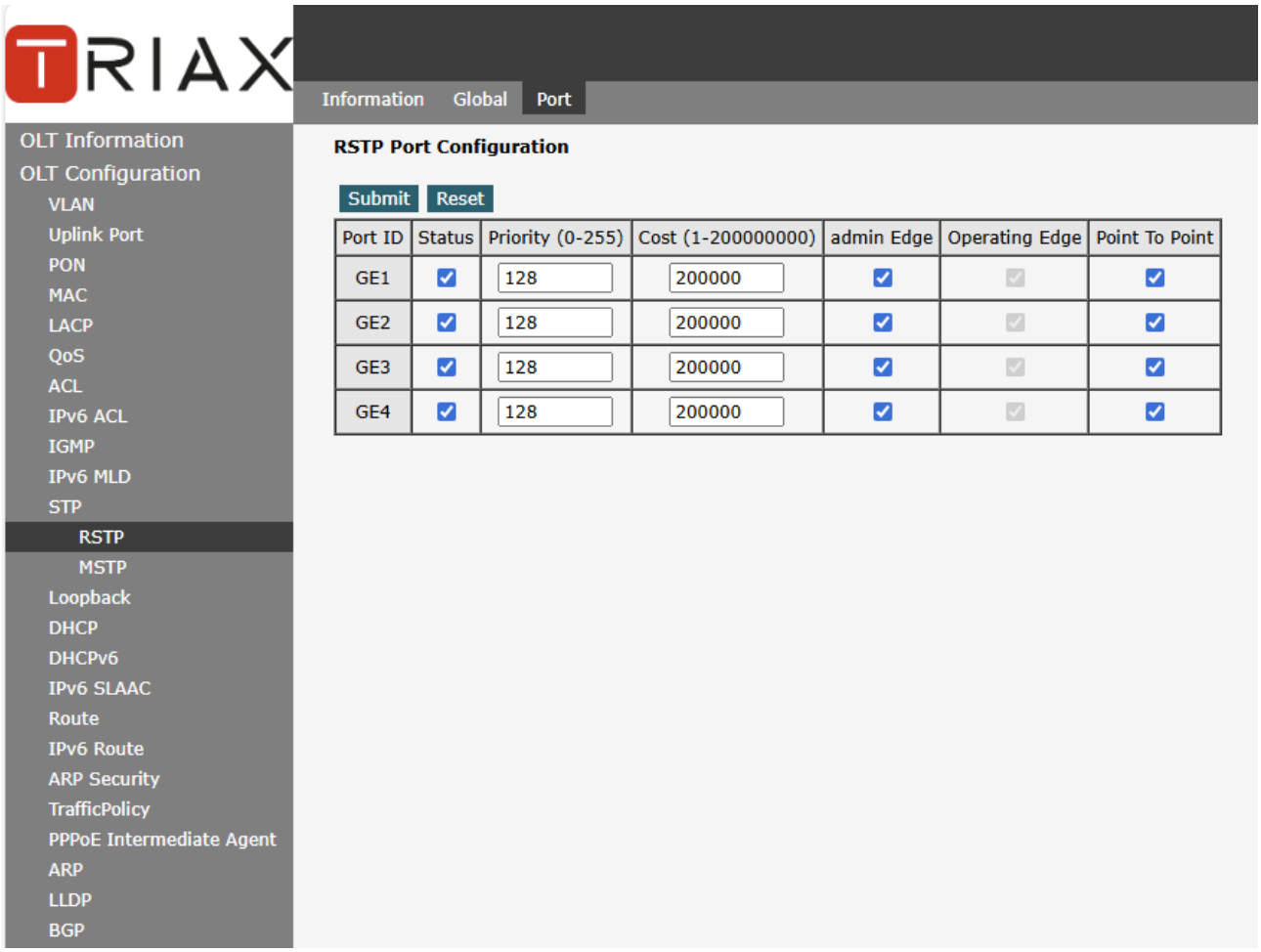


Figure 3.11-3: RSTP Port Settings

3.11.4 MSTP Information

OLT Configuration→STP→MSTP→Information

Global information mainly displays MSTP parameters of root bridge device.

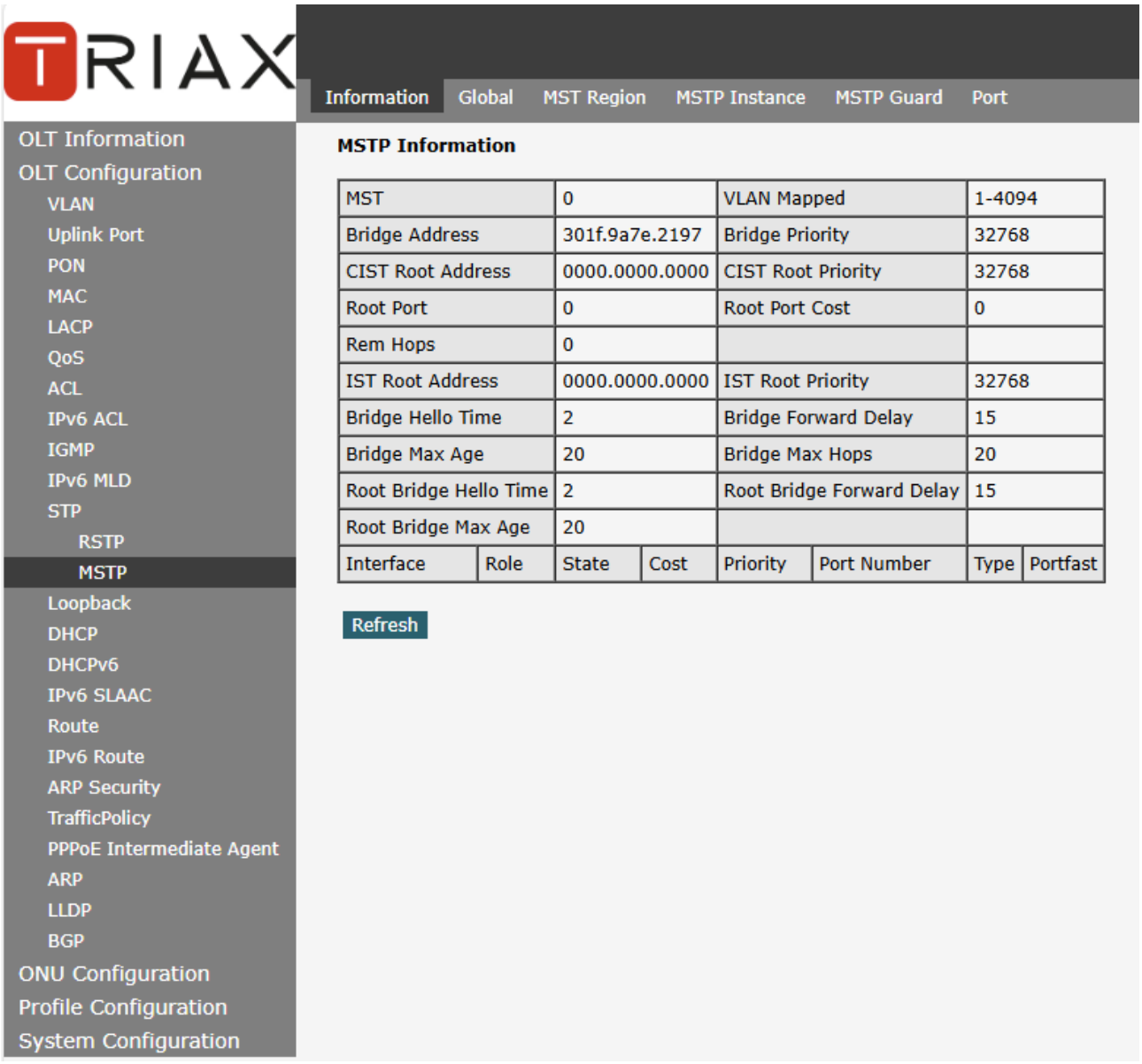


Figure 3.11-4: MSTP Information

3.11.5 MSTP Global

OLT Configuration→STP→MSTP →Global

This configuration is used to set MSTP parameters of the device, which contains MSTP switch, priority, hello time, max age, forward delay and MAC address.

Figure 3.11-5: MSTP Global Setup

3.11.6 Port

OLT Configuration→STP→MSTP →Port

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

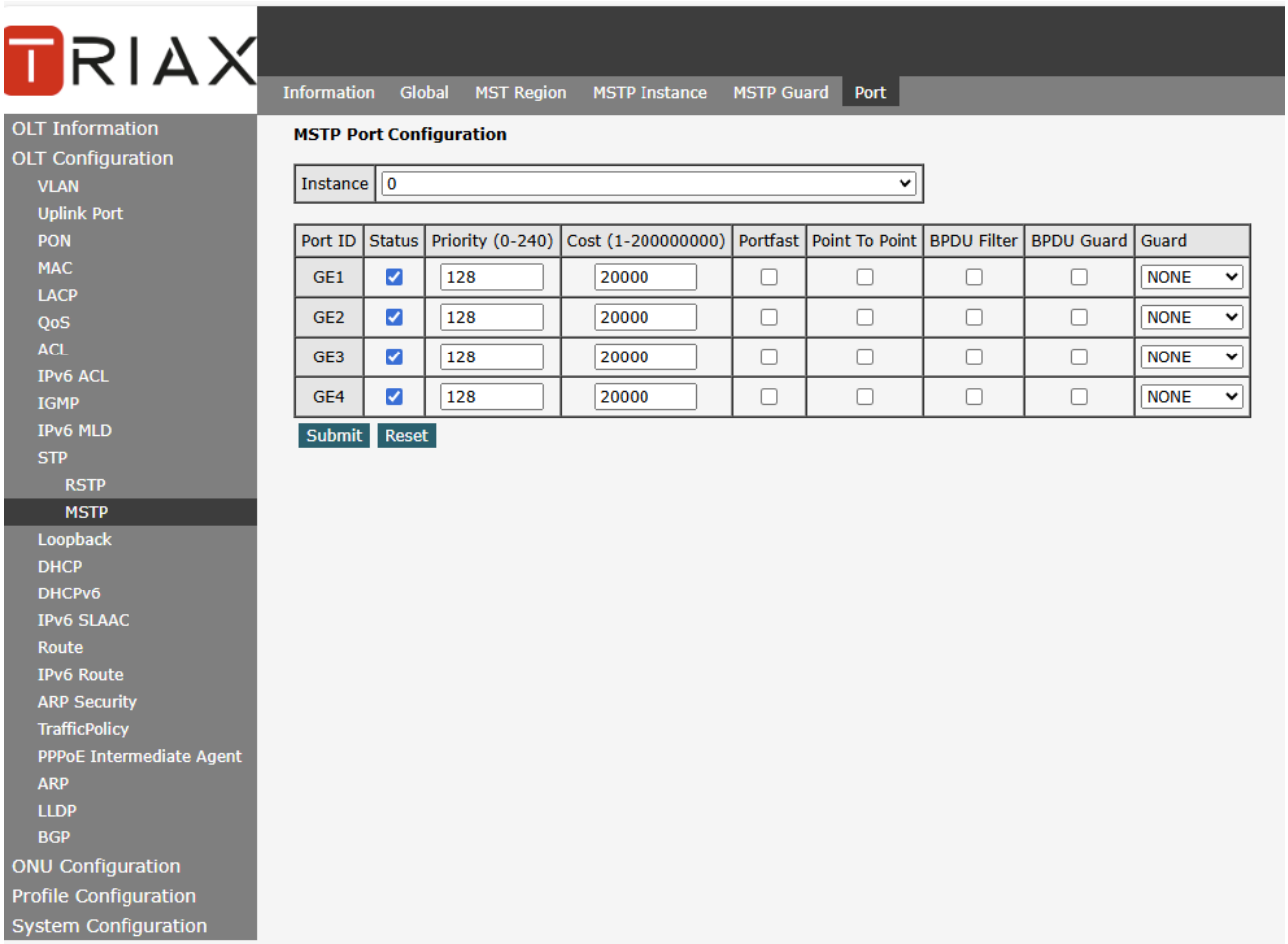


Figure 3.11-6: MSTP Port Settings

3.12 Loopback

Loopback can detect loop ports and process loop ports.

3.12.1 Information

OLT Configuration→Loopback→Information

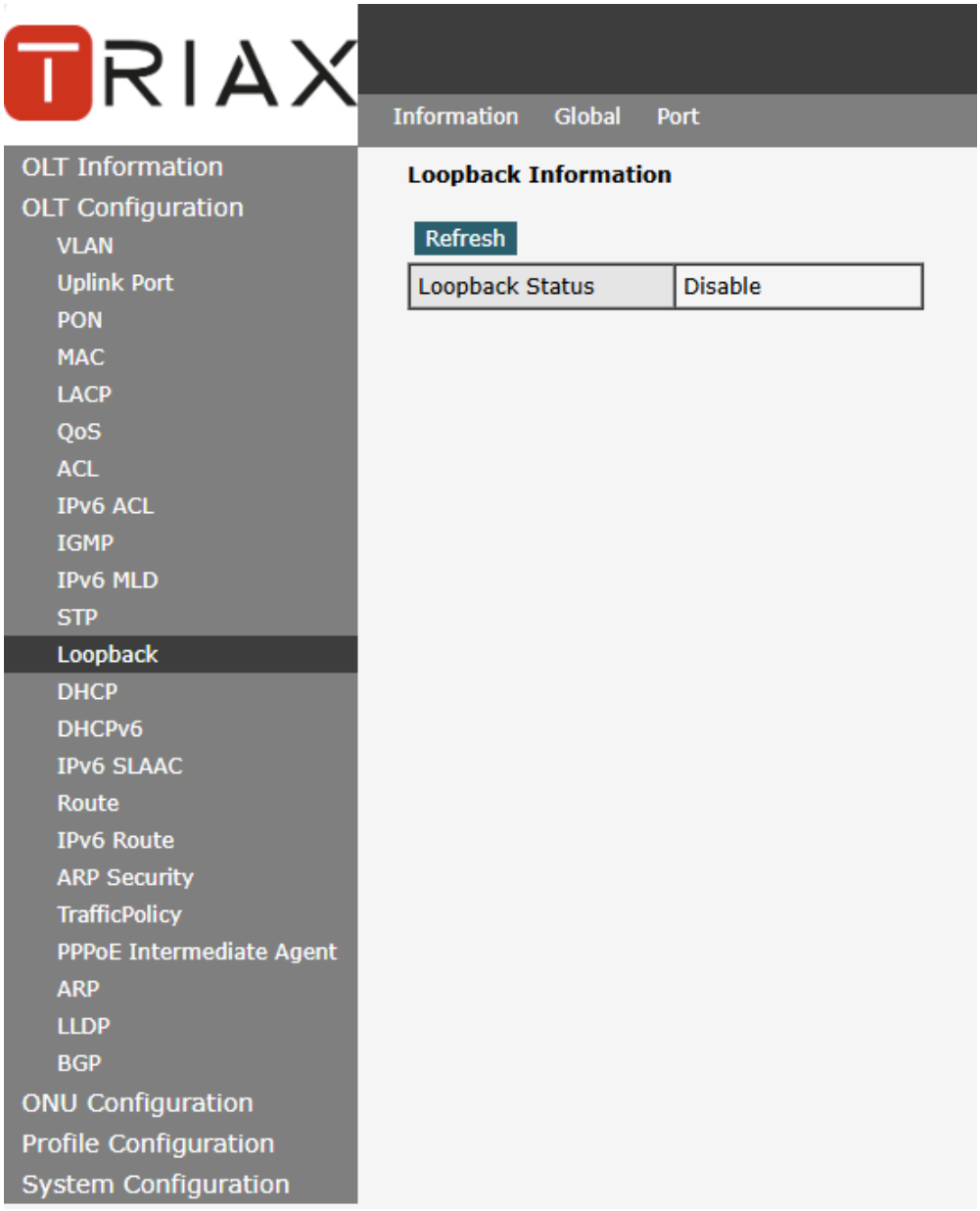


Figure 3.12-1: Loopback Information

3.12.2 Global

OLT Configuration→Loopback→Global

This page is used to enable or disable loopback detect and configure loopback mode, age time.

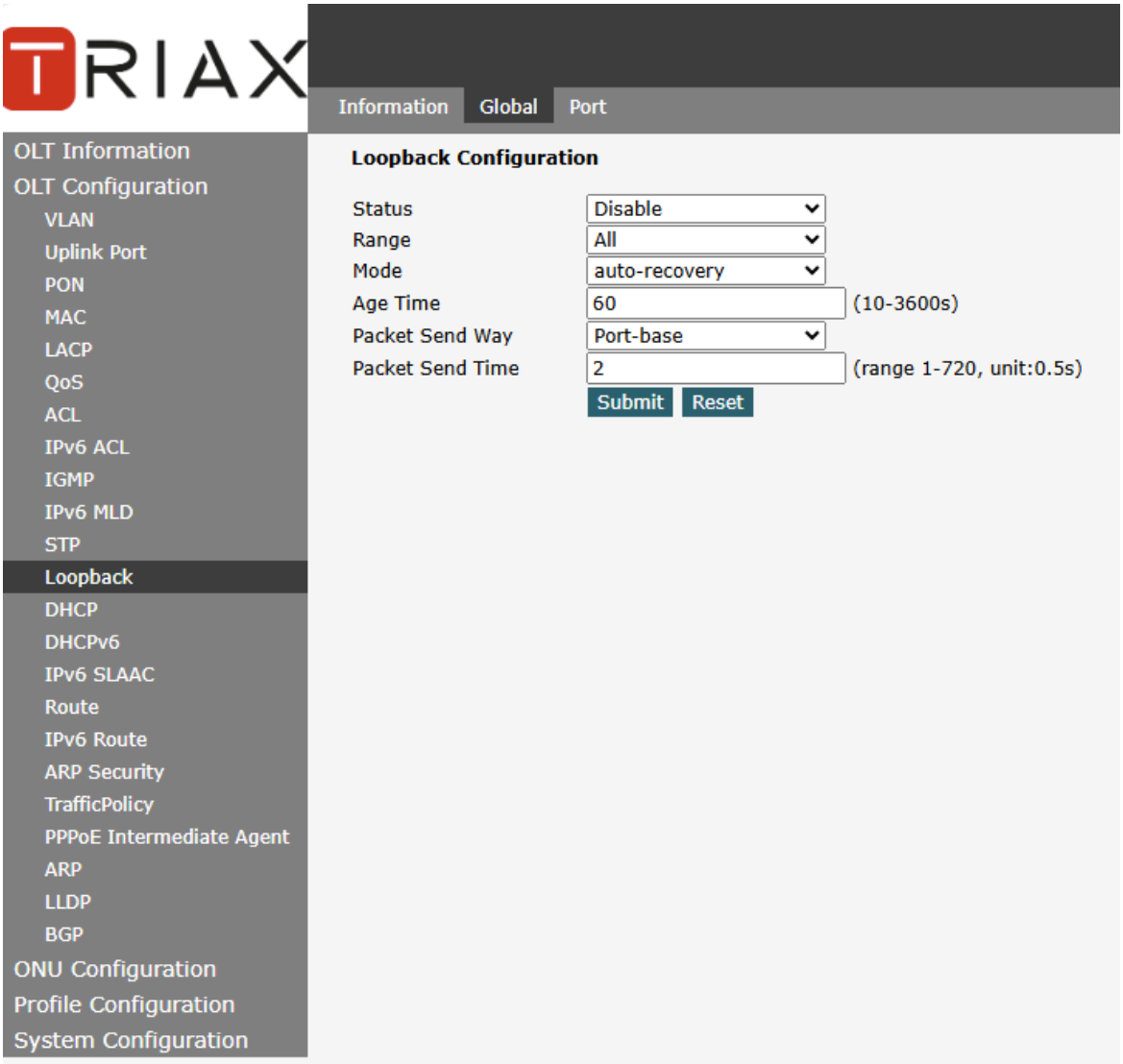


Figure 3.12-2: Loopback Global

3.12.3 Port

OLT Configuration→Loopback→Port

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

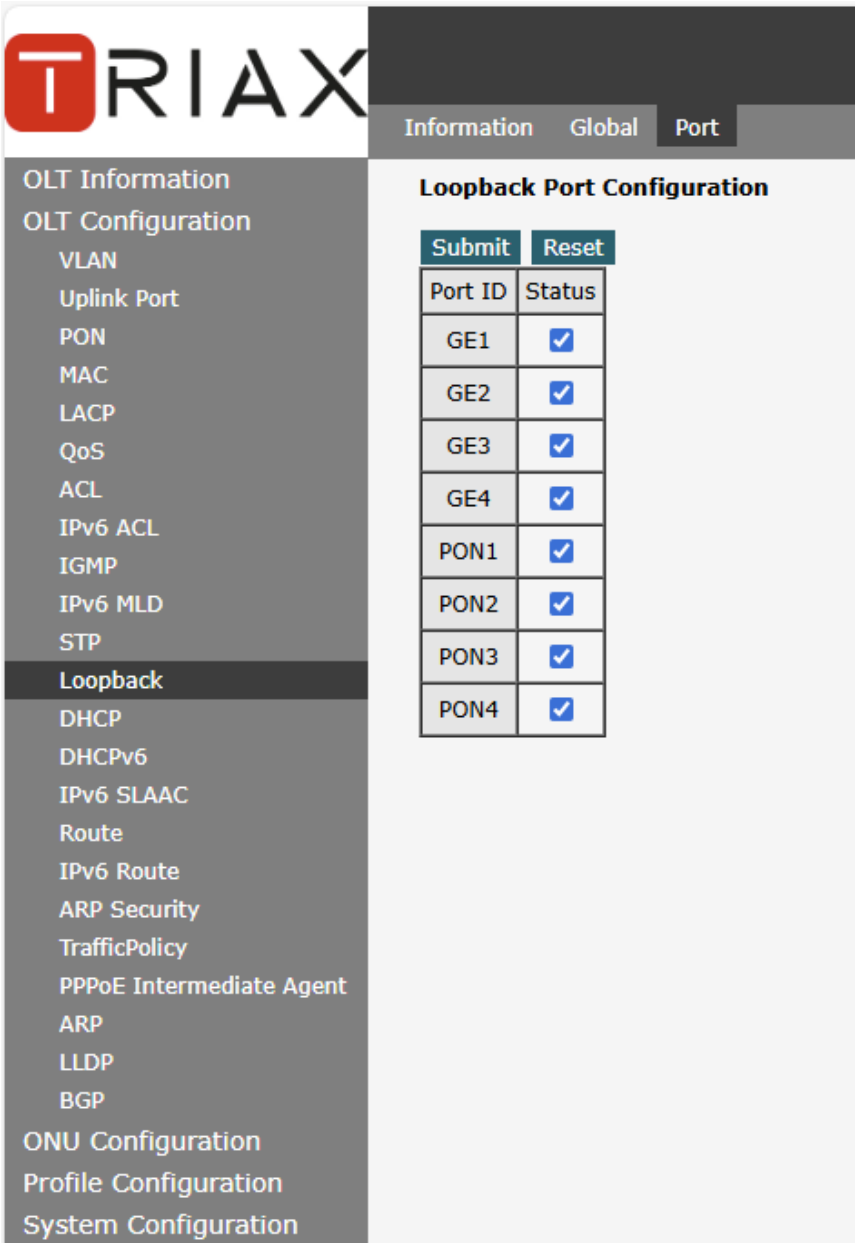


Figure 3.12-3: Loopback Port

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.

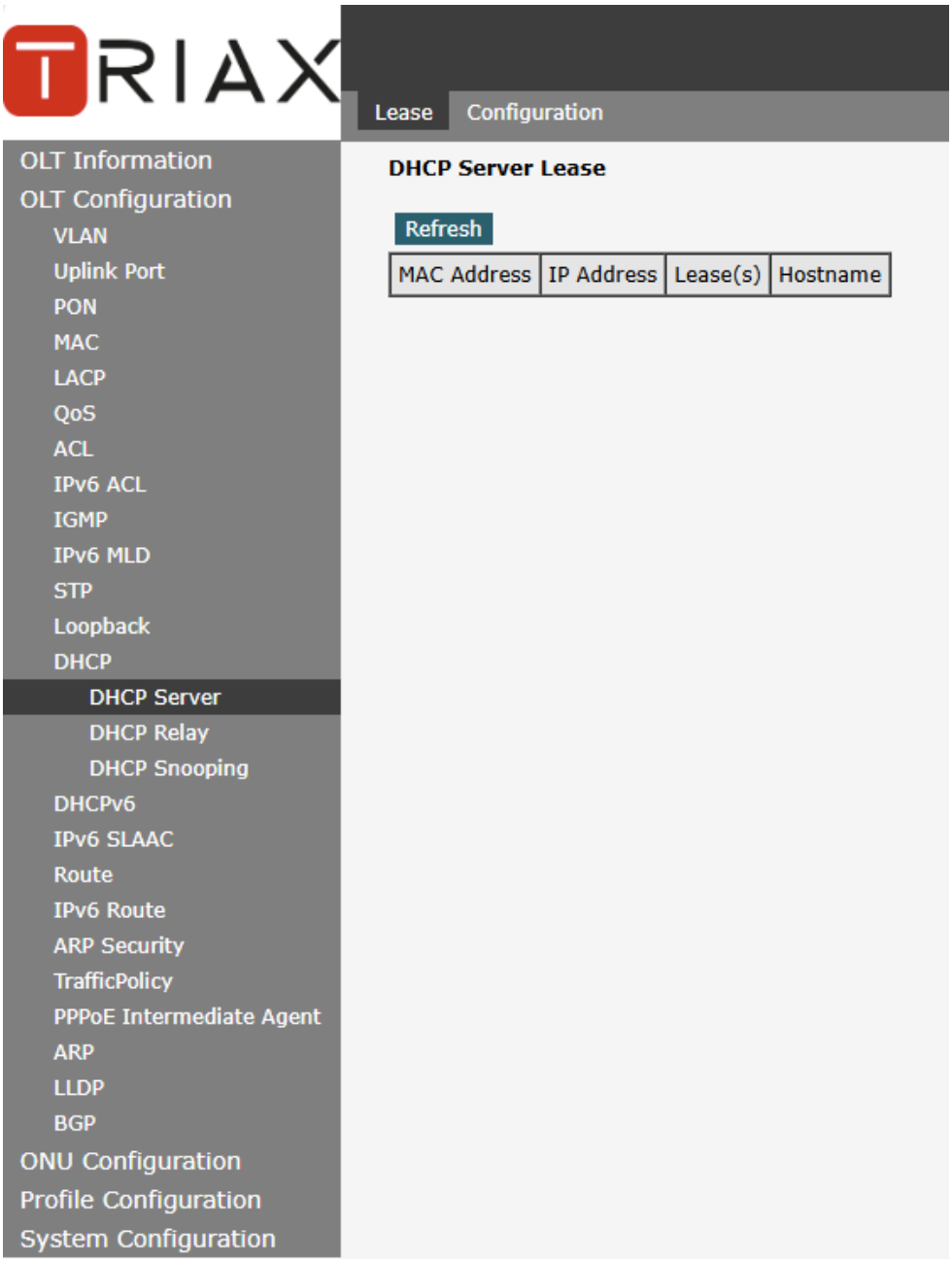


Figure 3.13-1: DHCP Lease

3.13.1.2 DHCP Configuration

OLT Configuration→DHCP→DHCP Server→Configuration

Sometimes the devices need dynamic IP addresses, but there is no special DHCP server in network. These configurations can solve the problem. OLT will be a DHCP server in network and assign IP addresses to other devices.

Before enabling DHCP server, you must configure IP address for the VLAN.

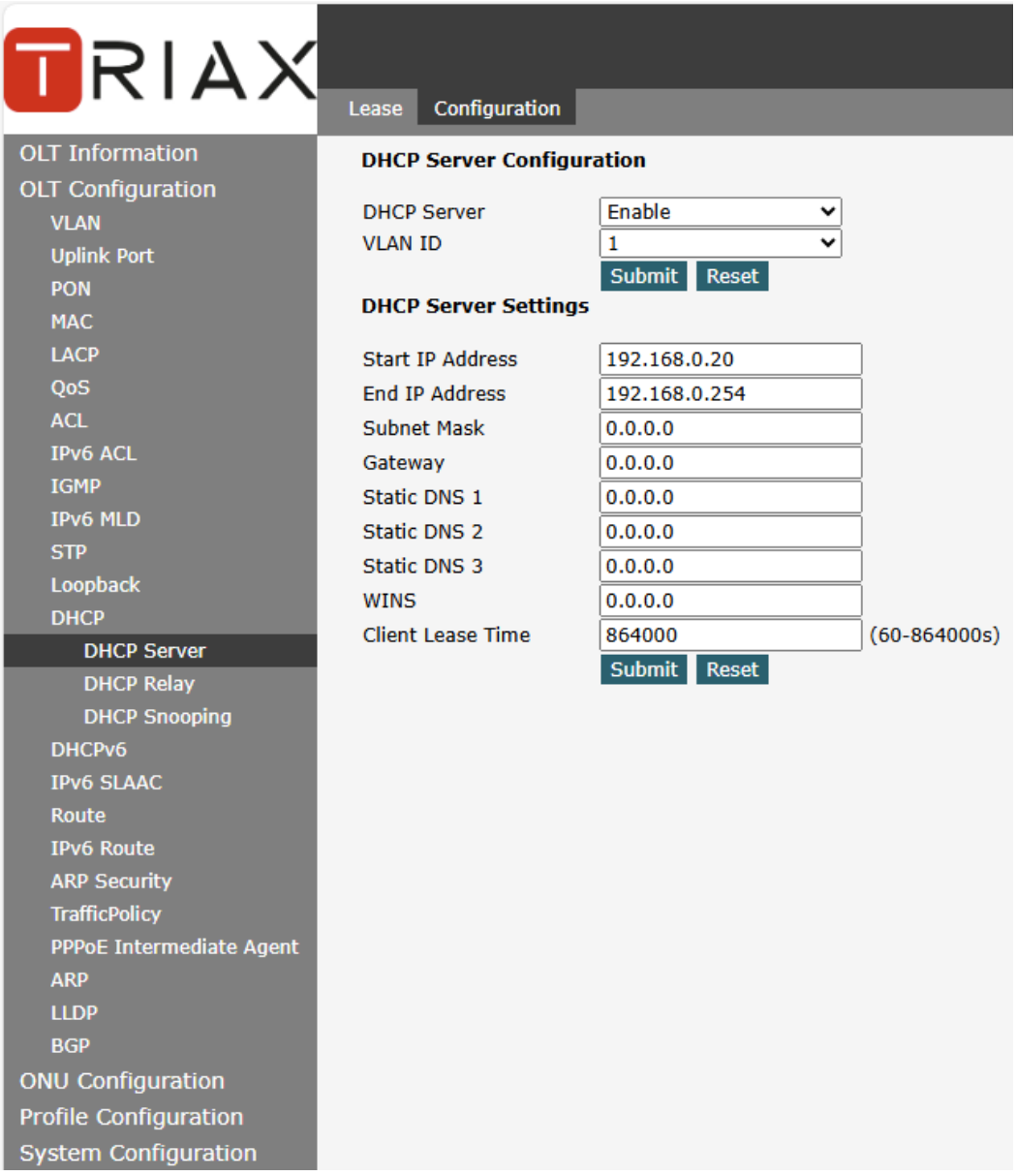


Figure 3.13-2: DHCP Configuration

3.13.2 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.

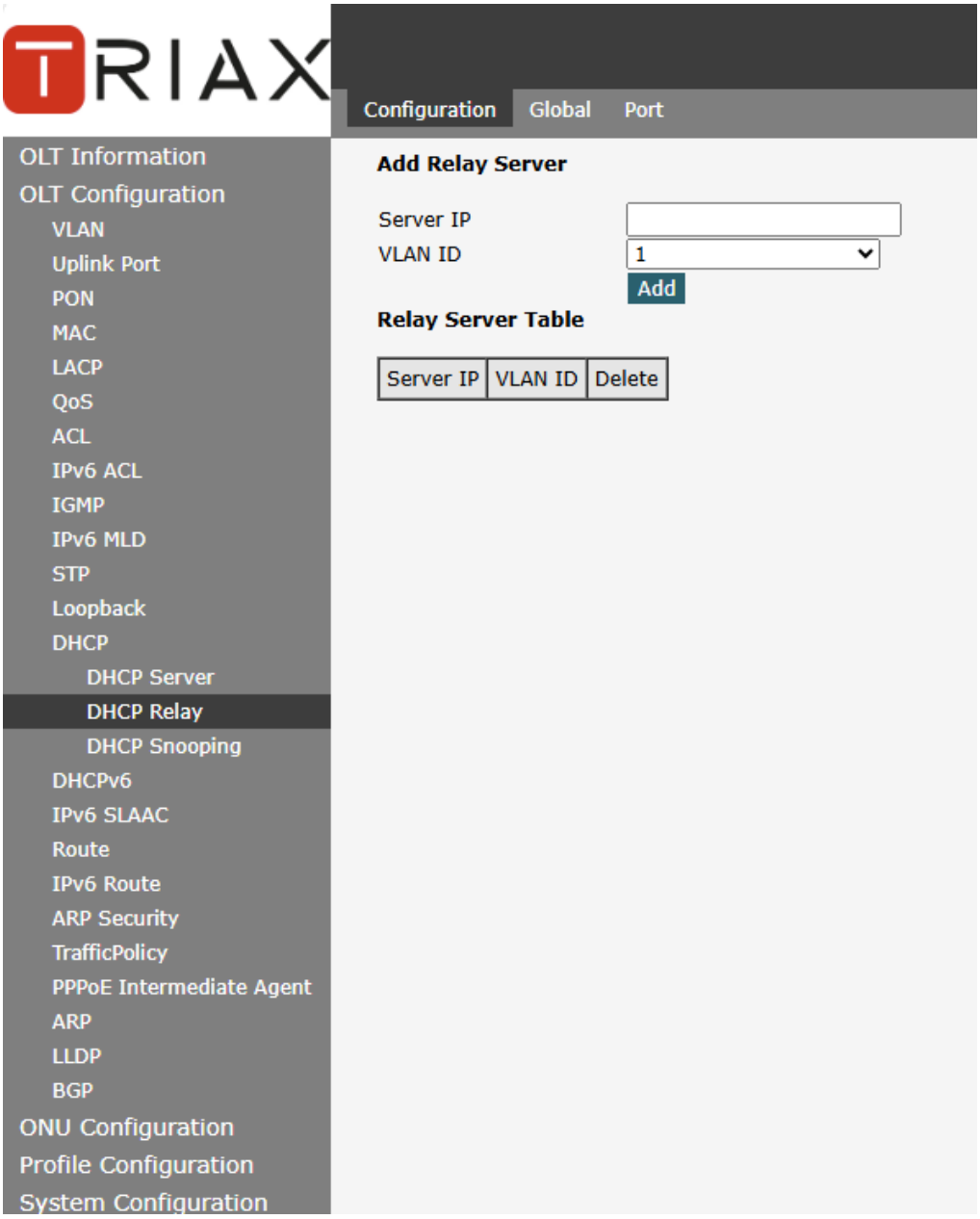


Figure 3.13-3: DHCP Relay Configuration

3.13.3 DHCP Snooping

3.13.3.1 Bind List

OLT Configuration→DHCP→DHCP Snooping→Bind List

The static bind of the DHCP Snooping will be shown in the table.

Figure 3.13-4: DHCP Snooping Bind List

3.13.3.2 Global

OLT Configuration→DHCP→DHCP Snooping→Global

DHCP Snooping is used to prevent the DHCP message attacking and guarantee network to get a correct IP address.

DHCP snooping global configuration mainly contains option 82 settings, DHCP traffic rate limit and snooping VLAN.

Figure 3.13-5: 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.

All the ports are untrust ports by default. 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.

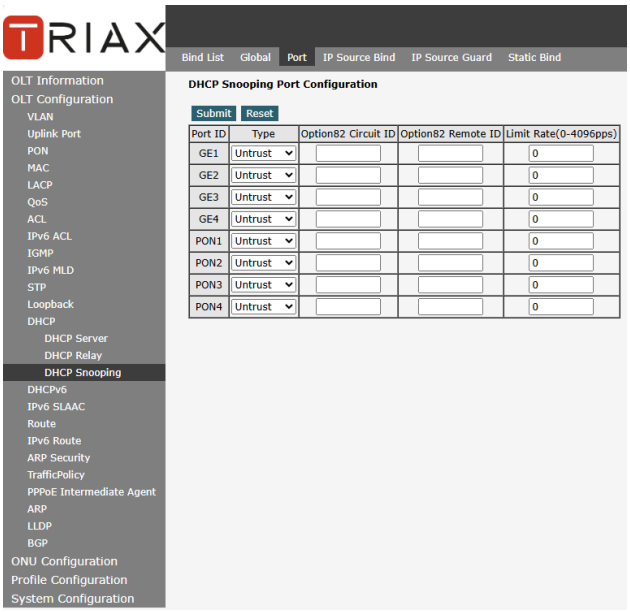


Figure 3.13-6: DHCP Snooping Port Setup

3.13.3.4 Static Bind

OLT Configuration→DHCP→DHCP Snooping→Static Bind

DHCP snooping binding is useful when a host needs a fixed IP address assigned by DHCP server from the specific port.

Figure 3.13-7: DHCP Snooping Static Bind

3.13.3.5 IP Source Guard

Only GPON OLT-B Series supports this feature.

OLT Configuration→DHCP→DHCP Snooping→IP Source Guard

This function is 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

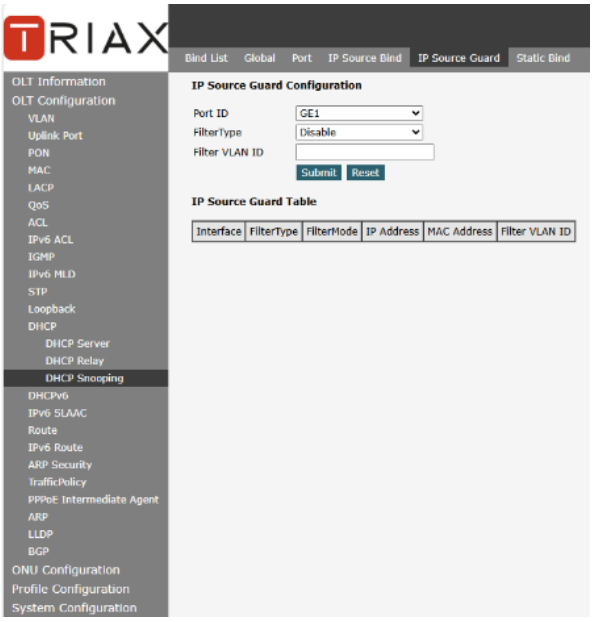


Figure 3.13-8: DHCP Snooping IP Source Guard

3.13.3.6 IP Source Bind

Only GPON OLT-B Series supports this feature.

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 page. It works as described in the previous section.

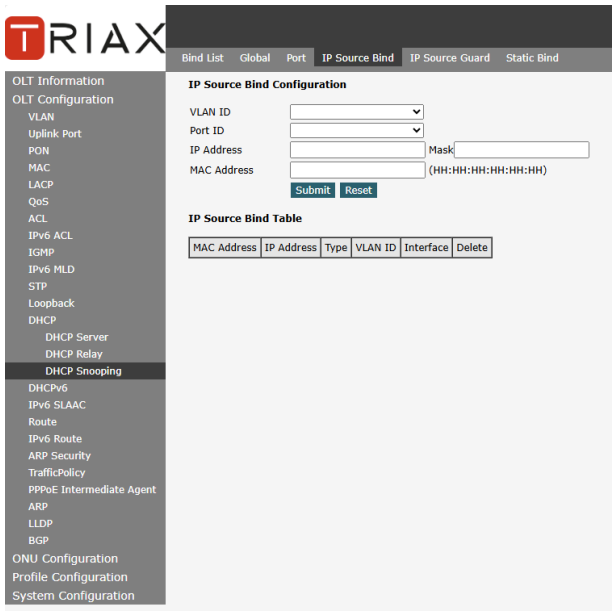


Figure 3.13-9: DHCP Snooping IP Source Bind

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.

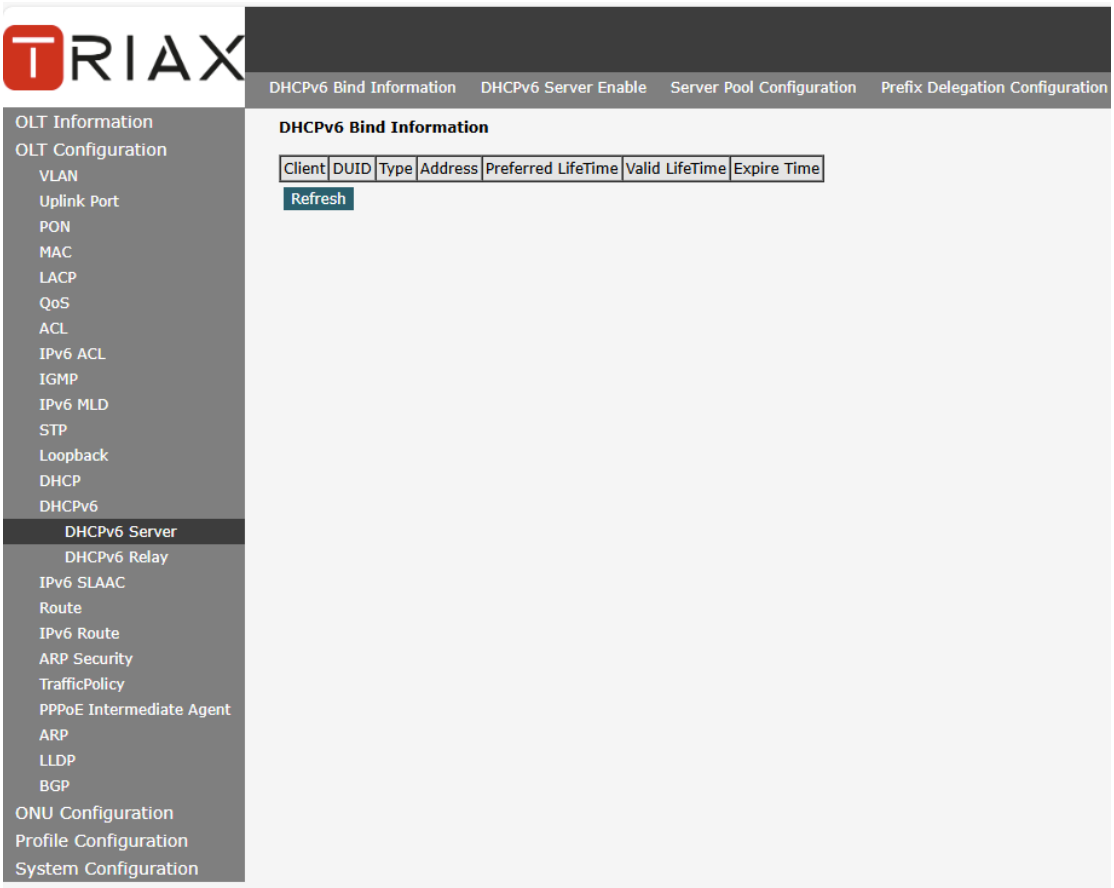


Figure 3.14-1: DHCPv6 Bind Information

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.

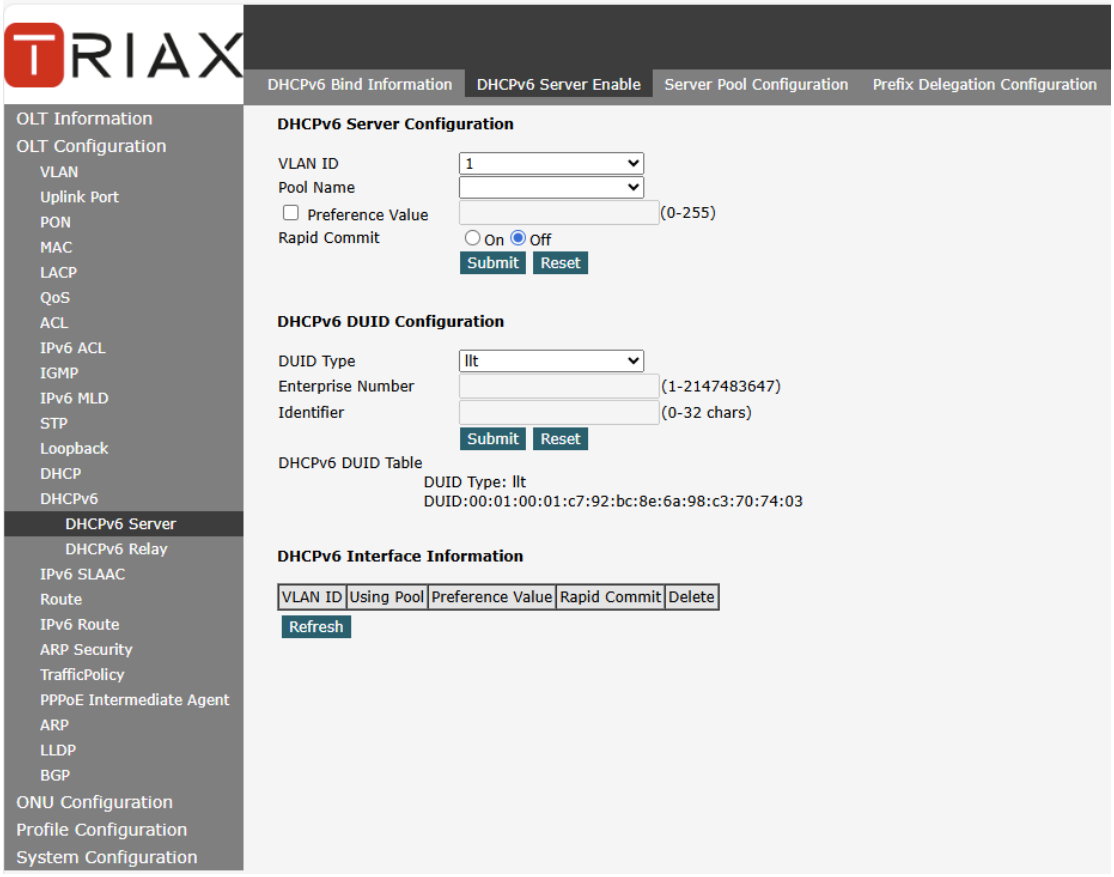


Figure 3.14-2: DHCPv6 Server

3.14.1.3 Server Pool Configuration

OLT Configuration → DHCPv6 → DHCPv6 Server → Server Pool Configuration

DHCPv6 pool specifies the range of assigned IPv6 address. Lifetime, DNS and domain also can be specified here for DHCPv6 client.

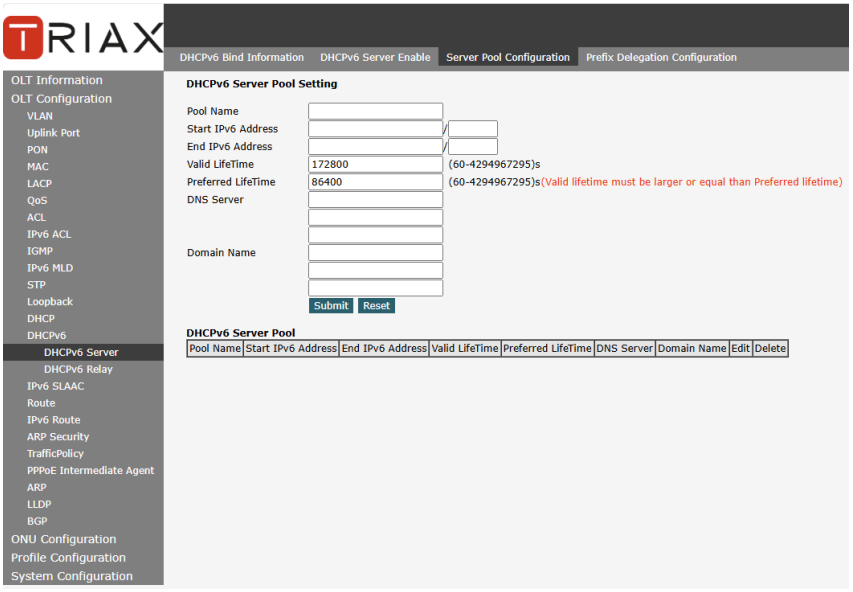


Figure 3.14-3: DHCPv6 Pool

3.14.2 DHCPv6 Relay

OLT Configuration → DHCPv6 → DHCPv6 Relay → Configuration

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

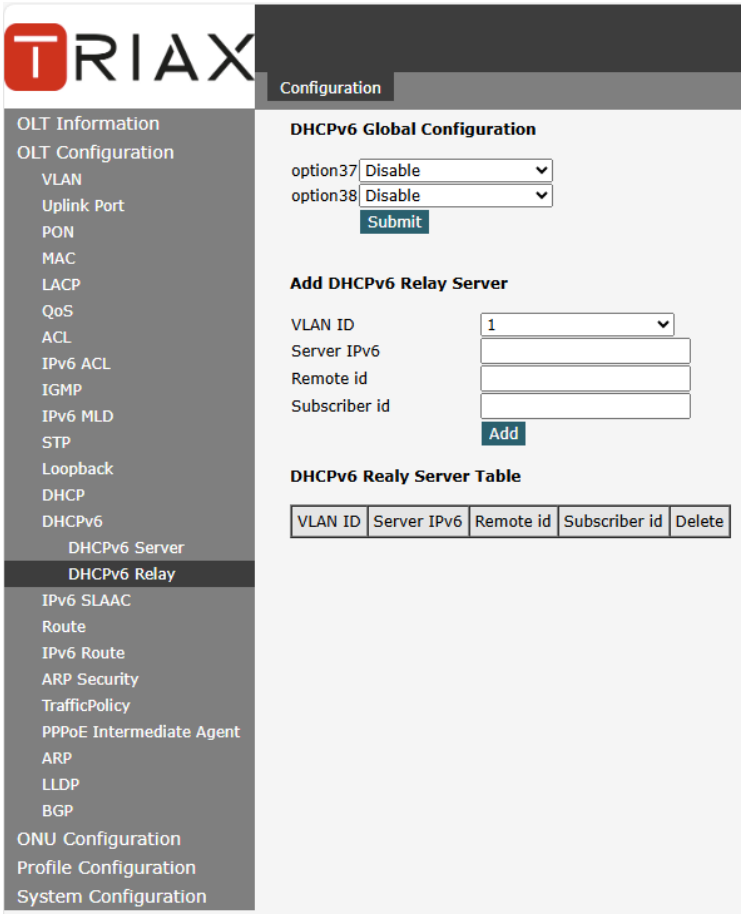


Figure 3.14-4: DHCPv6 Relay

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 neighbour 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 AutoConfiguration), OLT will send a route advertisement (RA) packet to it. This page is used to configure parameters of the route advertisement packet.

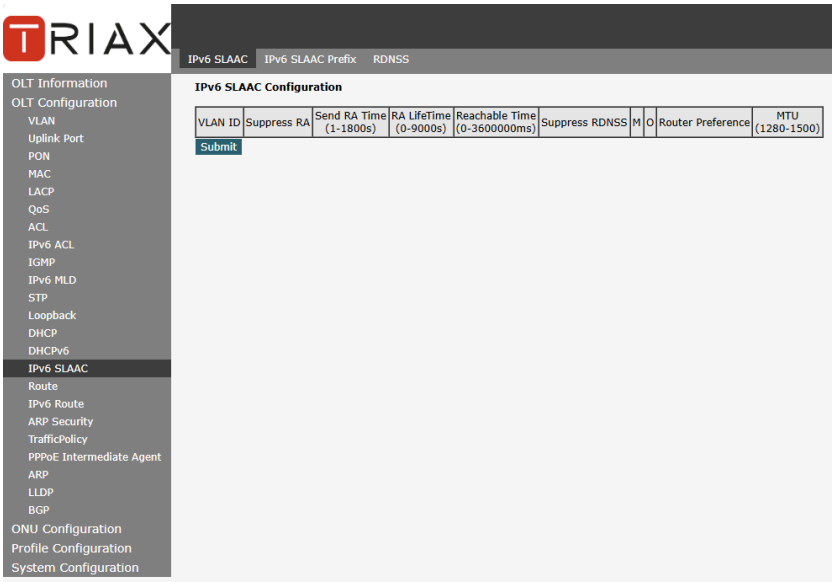


Figure 3.15-1: IPv6 SLAAC

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.

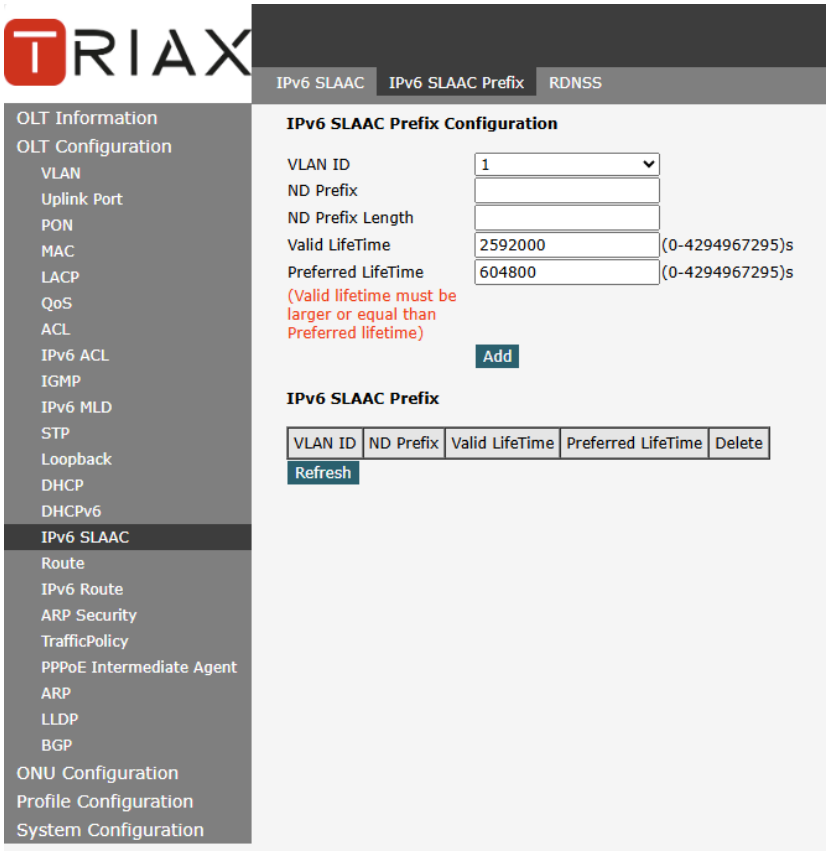


Figure 3.15-2: IPv6 SLAAC Prefix

3.15.3 RDNSS

OLT Configuration → IPv6 SLAAC → RDNSS

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

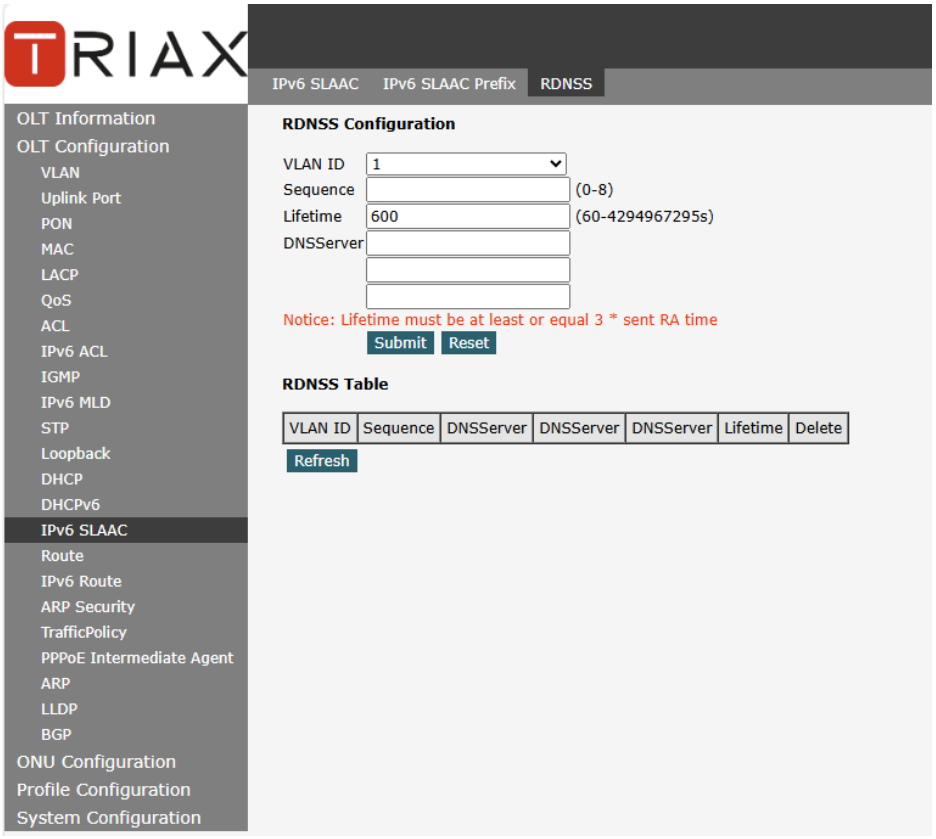


Figure 3.15-3: RDNSS

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.

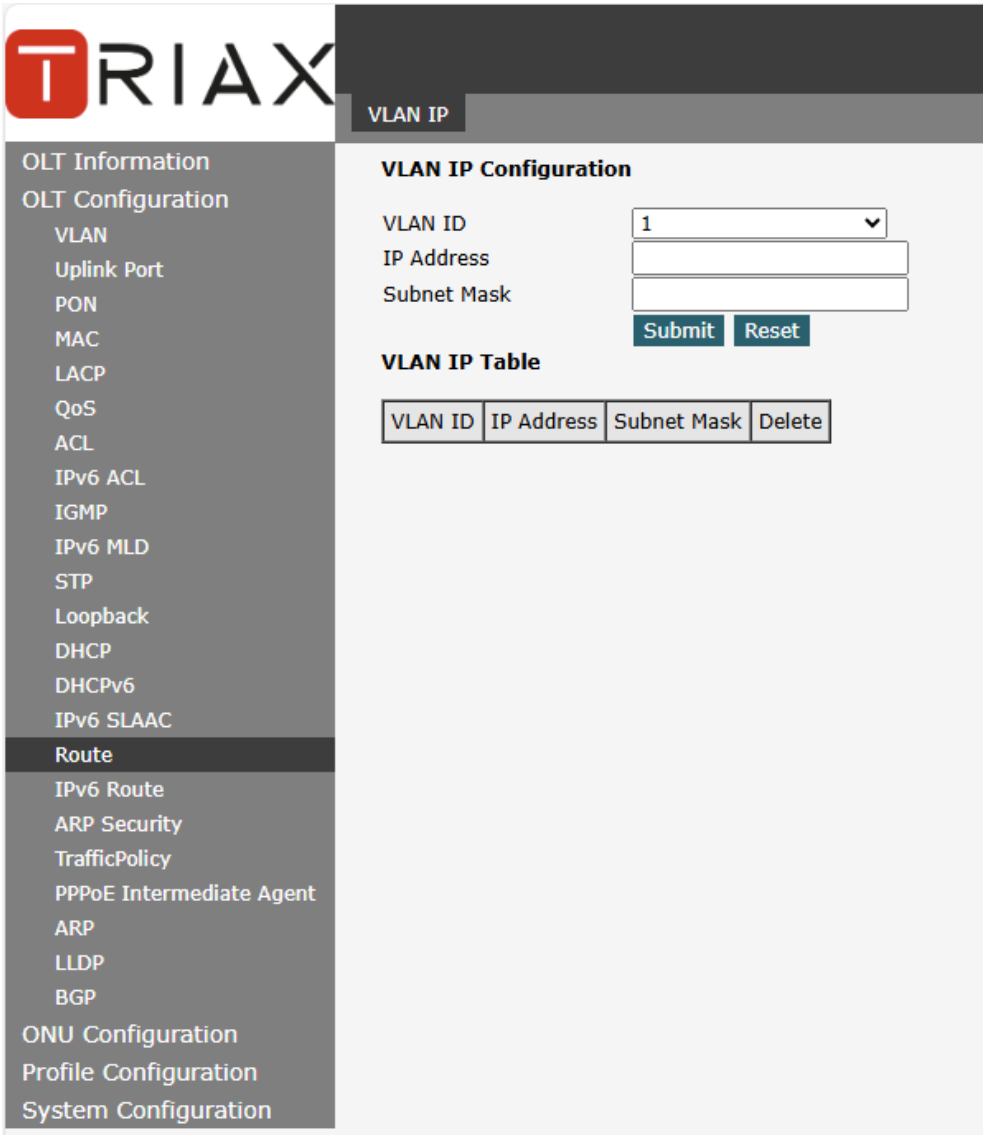


Figure 3.16-1: VLAN IP

3.16.1.2 ARP Proxy

ARP Proxy is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The ARP Proxy is aware of the location of the traffic's destination and offers its own MAC address as (ostensibly final) destination. The "captured" traffic is then typically routed by the Proxy to the intended destination via another interface or via a tunnel.

The process which results in the node responding with its own MAC address to an ARP request for a different IP address for proxying purposes is sometimes referred to as 'publishing'. This OLT does not support ARP Proxy.

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.

The OLT only supports static route. After configured VLAN IP address, add static routes to make the network on the different network segment communicate with each other.

OLT Configuration→Route→Static Route

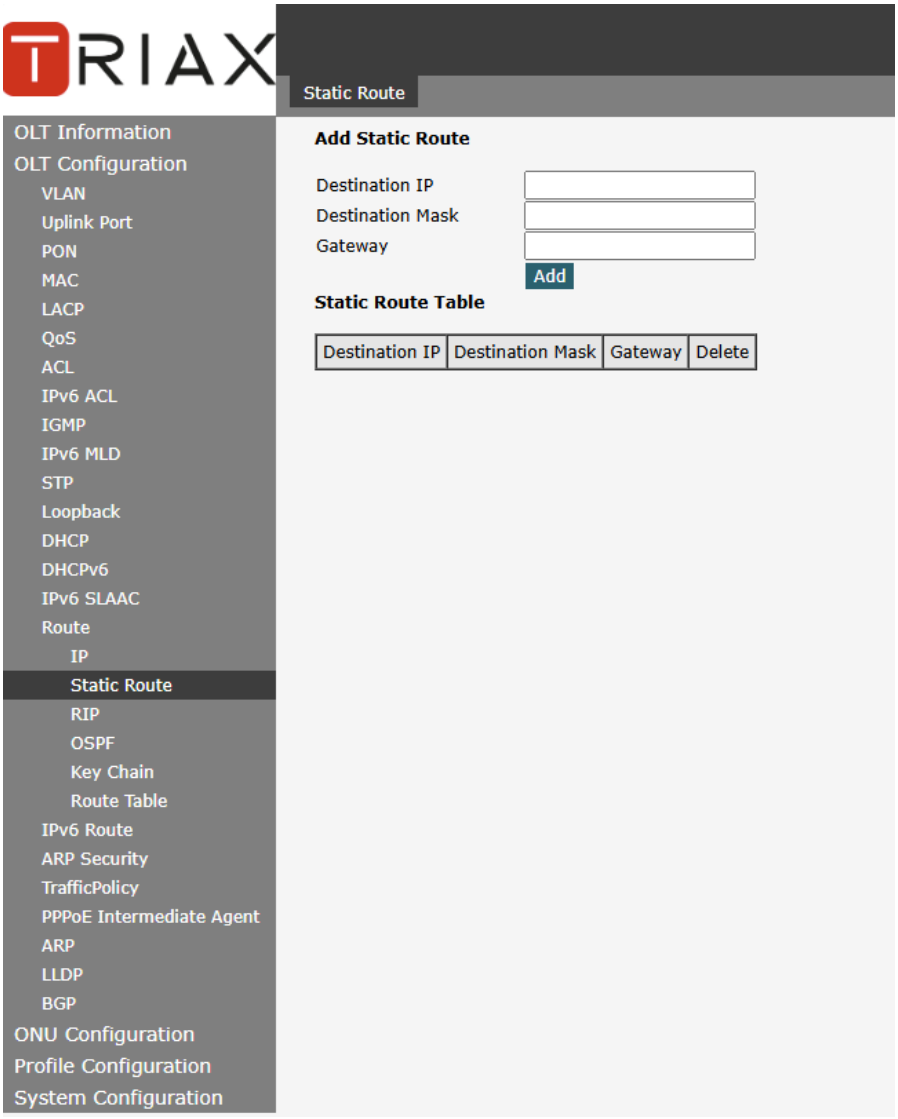


Figure 3.16-3: Static Route

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 datagram 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 page displays RIP information.

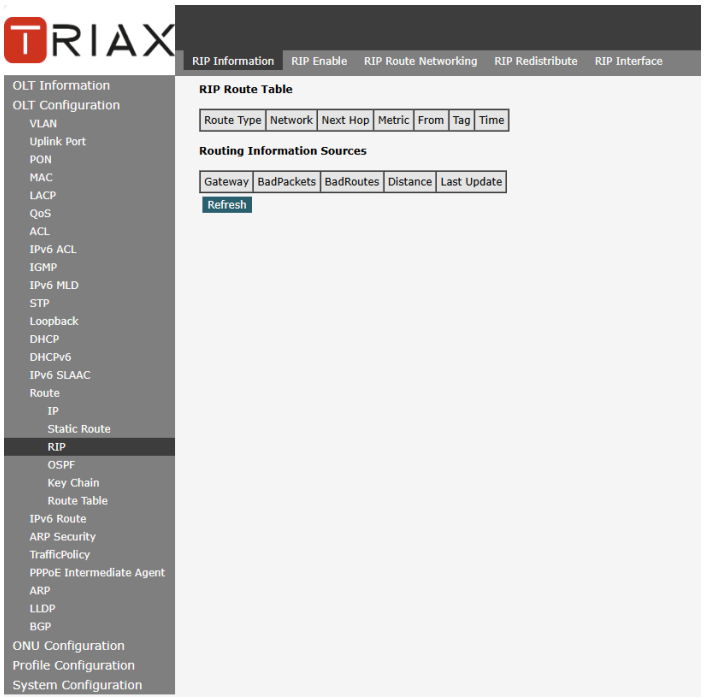


Figure 3.16-4: RIP Information

3.16.3.2 RIP Enable

OLT Configuration → Route → RIP → RIP Enable

Enable RIP protocol and configure RIP parameters.

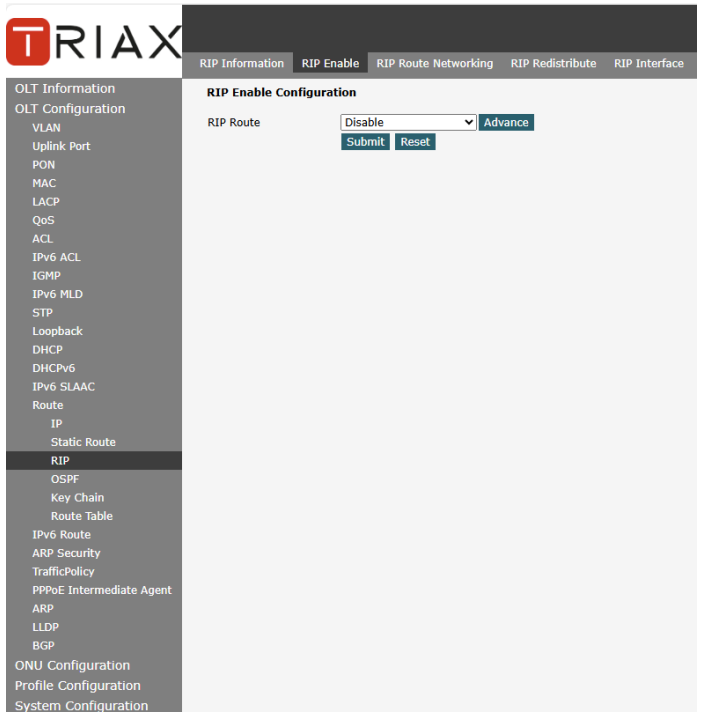


Figure 3.16-5: RIP Enable

3.16.3.3 RIP Route Networking

OLT Configuration → Route → RIP → RIP Route Networking

This page is used to add RIP route networking. VLAN IP address must be set before adding the VLAN to RIP route networking table.

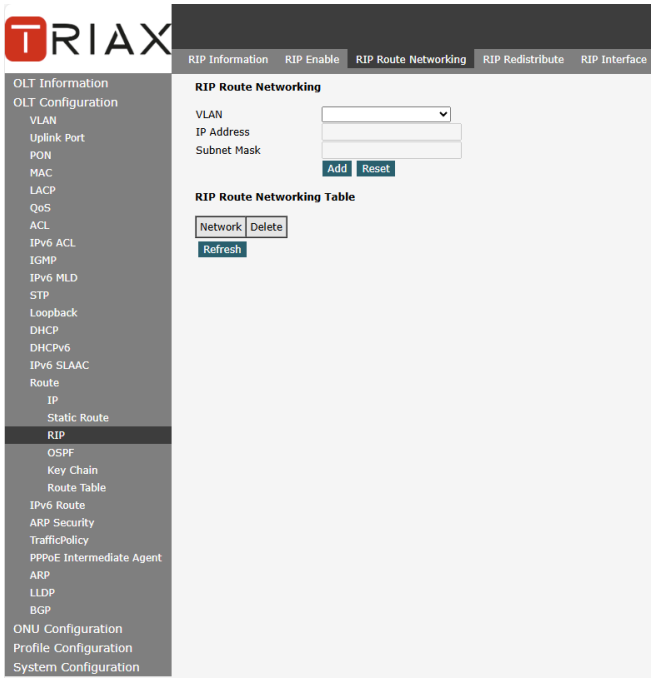


Figure 3.16-6: RIP Route Networking

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.

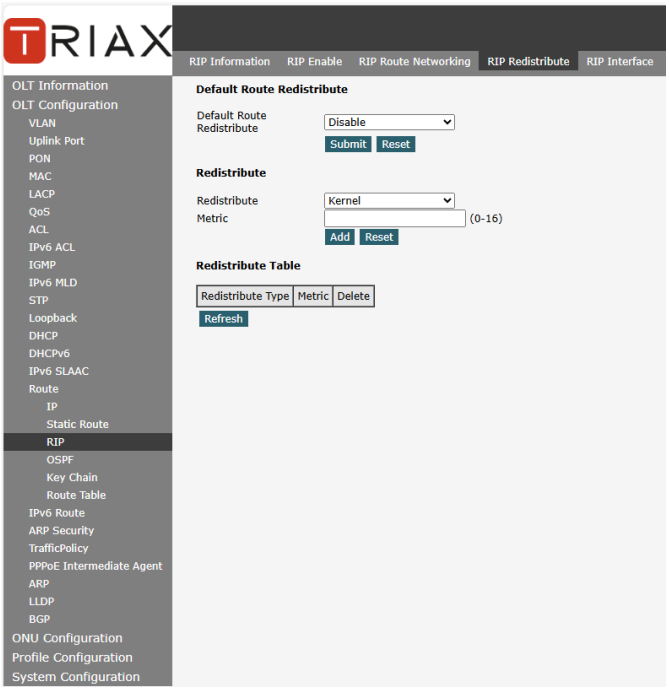


Figure 3.16-7: RIP Redistribute

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.

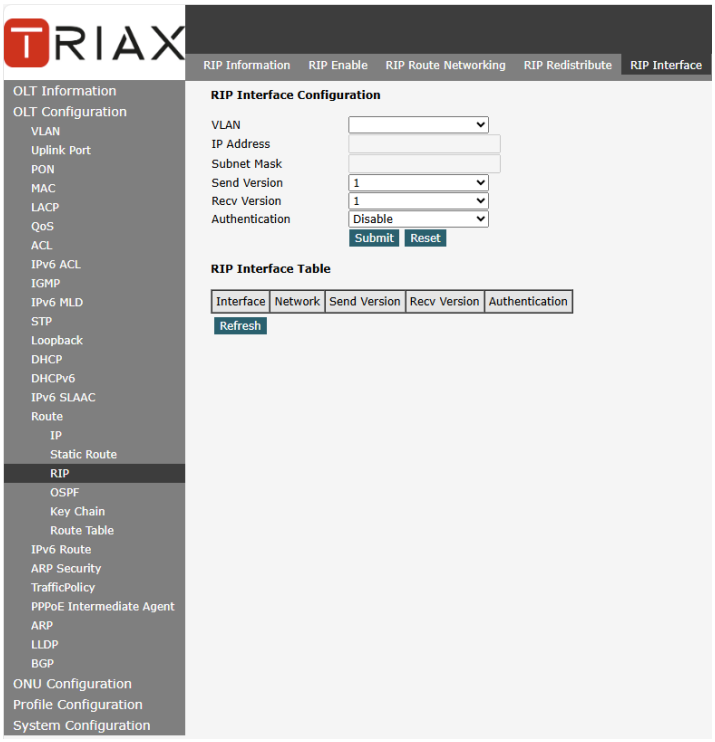


Figure 3.16-8: RIP Interface

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 neighbour information and OSPF routing information.

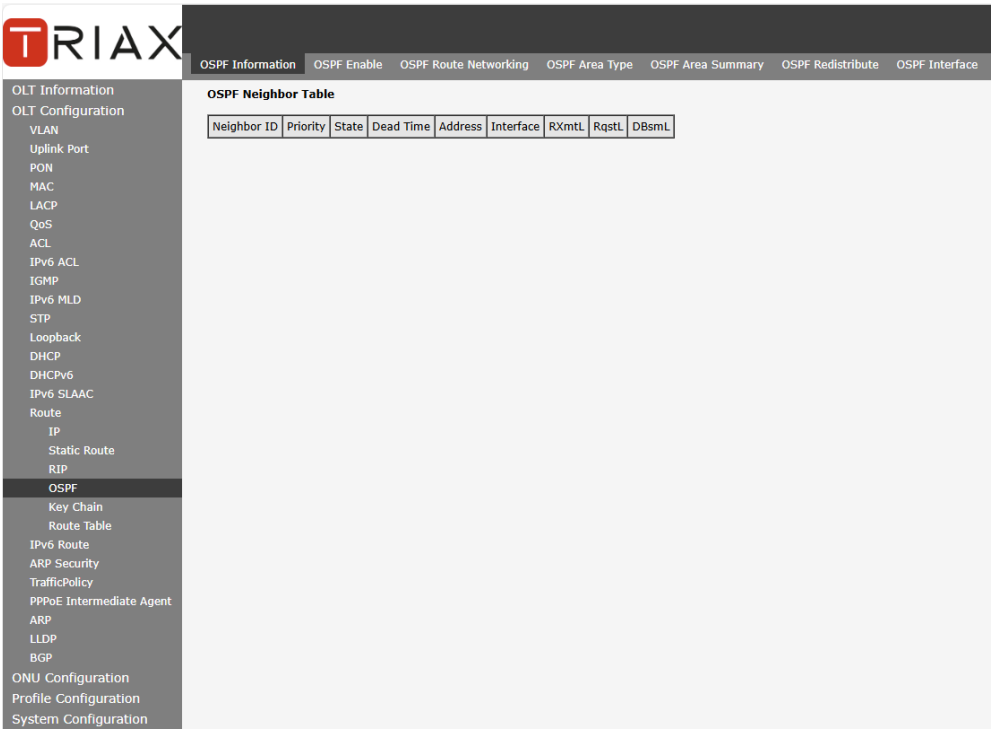


Figure 3.16-9: OSPF Information

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.

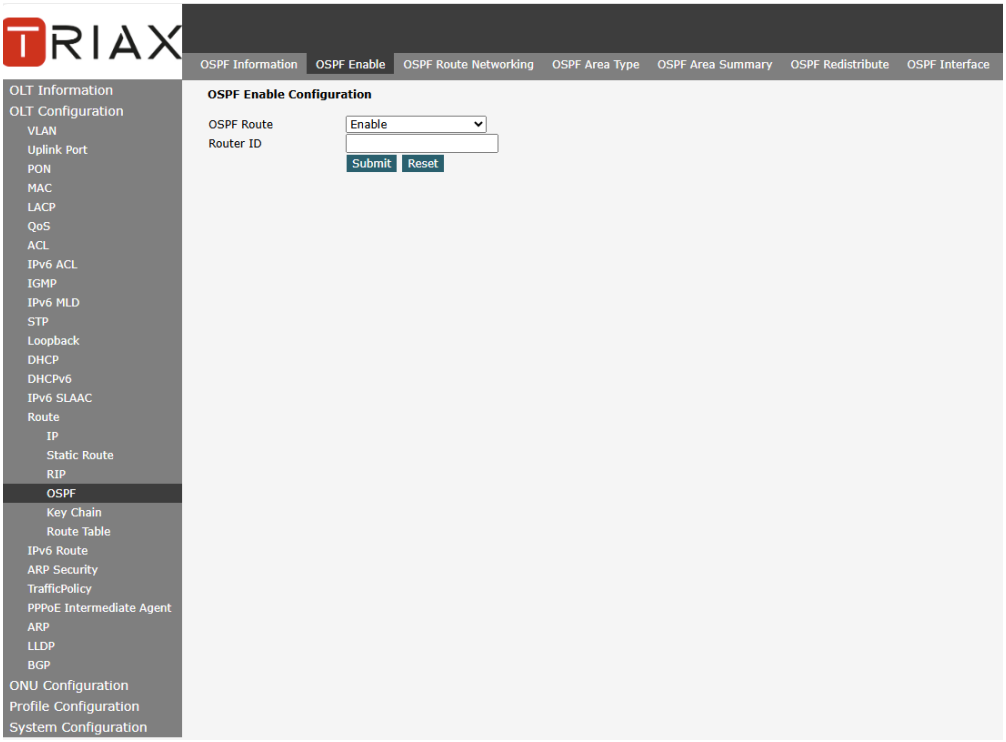


Figure 3.16-10: OSPF Enable

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.

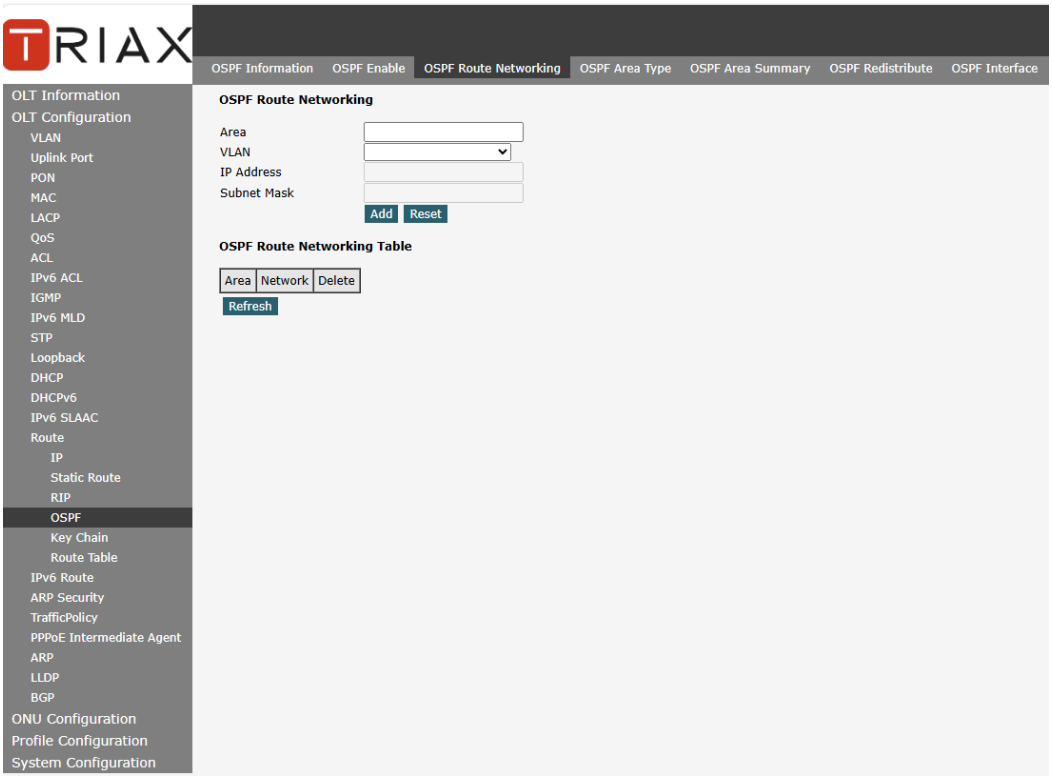


Figure 3.16-11: OSPF Route Networking

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.

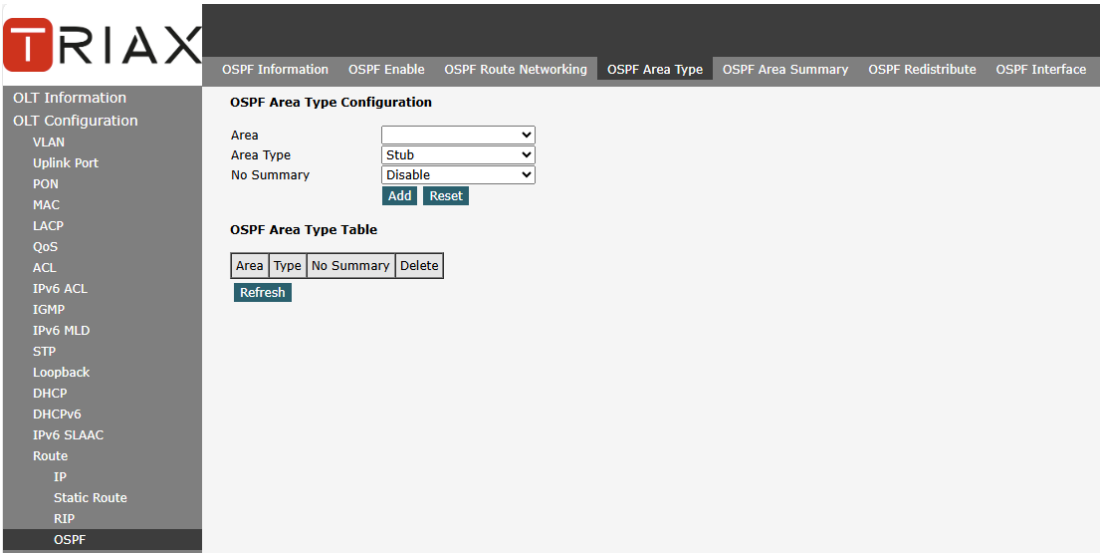


Figure 3.16-12: OSPF Area Type

3.16.4.5 OSPF Area Summary

OLT Configuration → Route → OSPF → OSPF Area Summary

This page is used to configure area IP address summary.

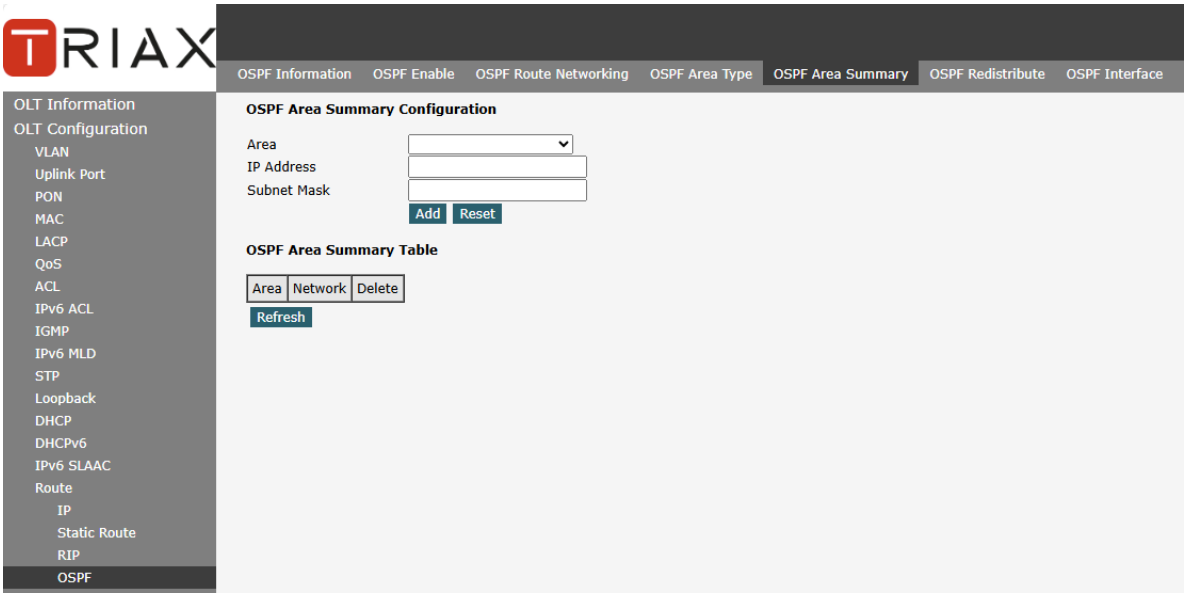


Figure 3.16-13: OSPF Area Summary

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

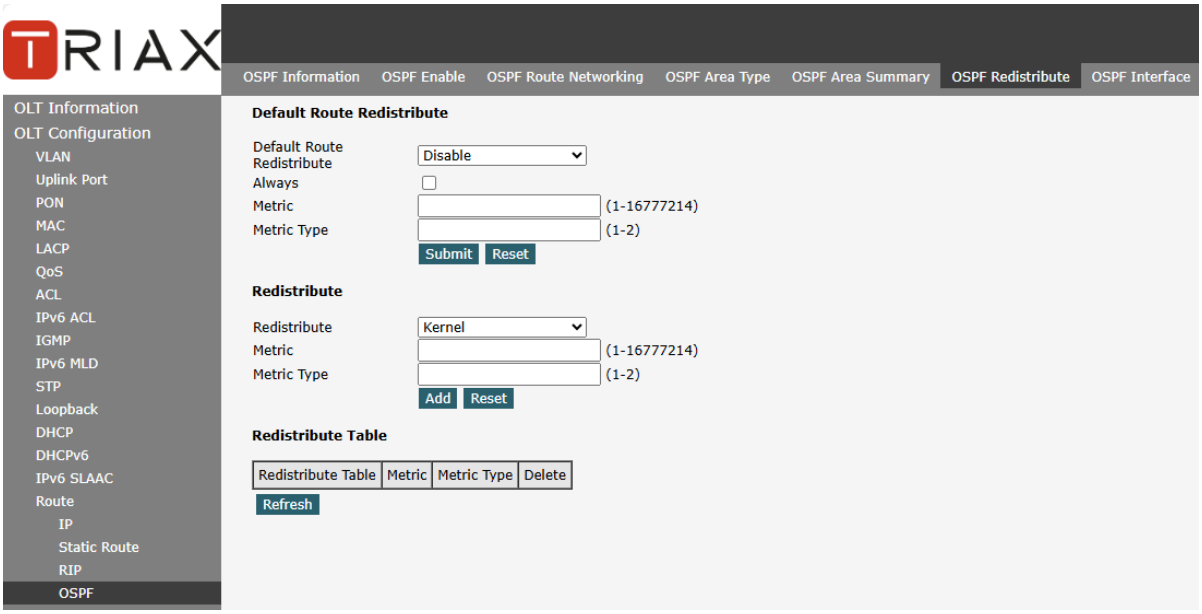


Figure 3.16-14: OSPF Redistribute

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.

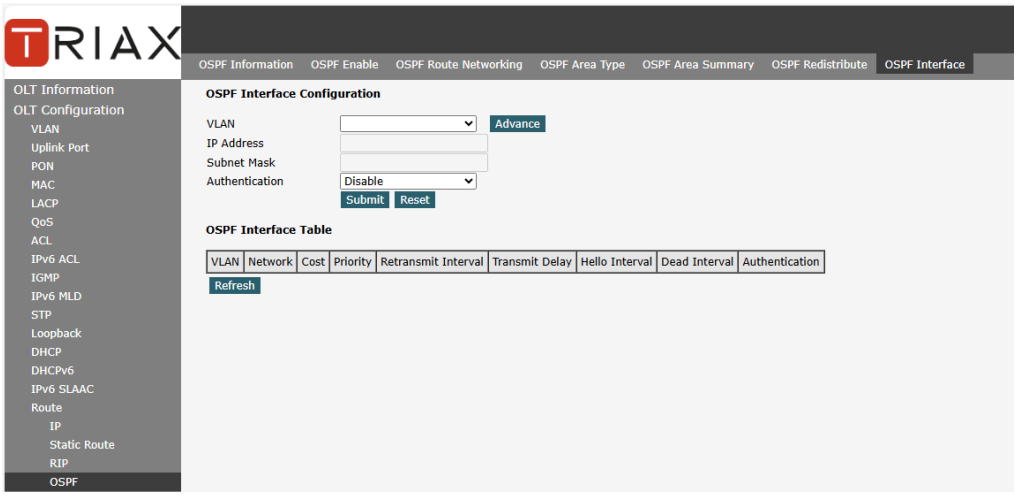


Figure 3.16-15: OSPF Interface

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

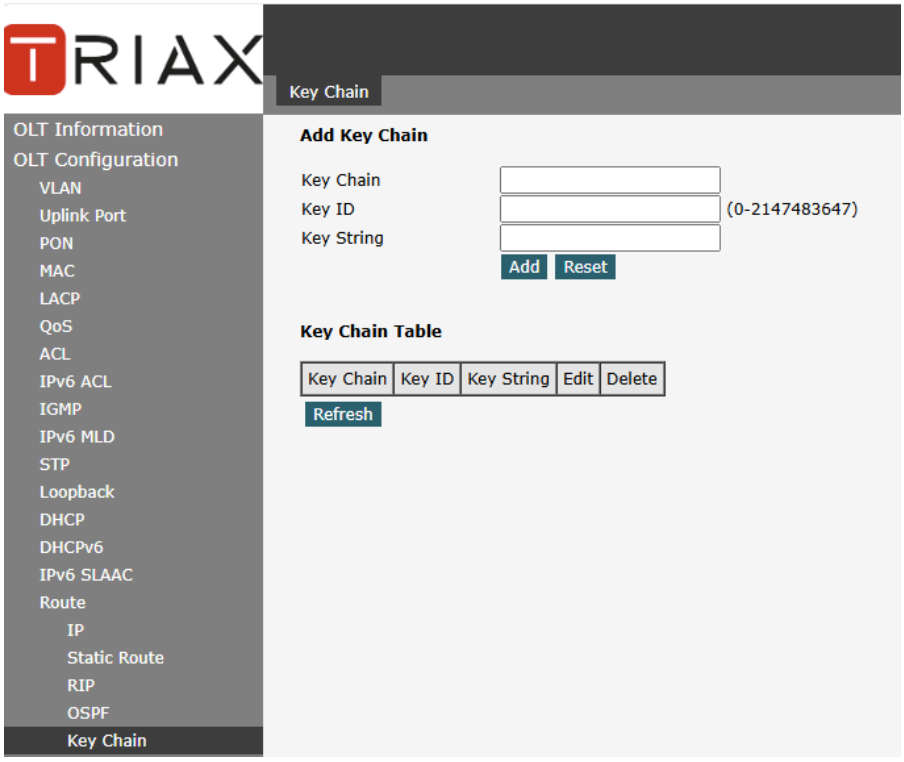


Figure 3.16-16: Key Chain

3.16.6 Route Table

OLT Configuration → Route → Route Table

This page displays routing items of OLT.

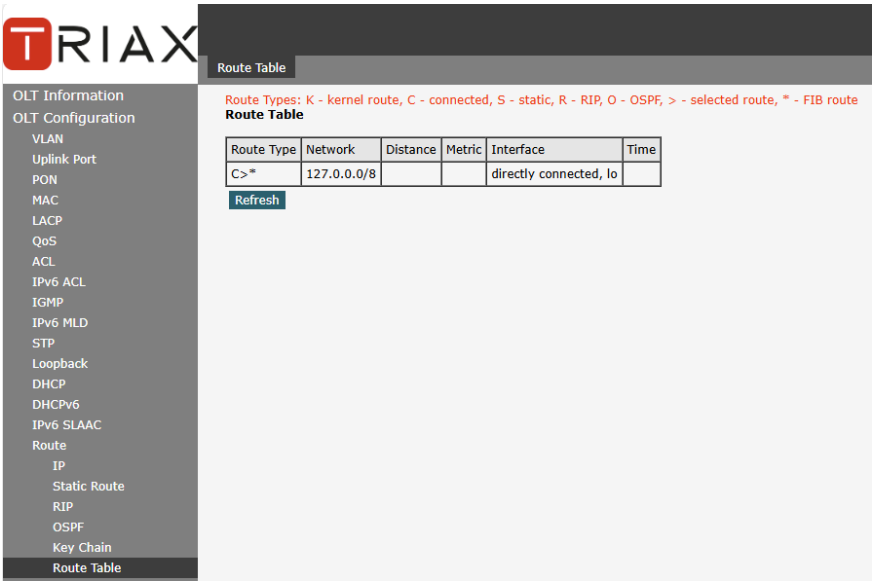


Figure 3.16-17: Route Table

3.17 IPv6 Route

3.17.1 IPv6

OLT Configuration → IPv6 Route → IPv6 → VLAN IPv6

Configure IPv6 address for VLAN that has been created.

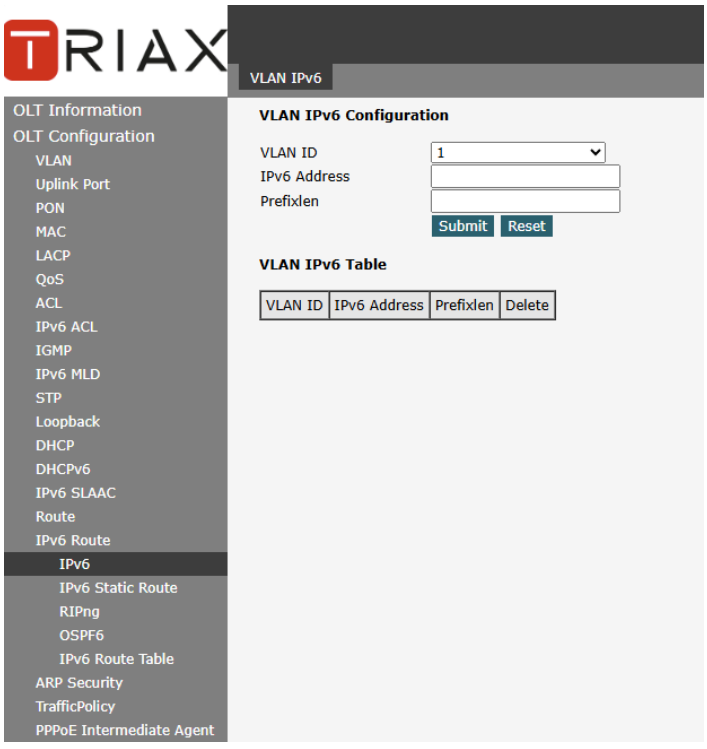


Figure 3.17-1: VLAN IPv6

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.

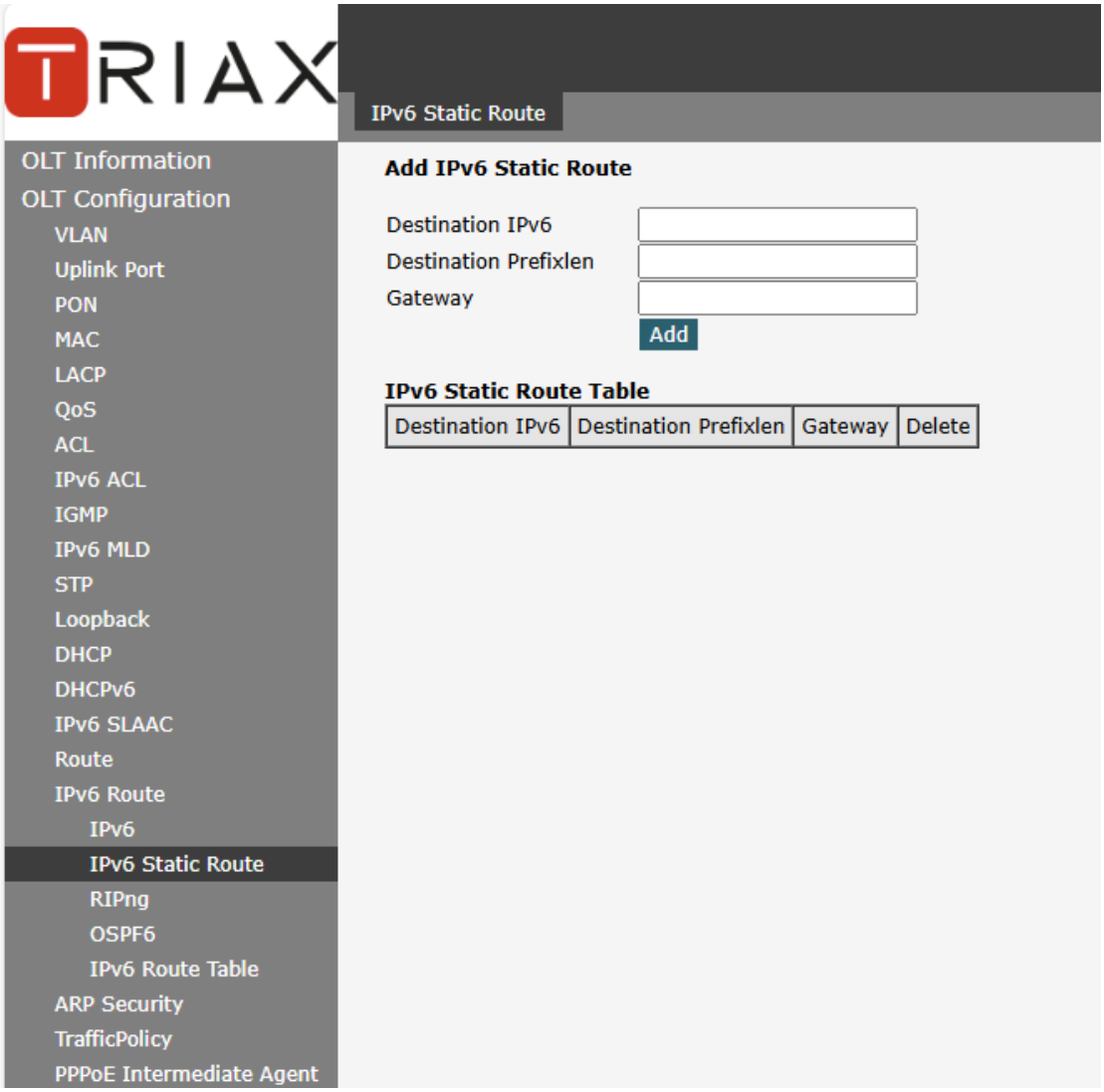


Figure 3.17-2: IPv6 Static Route

3.17.3 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.

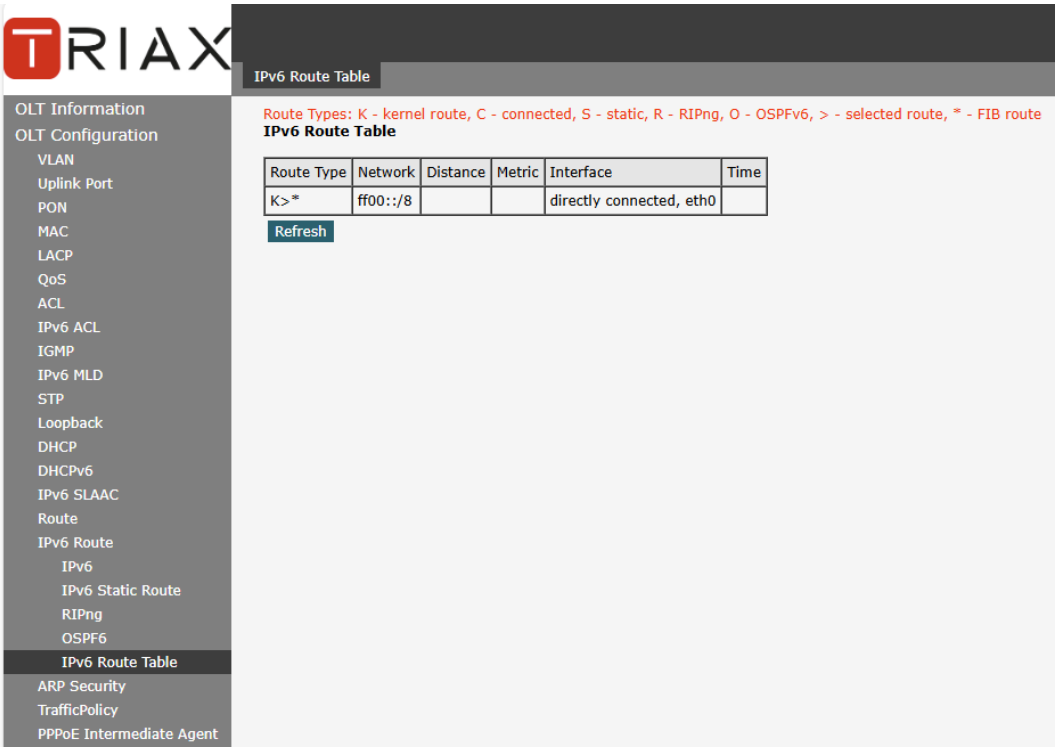


Figure 3.17-3: IPv6 Route Table

3.18 ARP Security

3.18.1 Dynamic ARP Inspection

OLT Configuration → ARP Security → Dynamic ARP Inspection (DAI)

Configure IPv6 address for VLAN that has been created.

Dynamic ARP Inspection is a security feature that checks ARP packets on the network to prevent ARP spoofing attacks.

- **Trusted Port**: Allows ARP packets without inspection (used for uplink ports or known safe devices).
- **Untrusted Port**: ARP packets are inspected and only allowed if they match the IP–MAC binding table. You can apply DAI per VLAN, so only ARP traffic in those VLANs is monitored.

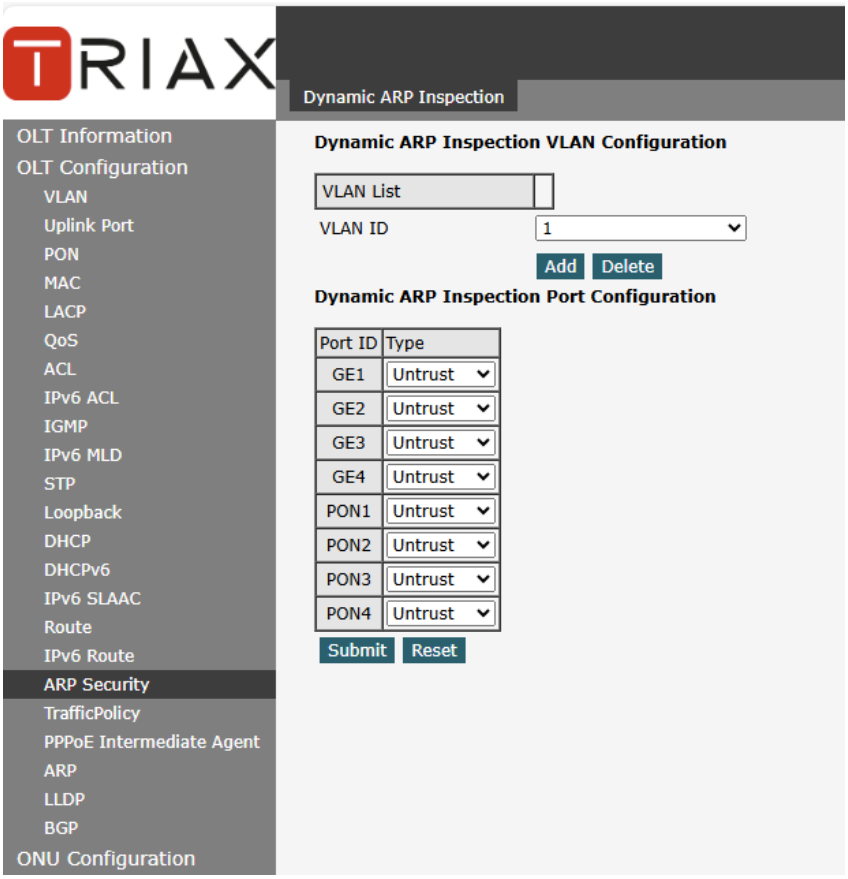


Figure 3.18.1: ARP Security

3.19 Traffic policy

OLT Configuration → Traffic Policy

Traffic Policy is used to identify and control different types of network traffic based on set rules, helping manage bandwidth and priority.

- **Classifier**:
  Defines the matching conditions to identify specific traffic.
  Examples: match by VLAN ID, IP address, protocol, port number, or DSCP value.
  This is like a filter that “marks” the packets you want to control.

- **Behaviour**:
  Defines what action to take for traffic that matches a classifier.
  Examples: limit bandwidth, change priority, allow/deny, or redirect traffic.
  This is like the “rule” applied once the packets are identified.

By combining a **Classifier** with a **Behaviour**, you can shape traffic flow, protect important services, and prevent network congestion.

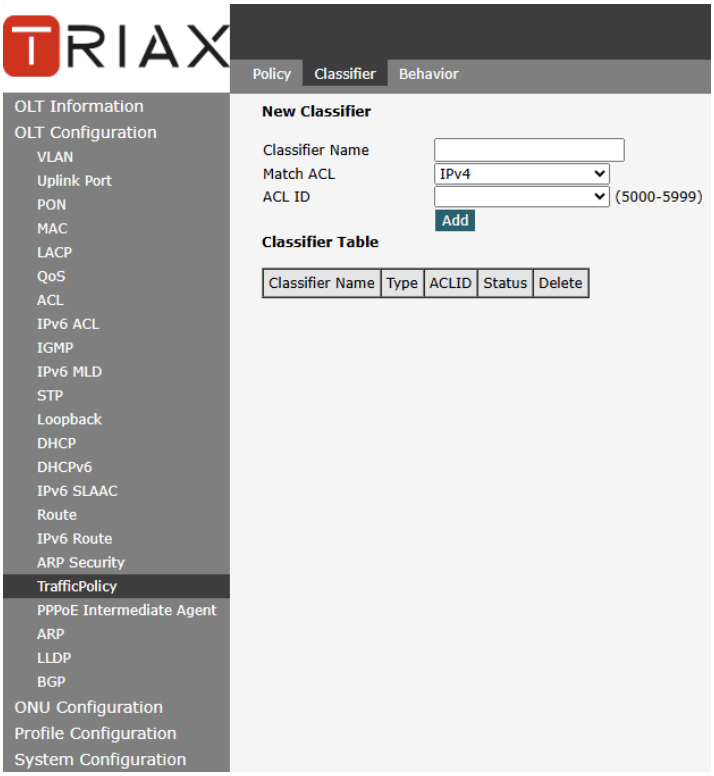


Figure 3.19: Traffic Policy

3.20 PPPoE Intermediate Agent

OLT Configuration → PPPoE Intermediate Agent

The PPPoE Intermediate Agent adds extra information (like VLAN ID or port ID) into PPPoE discovery packets between the ONU and the PPPoE server.
This helps the server identify which user is connecting and from where, making user management and authentication easier.

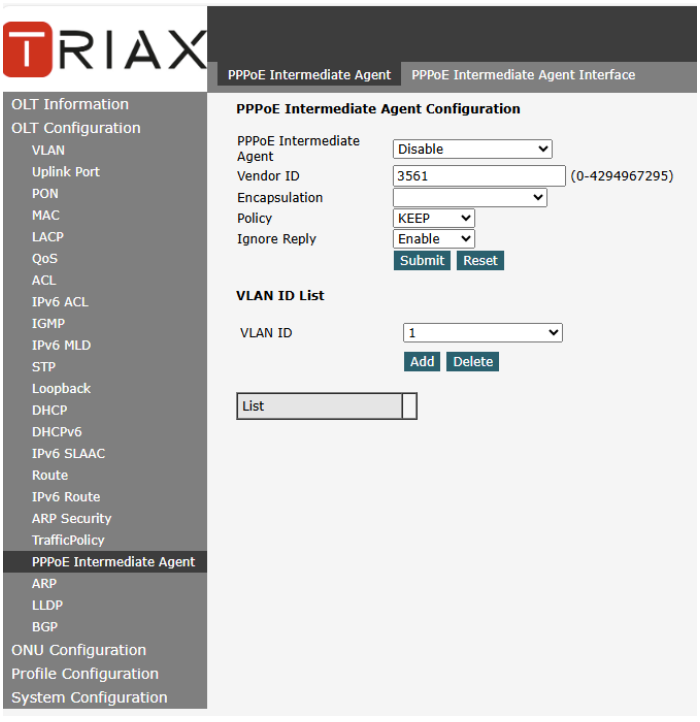


Figure 3.20.1: PPPoE Intermediate Agent

3.20.1 IPv6

OLT Configuration → PPPoE Intermediate Agent → PPPoE Intermediate Agent interface

Let's you select which OLT ports or VLANs will use the PPPoE Intermediate Agent.
This way, only traffic from certain interfaces will carry the extra identification tags.

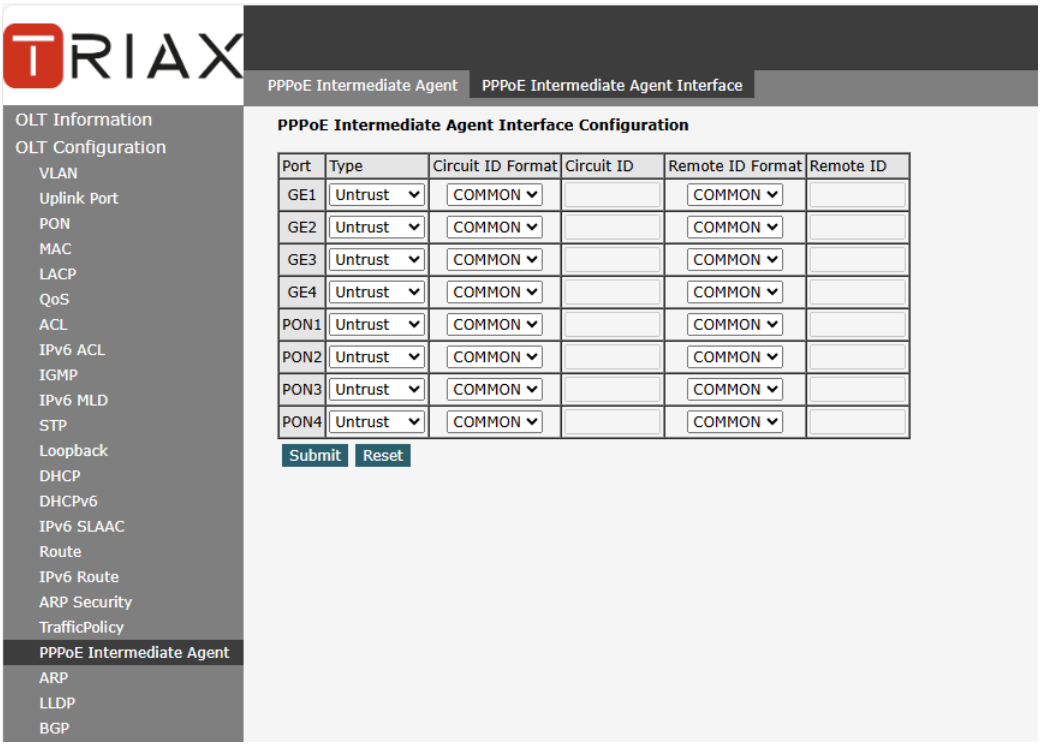


Figure 3.20.2: PPPoE Intermediate Agent interface

3.21 ARP

3.21.1 ARP Table

OLT Configuration → ARP→ ARP Table

ARP is used to map an IP address to its corresponding MAC address so devices can communicate within the network. ARP Table: Shows the current IP-to-MAC address mappings learned by the OLT. This is like a phonebook for the network, telling the OLT which MAC address belongs to which IP.

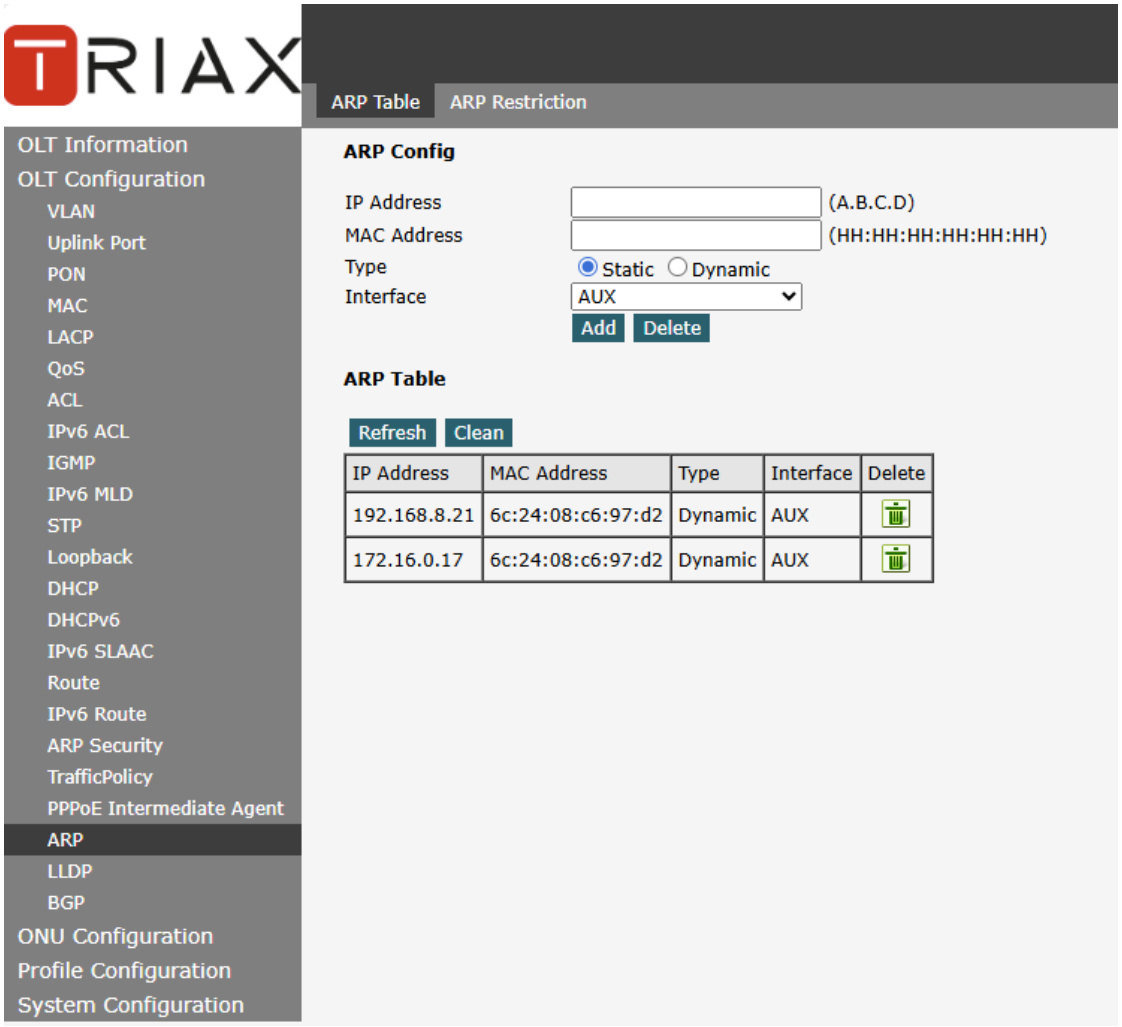


Figure 3.21.1: ARP Table

3.21.2 ARP Restriction

OLT Configuration → ARP→ ARP Restriction

Let's you control which IP–MAC pairs are allowed to communicate.
You can set static bindings to prevent unauthorized devices from using a valid IP address (protects against ARP spoofing).

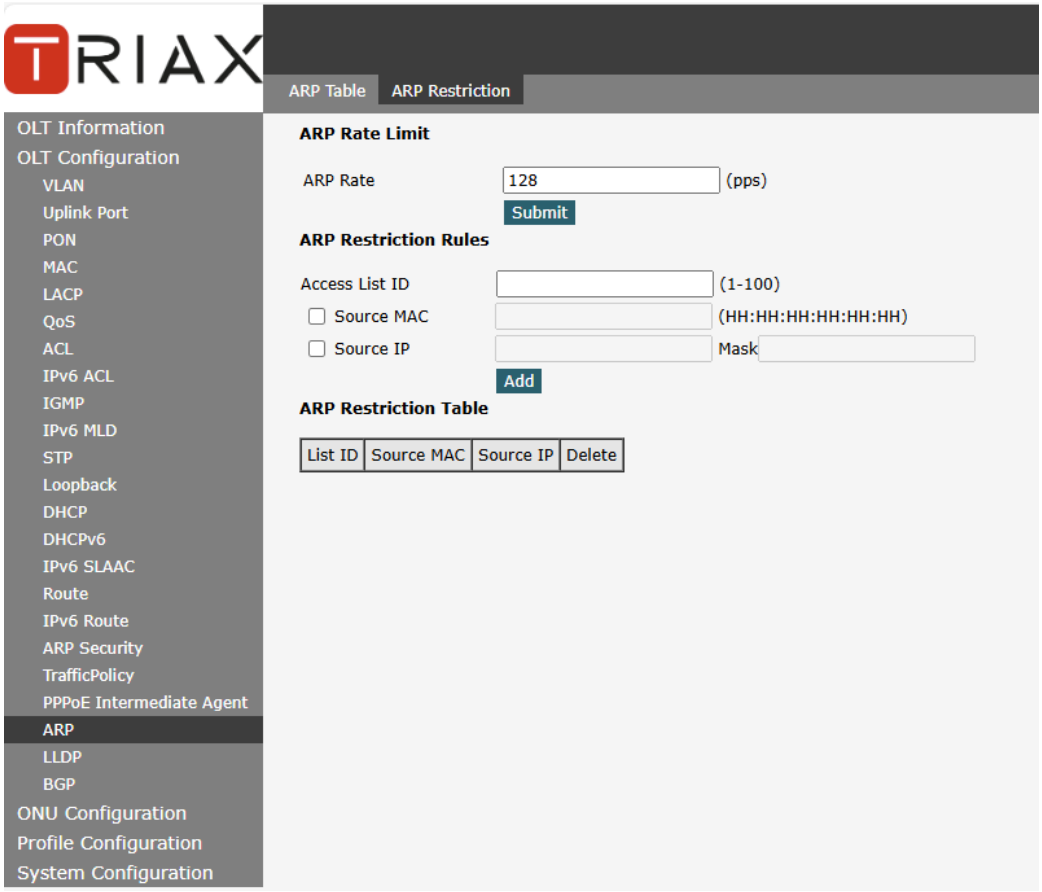


Figure 3.21.2: ARP Restriction

3.22 LLDP

OLT Configuration → LLDP

LLDP is a vendor-neutral protocol used by network devices to announce their identity and capabilities to directly connected neighbours. It helps network administrators discover device details, verify connections, and build accurate network topology maps.

3.22.1 LLDP Information

OLT Configuration → LLDP→ Information

Shows a list of neighbouring devices detected via LLDP, including their system name, port ID, VLAN information, and supported features (e.g., PoE, capabilities). Useful for confirming correct cabling and connectivity.

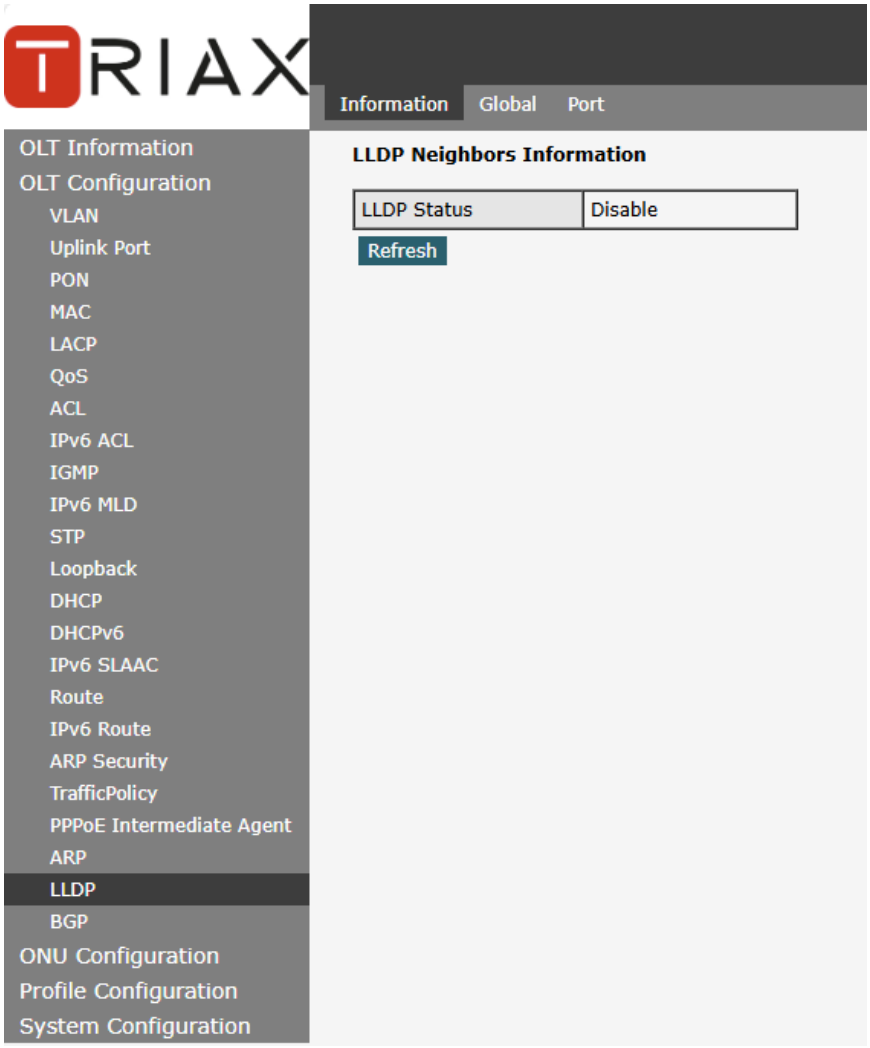


Figure 3.22.1: LLDP Information

3.22.2 LLDP Global

OLT Configuration → LLDP→ Global

Enables or disables LLDP across the entire OLT.
Here you can set parameters such as:

- Transmit Interval – how often LLDP packets are sent
- Hold Time – how long neighbour information is kept before it expires
- Re-initialization Delay – wait time before restarting LLDP after a change

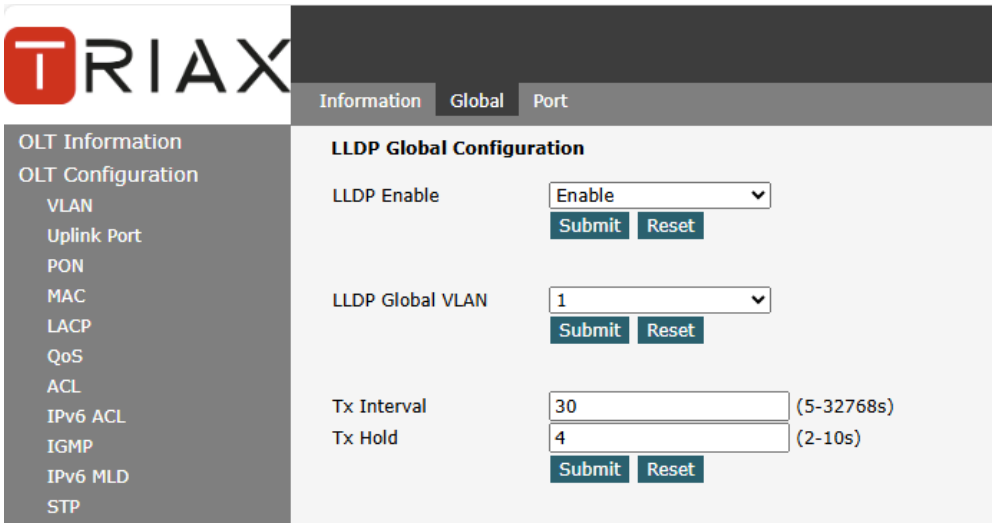


Figure 3.22.2: LLDP Information

3.22.3 LLDP Global

OLT Configuration → LLDP→ Port

Allows enabling/disabling LLDP on specific OLT ports and choosing what information each port advertises (e.g., port description, VLAN, capabilities).
This is useful for enabling LLDP only where it's needed or limiting information for security.

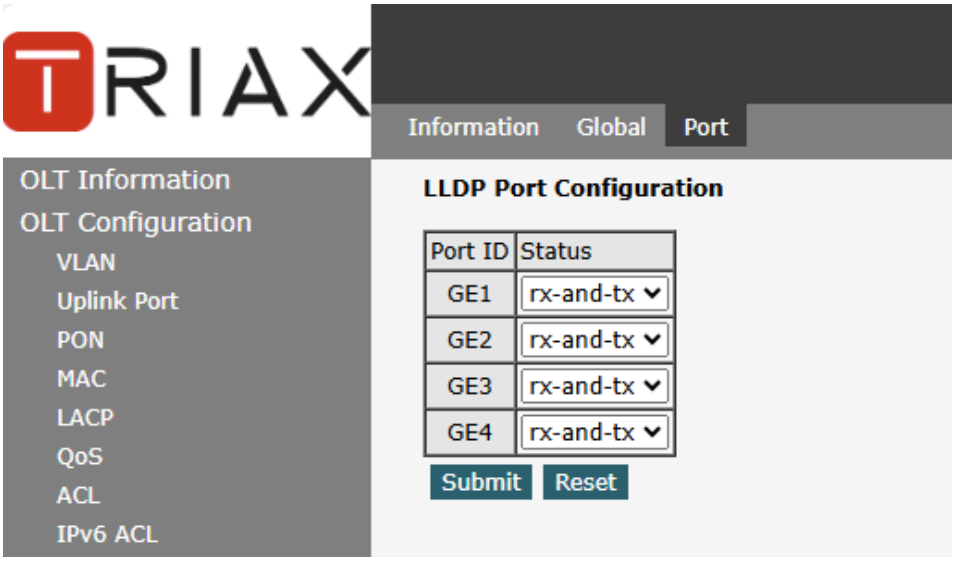


Figure 3.22.3: LLDP Port

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 ONUs will be displayed in this interface. You can check ONU using profile, Registration mode and do some operations to every ONU.

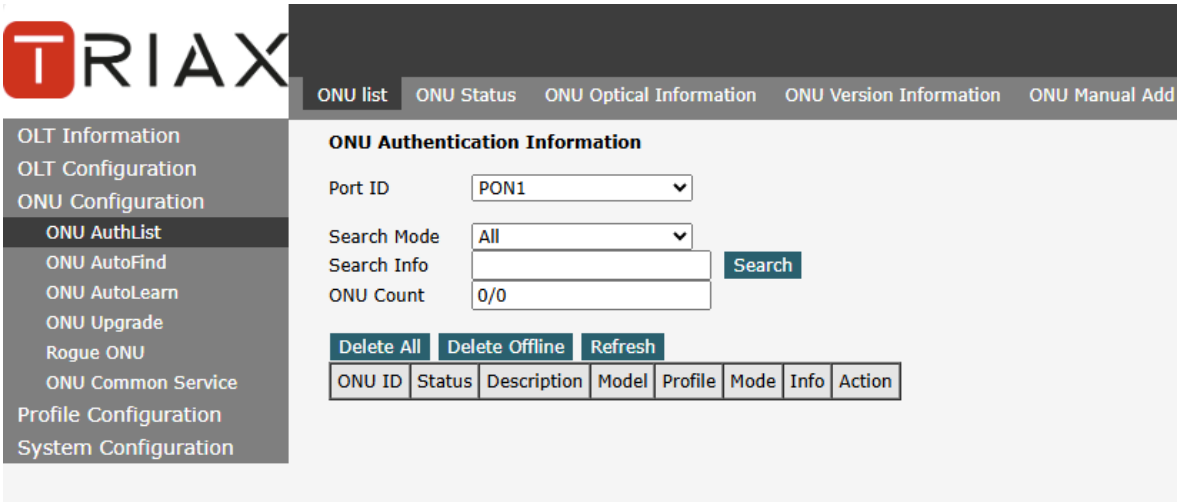


Figure 4.1-1: ONU List

4.1.1.1 Config

ONU Configuration→ONU AuthList→ONU List→Config

Configure ONU parameter information which you selected.

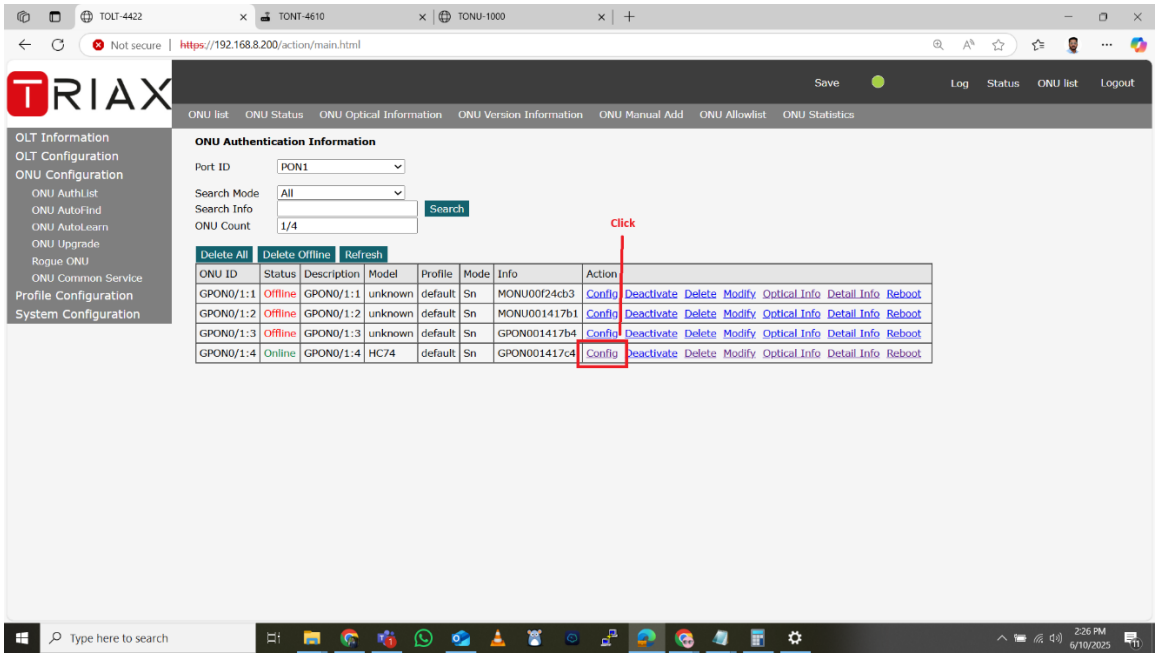


Figure 4.1-2: Configure ONU

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.

Create tcont ID and bind DBA profile. Tcont name is optional.

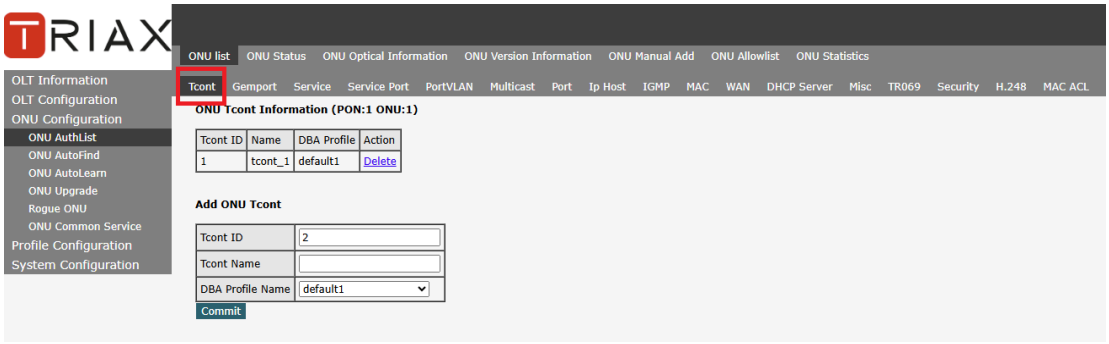


Figure 4.1-3: Create Tcont

4.1.1.1.2 Gemport

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

Create gemport ID and bind tcont ID.

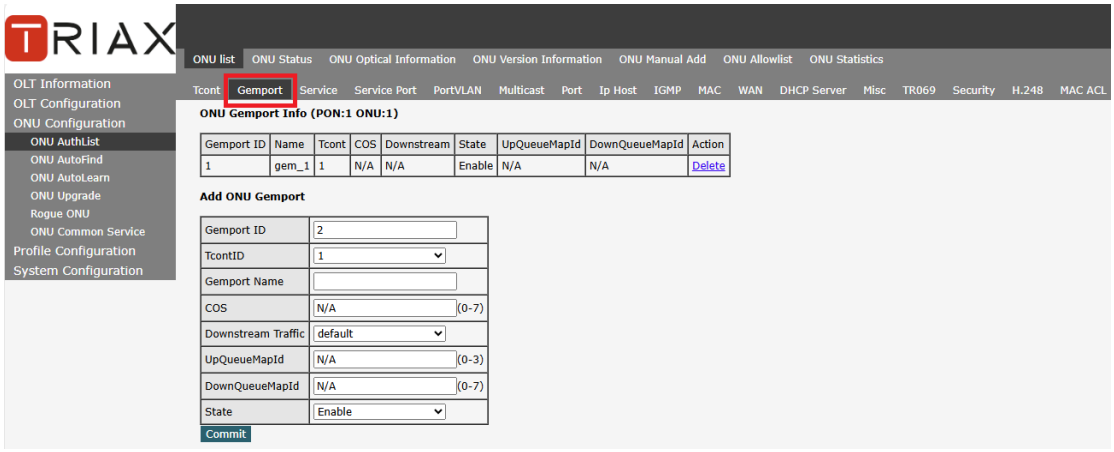


Figure 4.1-4: Create gemport

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.

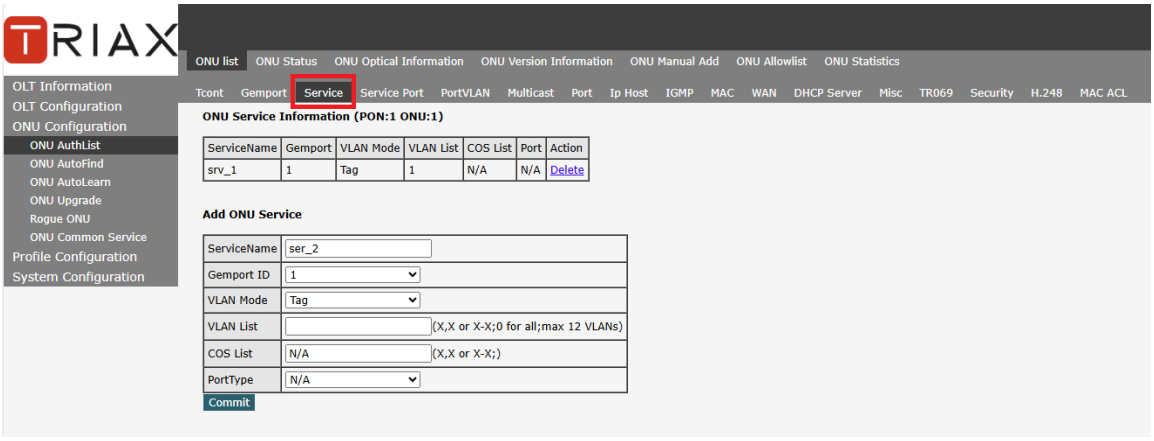


Figure 4.1-5: Create service

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.

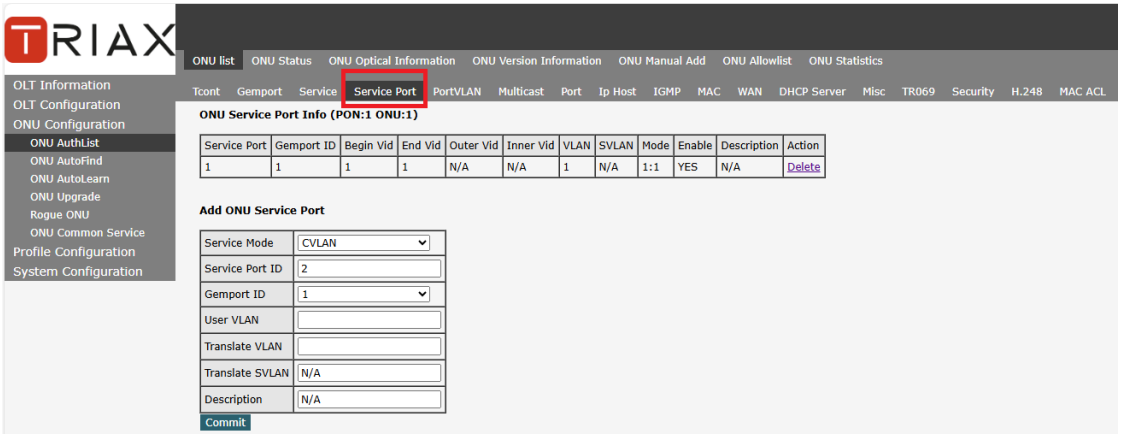


Figure 4.1-6: Create service port

4.1.1.1.5 PortVlan

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

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

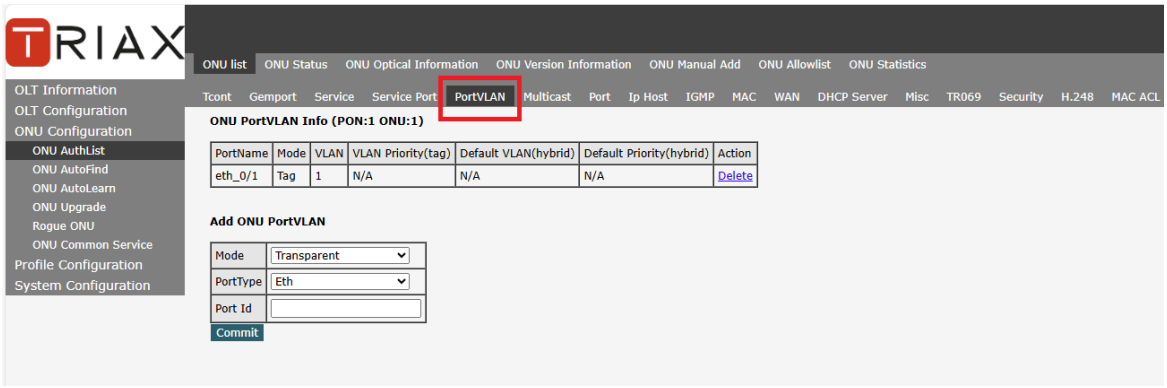


Figure 4.1-7: Configure port VLAN mode

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's port.

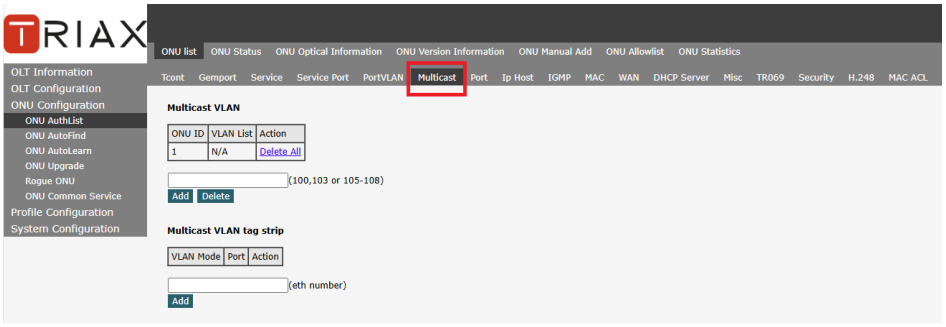


Figure 4.1-8: Configure multicast VLAN

4.1.1.1.7 Port

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

Set attribute of ONU LAN port.

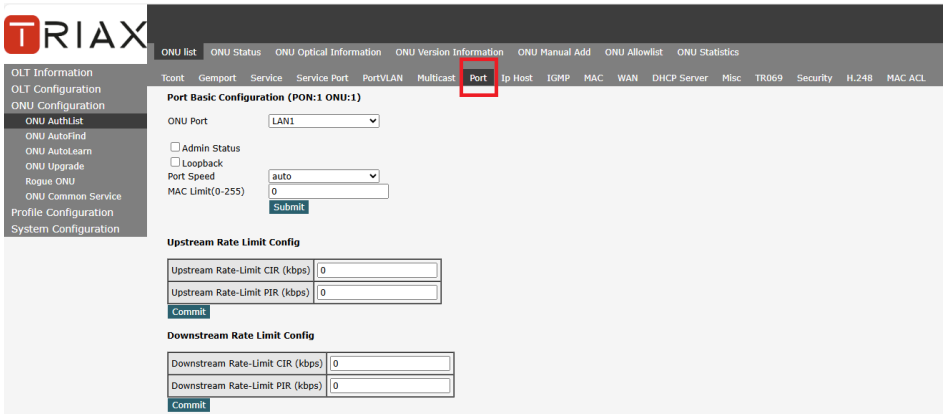


Figure 4.1-9: ONU port attibute

4.1.1.1.8 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.

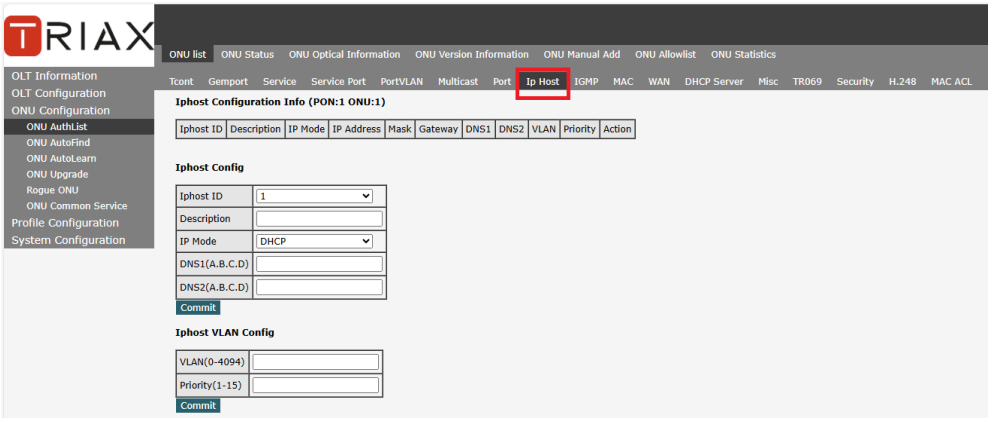


Figure 4.1-10: Configure IPhost

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.

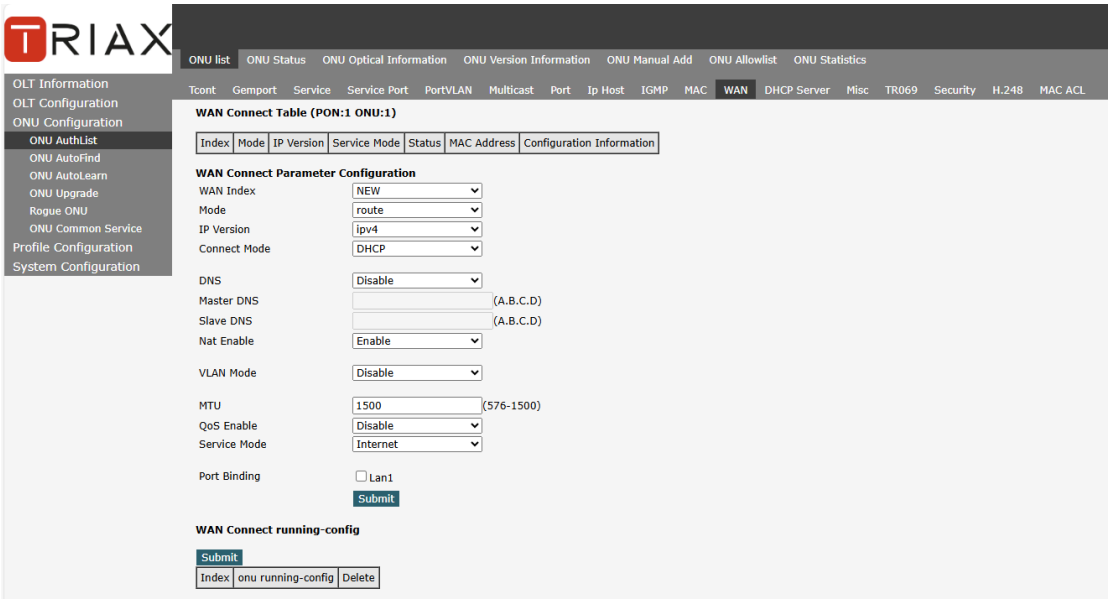


Figure 4.1-11: Configure WAN

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.

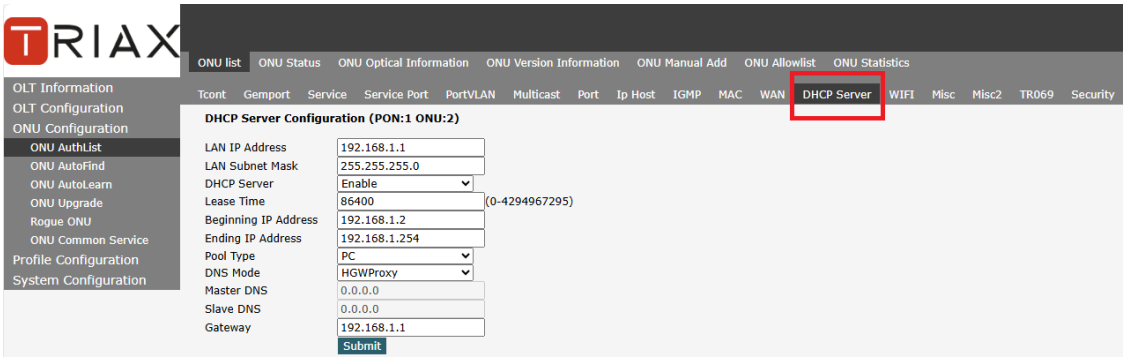


Figure 4.1-12: ONU DHCP Server

4.1.1.1.11 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.

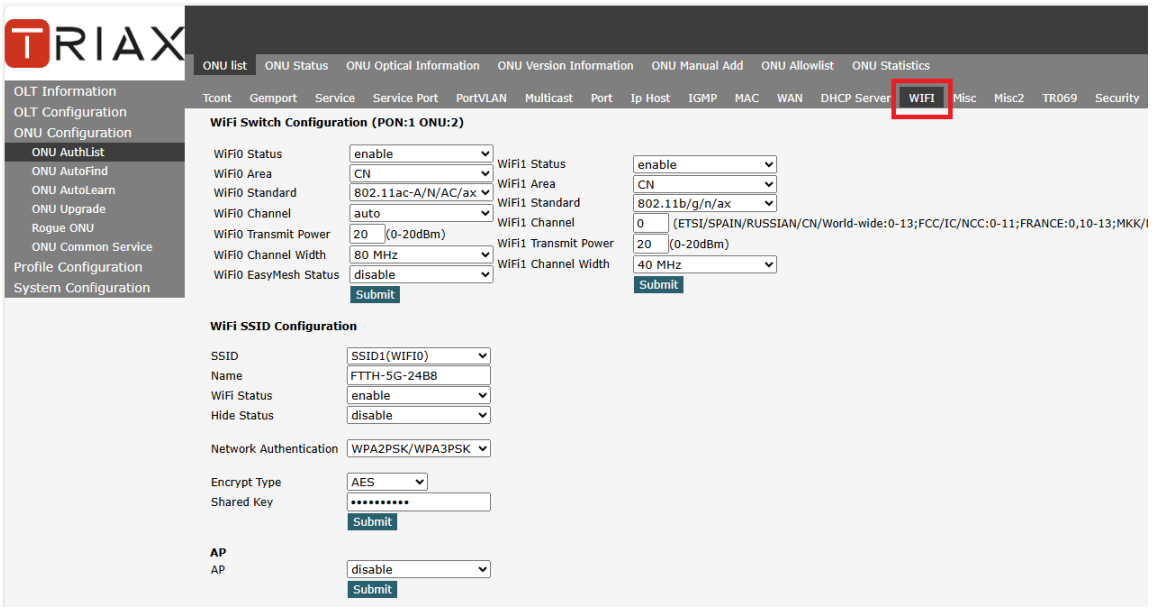


Figure 4.1-14: WIFI Configuration

4.1.1.1.12 Misc

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

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

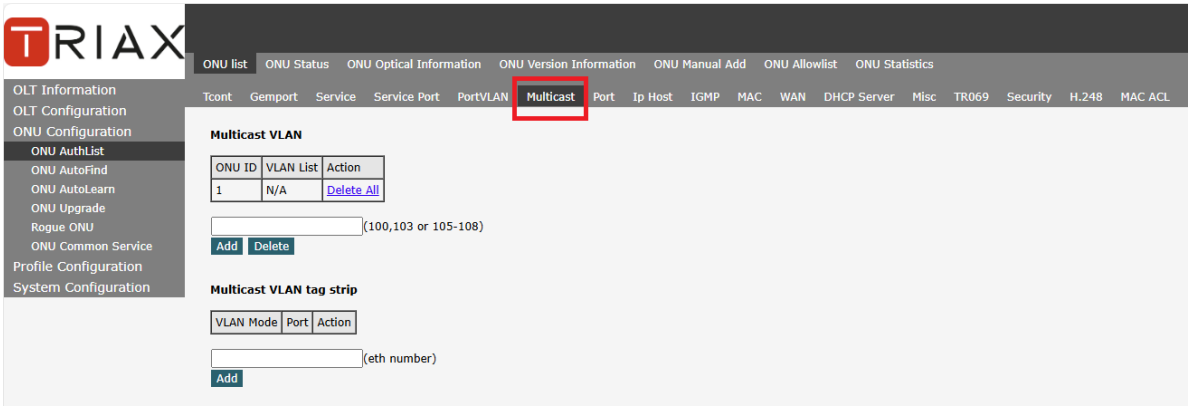


Figure 4.1-18: Misc Configuration

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.

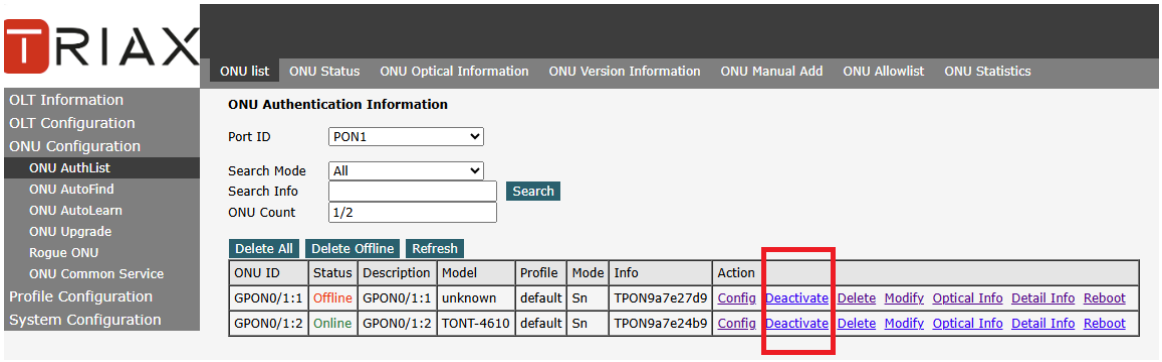


Figure 4.1-19: Deactivate/Activate ONU

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.

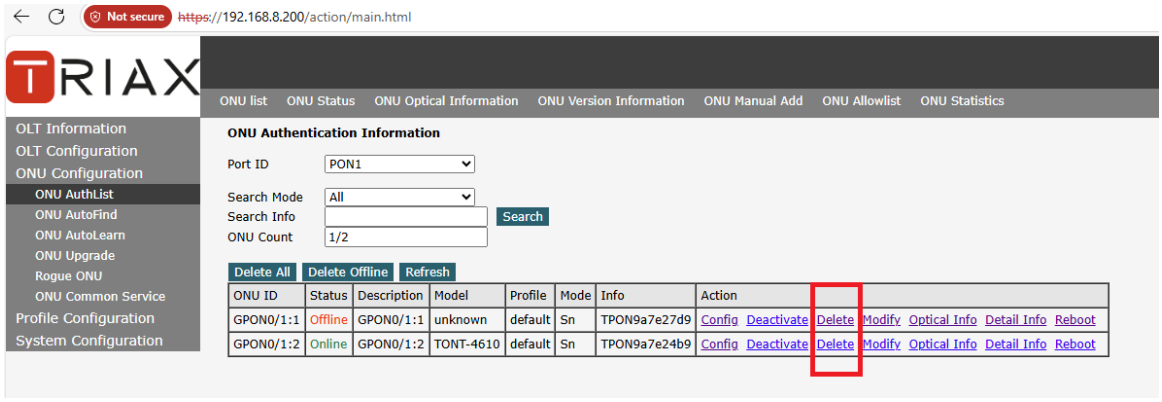


Figure 4.1-20: Delete ONU

4.1.1.4 Modify

ONU Configuration→ONU AuthList→ONU List→Modify

This is used to modify ONU authentication mode.

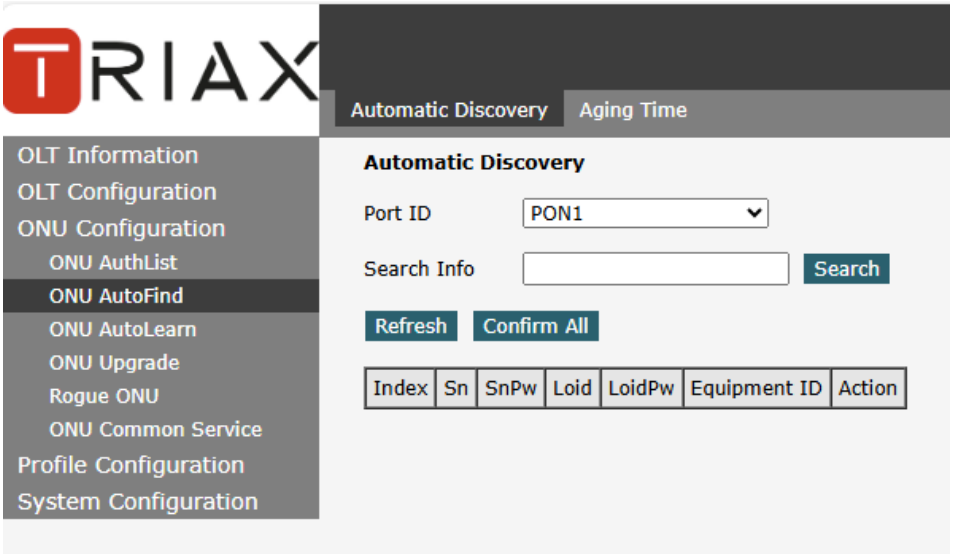
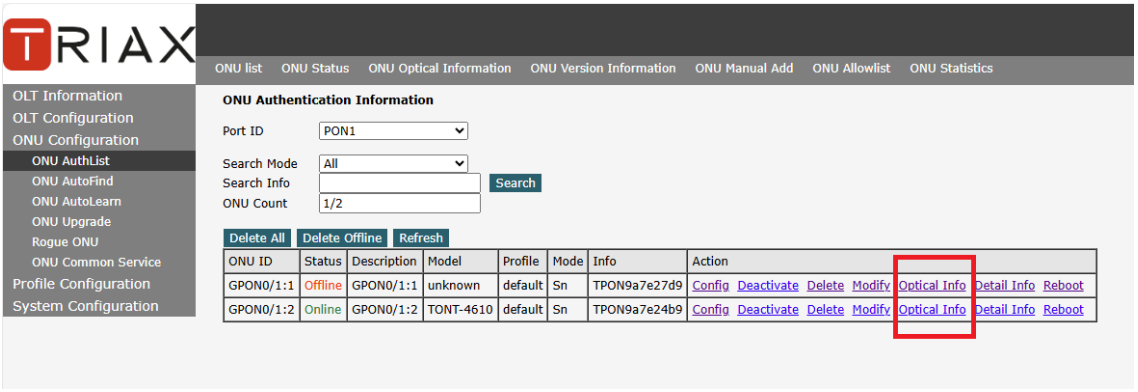


Figure 4.1-21: Modify ONU Authentication mode

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.



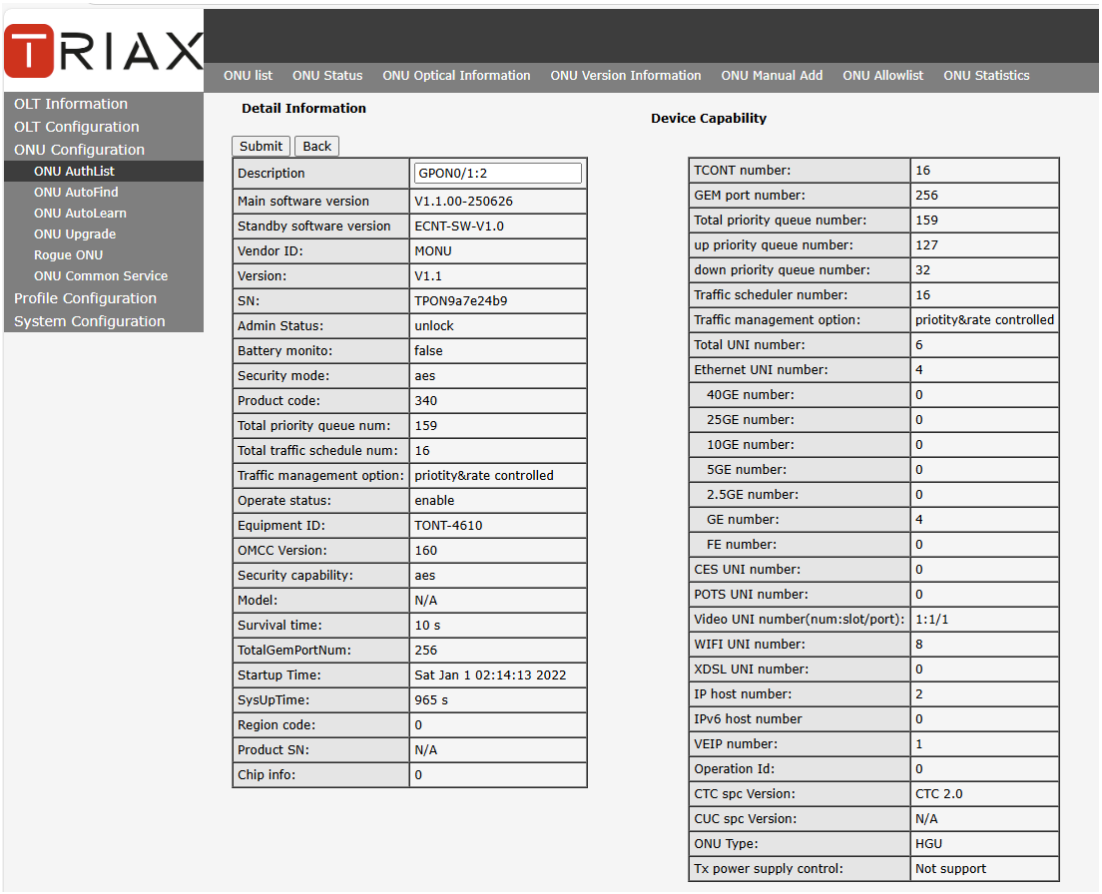


Figure 4.1-22: Optical info of ONU

4.1.1.6 Detail Info

ONU Configuration→ONU AuthList→ONU List→Detail Info

Check the Detail Info of ONU which you selected.

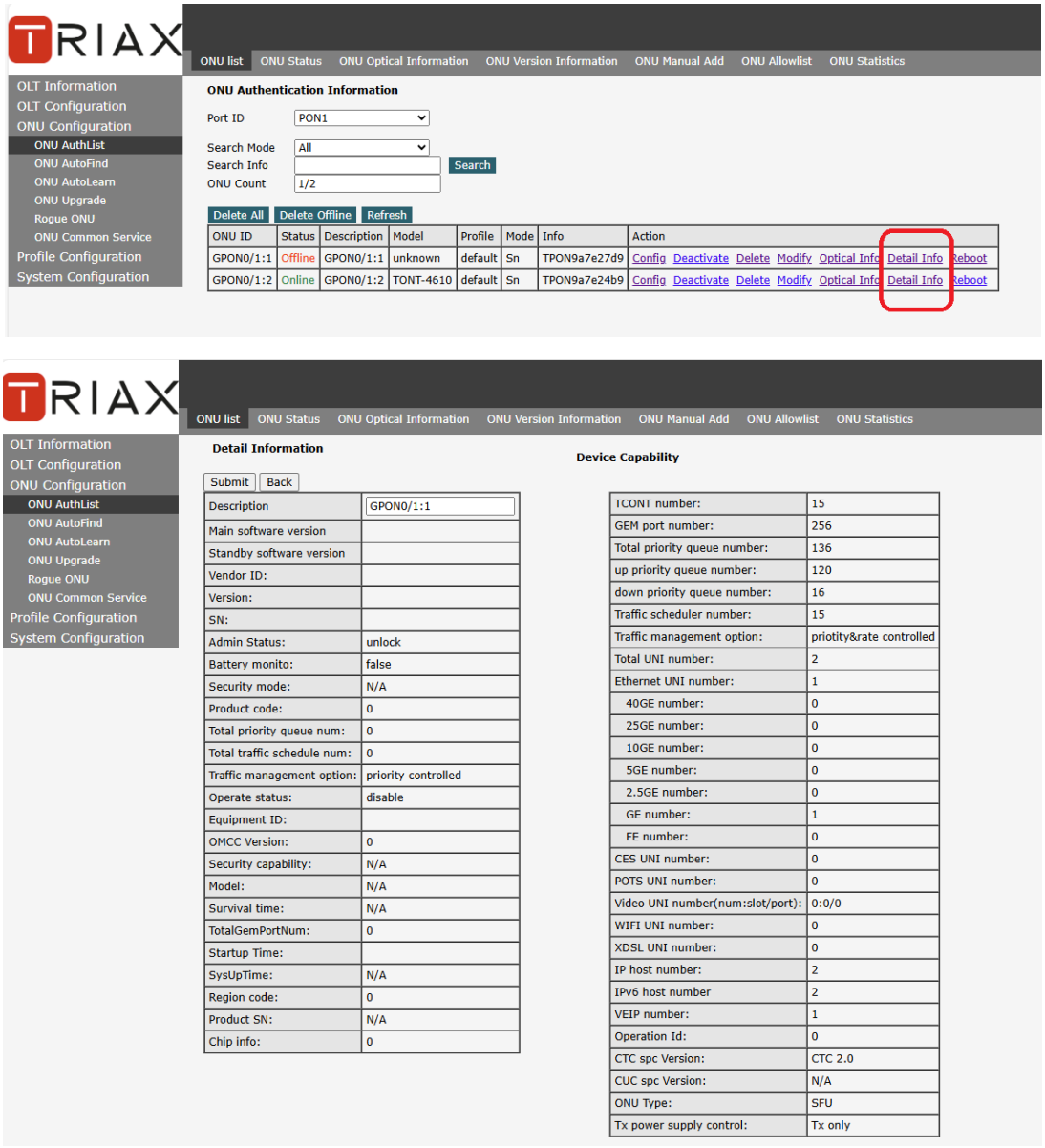


Figure 4.1-23: Detail info of ONU

4.1.1.7 Reboot

ONU Configuration→ONU AuthList→ONU List→Reboot

Reboot ONU which you selected.

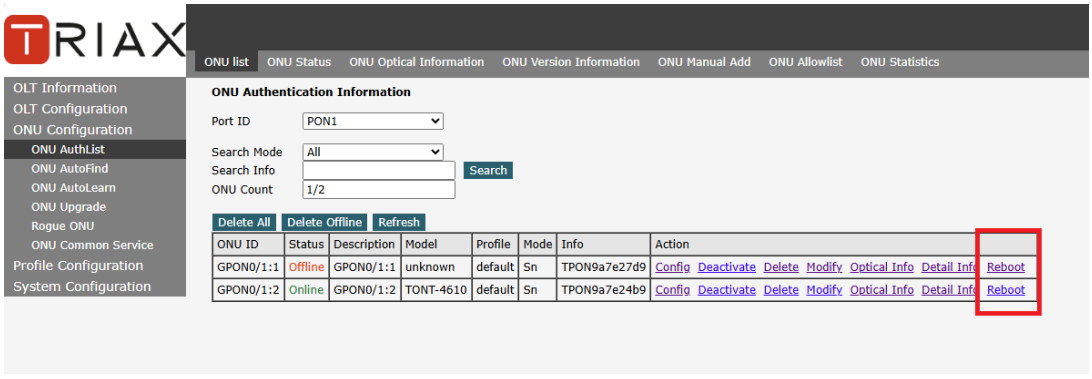


Figure 4.1-24: Reboot ONU

4.1.2 ONU Status

ONU Configuration→ONU AuthList→ONU Status

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

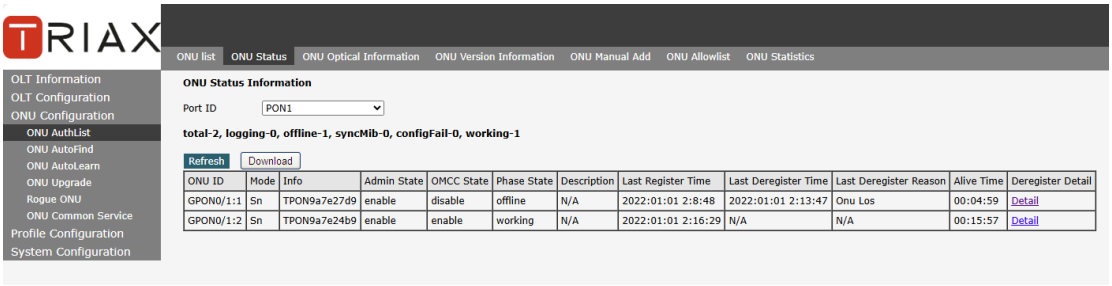


Figure 4.1-25: ONU Status

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.

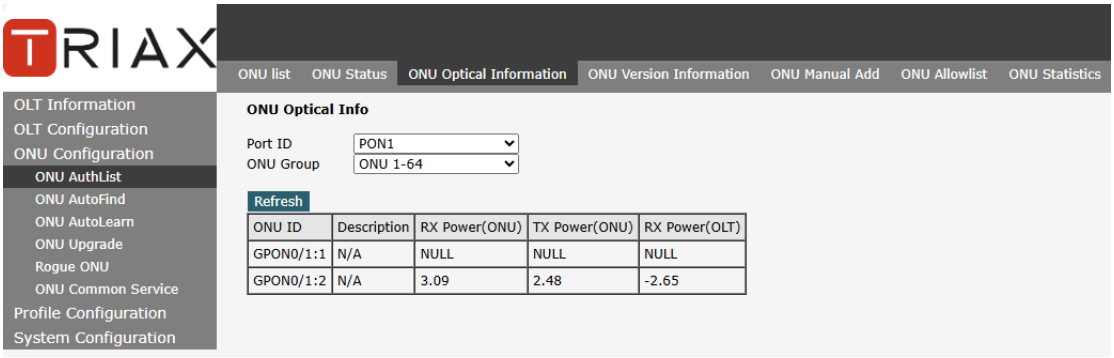


Figure 4.1-26: ONU Optical Info

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.

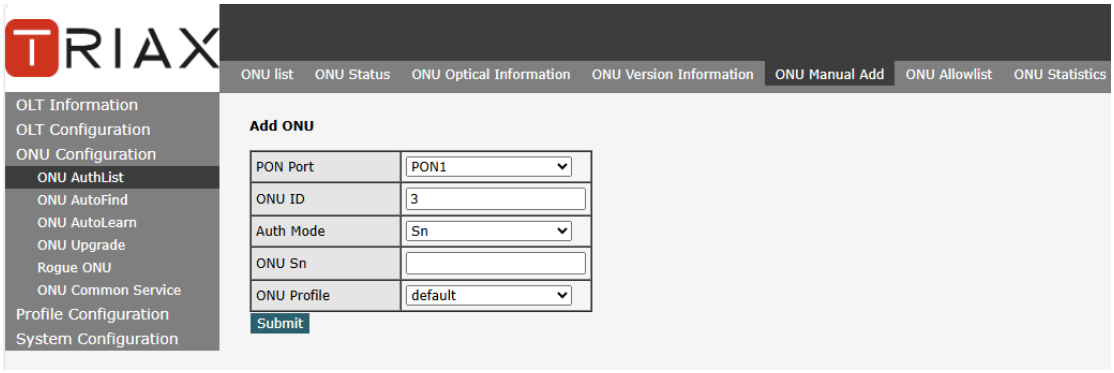


Figure 4.1-27: Add ONU Manually

4.1.5 ONU Allowlist

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.

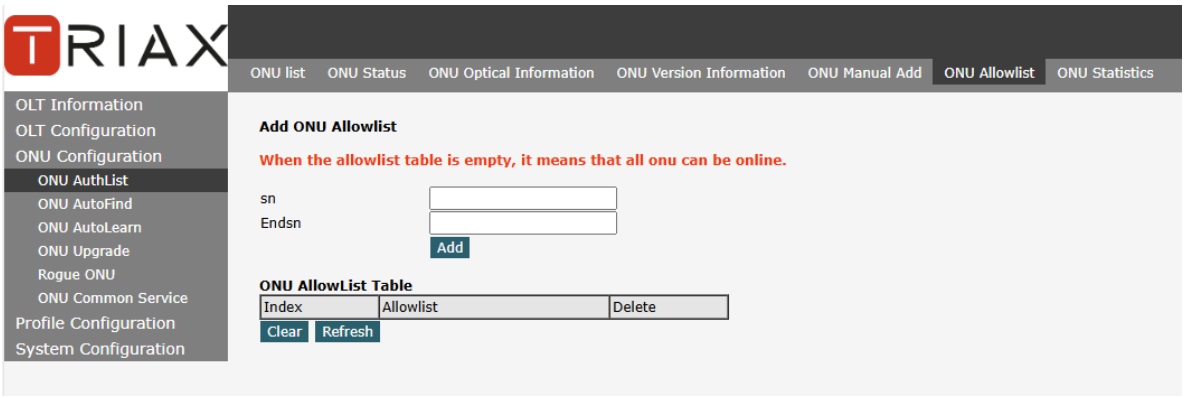


Figure 4.1-28: ONU Whitelist

4.1.6 ONU Statistics

ONU Configuration→ONU AuthList→ONU Statistics

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

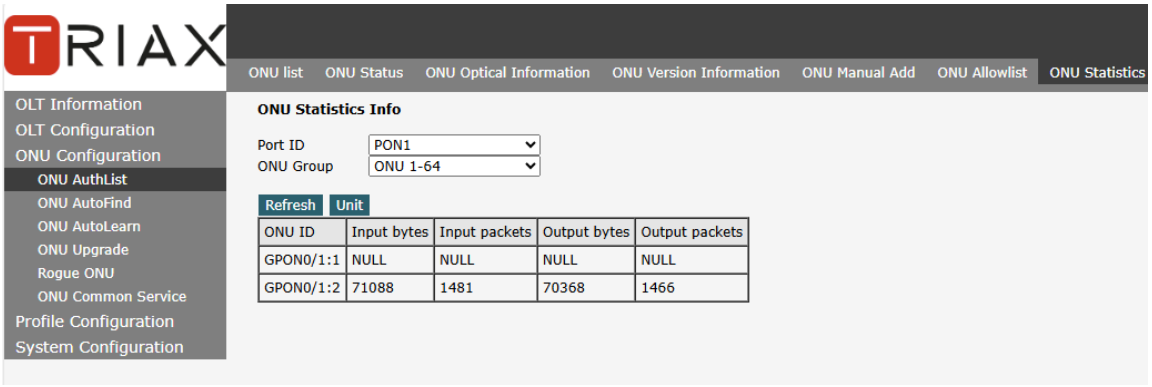


Figure 4.1-29: ONU Statistics

4.2 AutoFind

ONU Configuration→ONU AutoFind

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

More information will be shown under the ONU Detail menu.

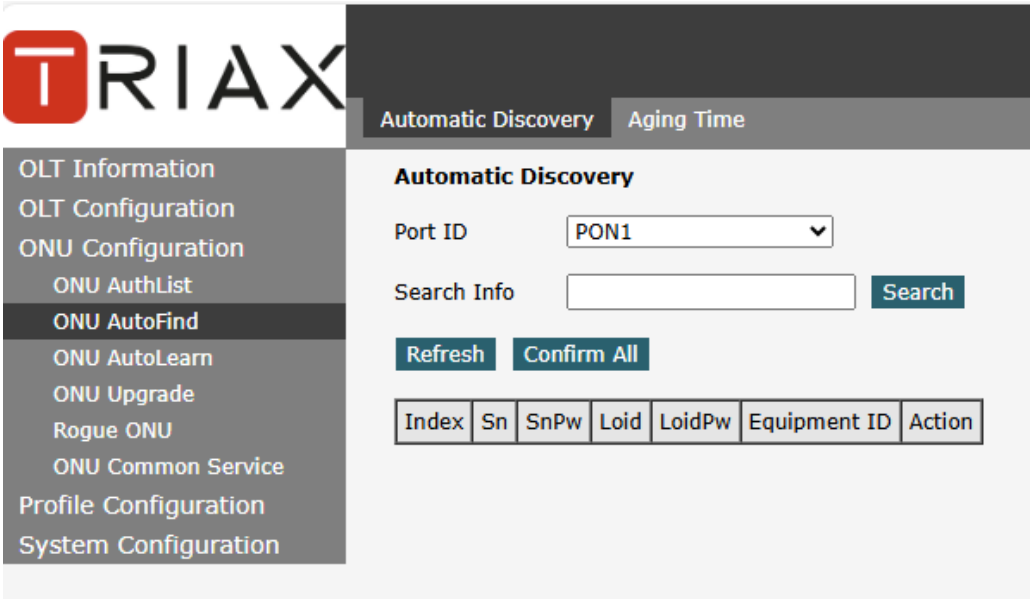


Figure 4.2-1: Automatic Discovery

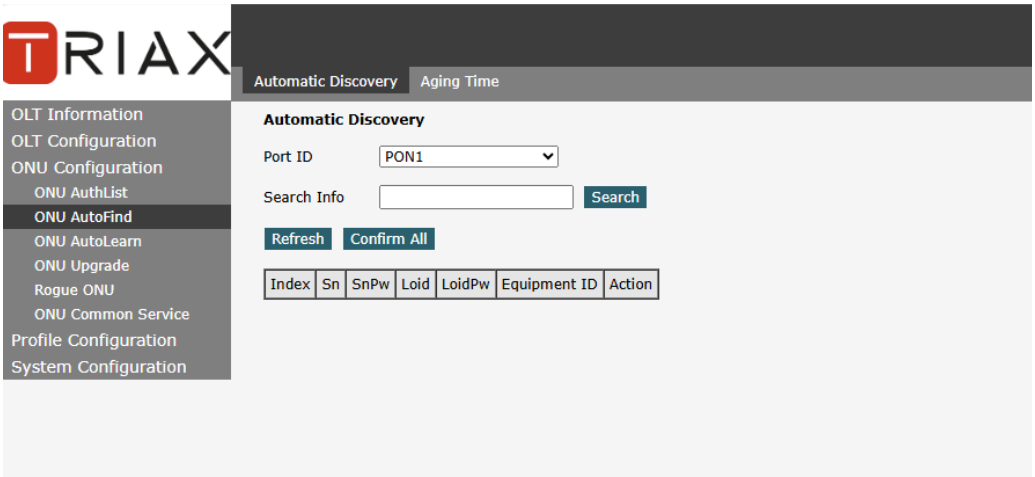


Figure 4.2-2: Detail info

4.3 AutoLearn

4.3.1 ONU AutoLearn

Configuration→AutoLearn→ONU AutoLearn

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

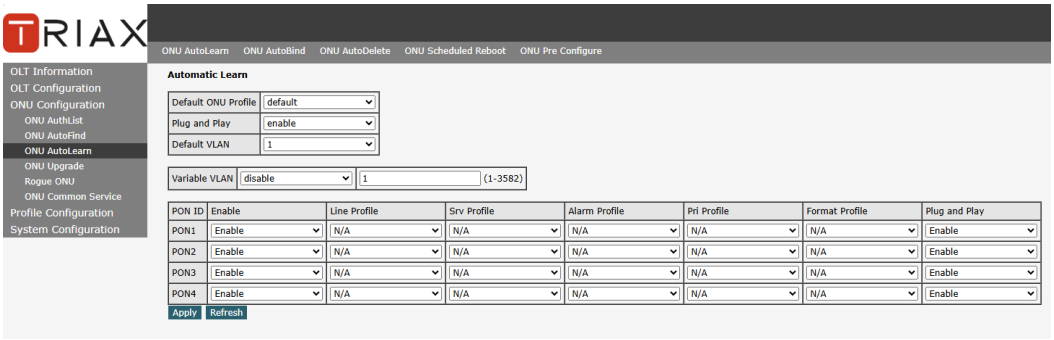


Figure 4.3-1: Automatic learn

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.

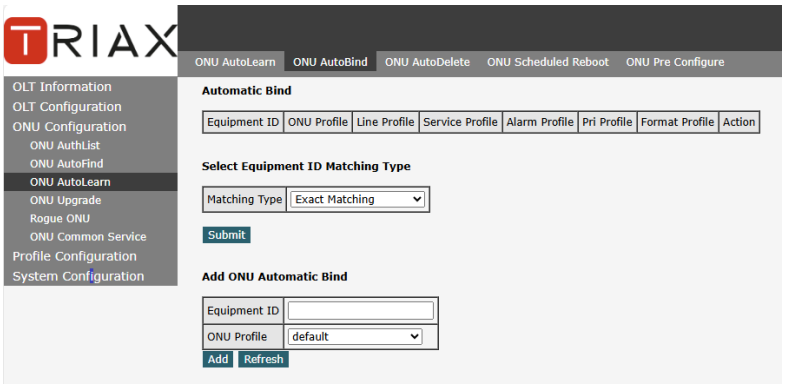


Figure 4.3-2: Bind profile

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.

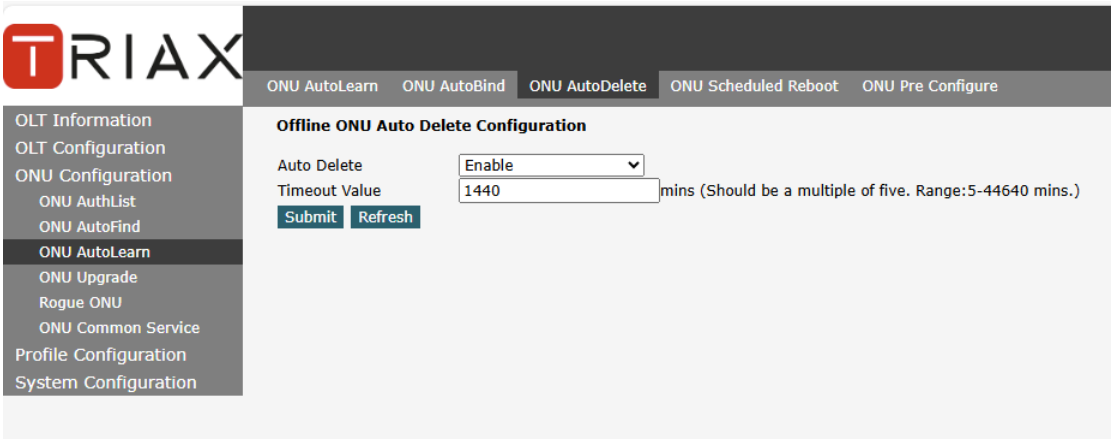


Figure 4.3-3: ONU AutoDelete

4.4 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's RAM.

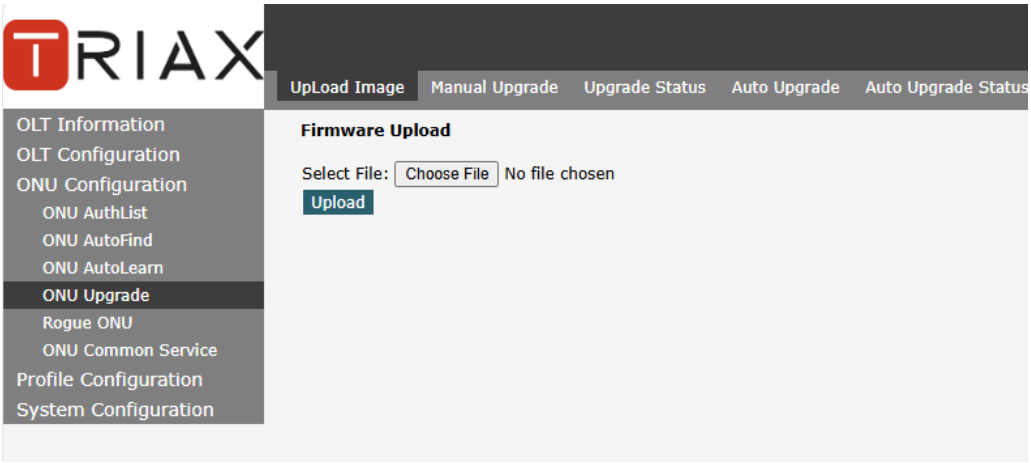


Figure 4.4-1: Upload image

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.

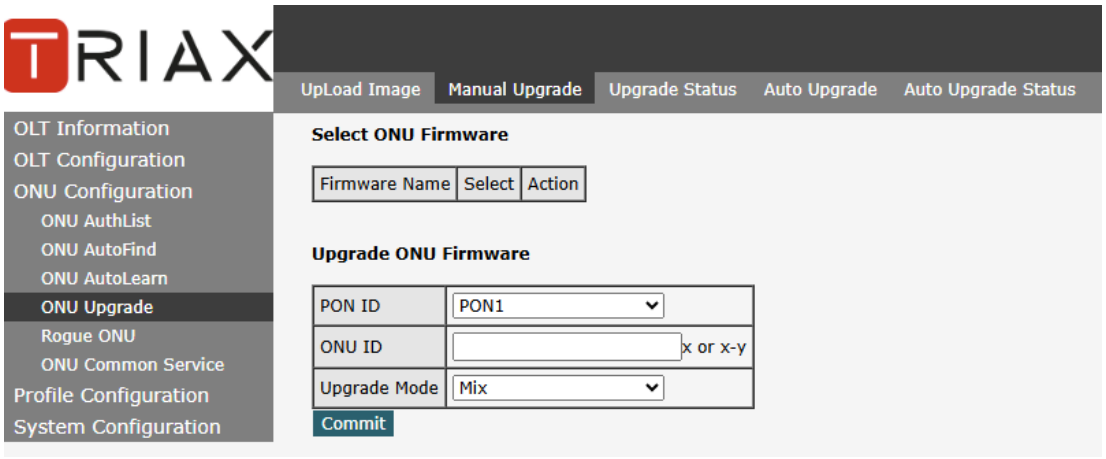


Figure 4.4-2: Manual Upgrade

4.4.3 Upgrade Status

Configuration→ONU Upgrade→Upgrade Status

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

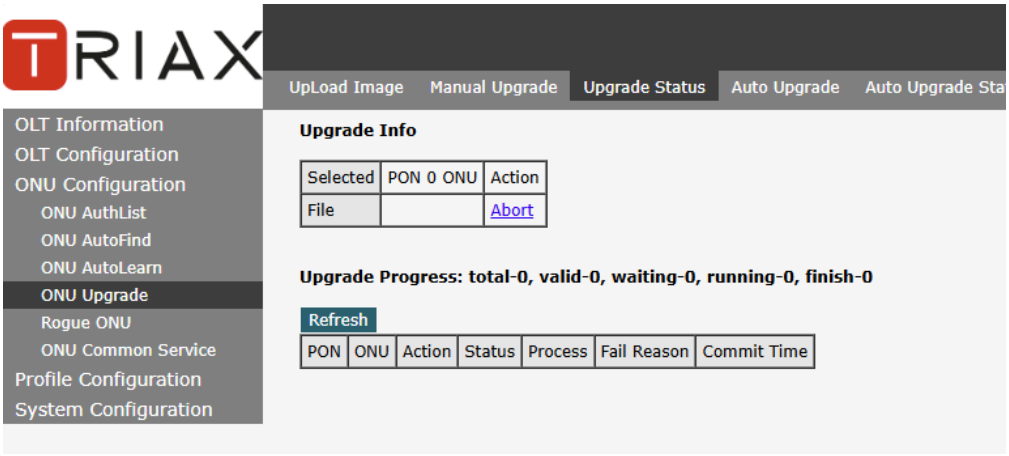


Figure 4.4-3: ONU Upgrade Status

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.

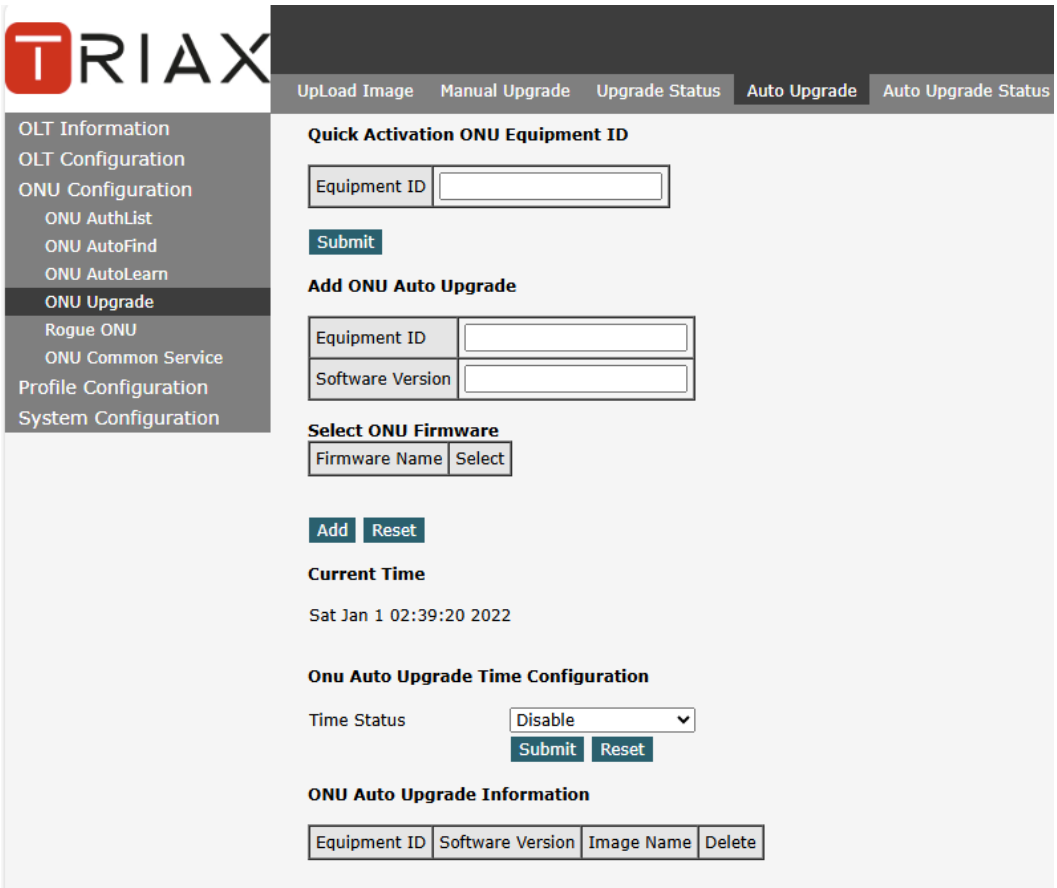


Figure 4.4-4: Auto-Upgrade

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.

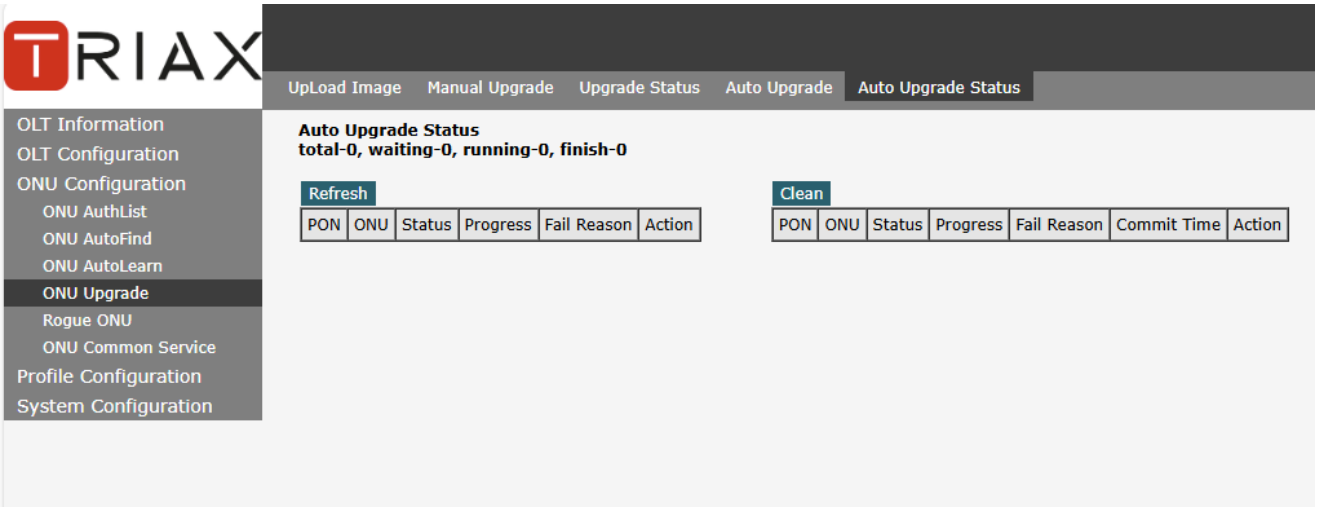


Figure 4.4-5: Auto Upgrade Status

4.5 Rogue ONU

ONU Configuration→Rogue ONU

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

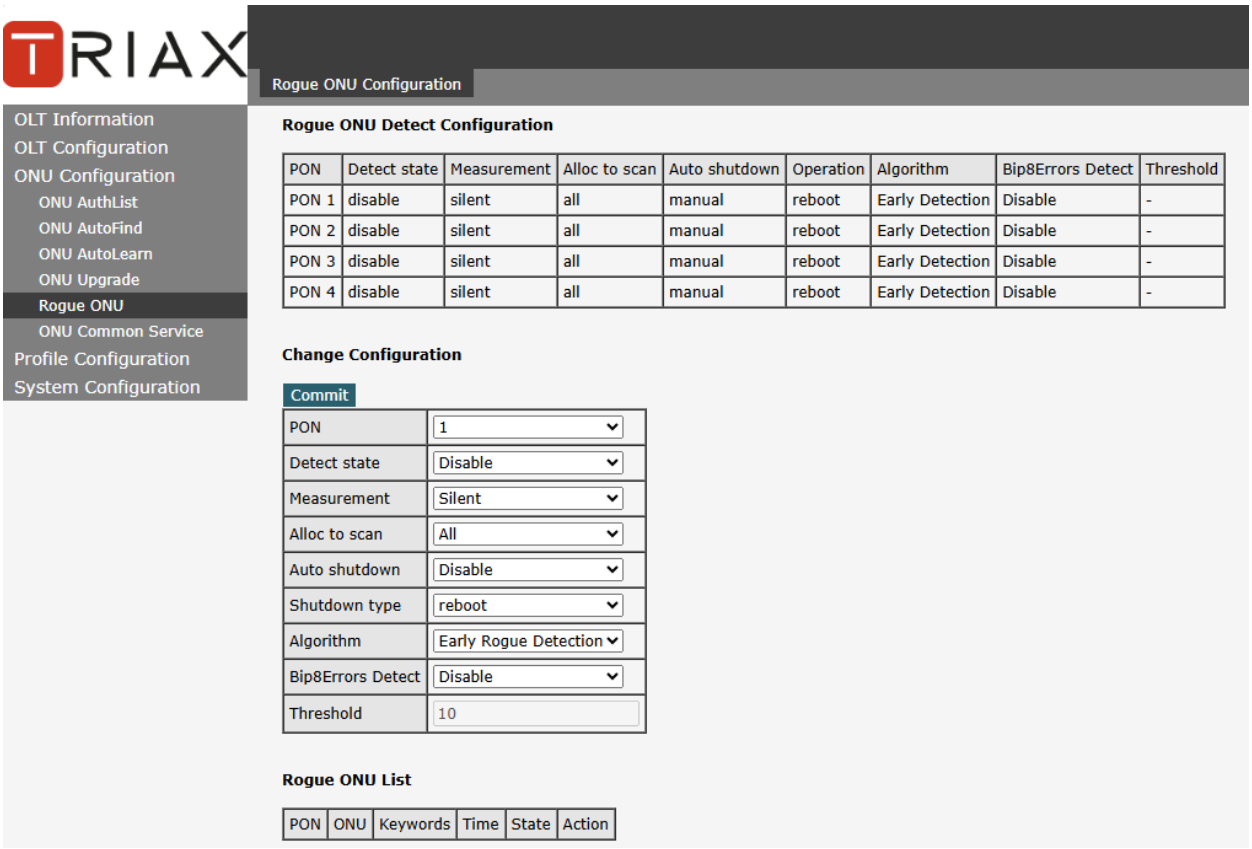


Figure 4.5-1: Rogue ONU detection

4.6 ONU Common Service

Only GPON OLT-B Series supports this feature.

ONU Configuration→ONU Common Service

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

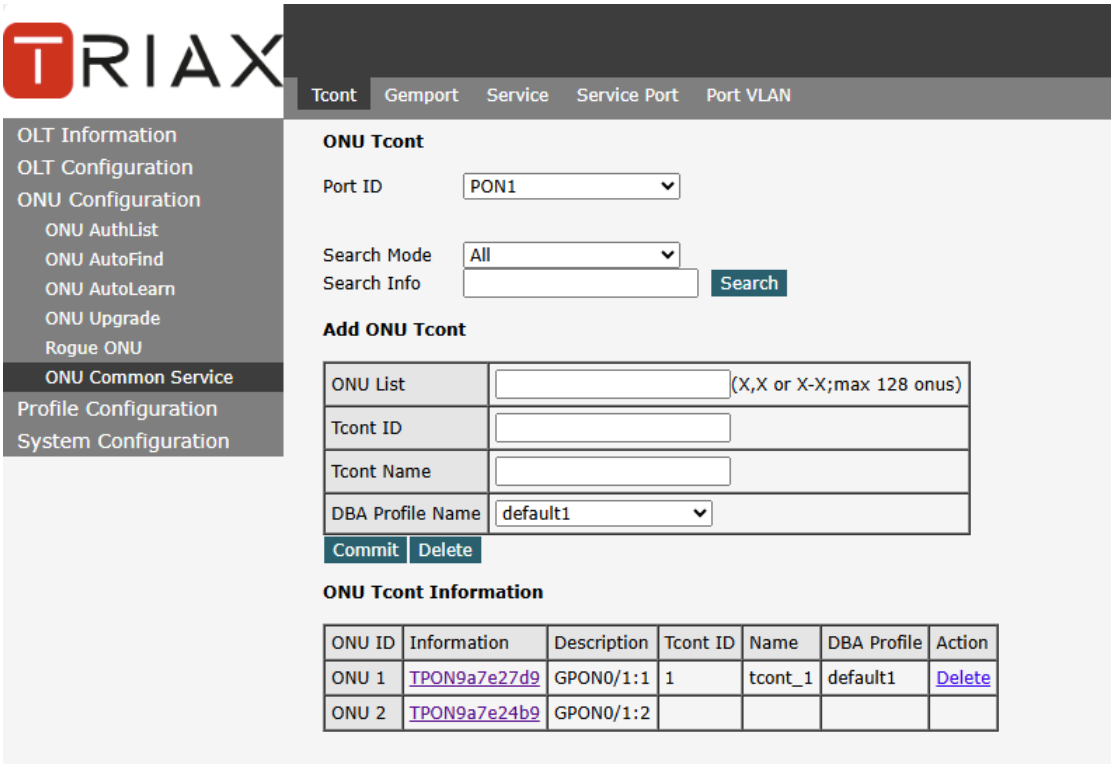


Figure 4.6-1: ONU Common Service

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.

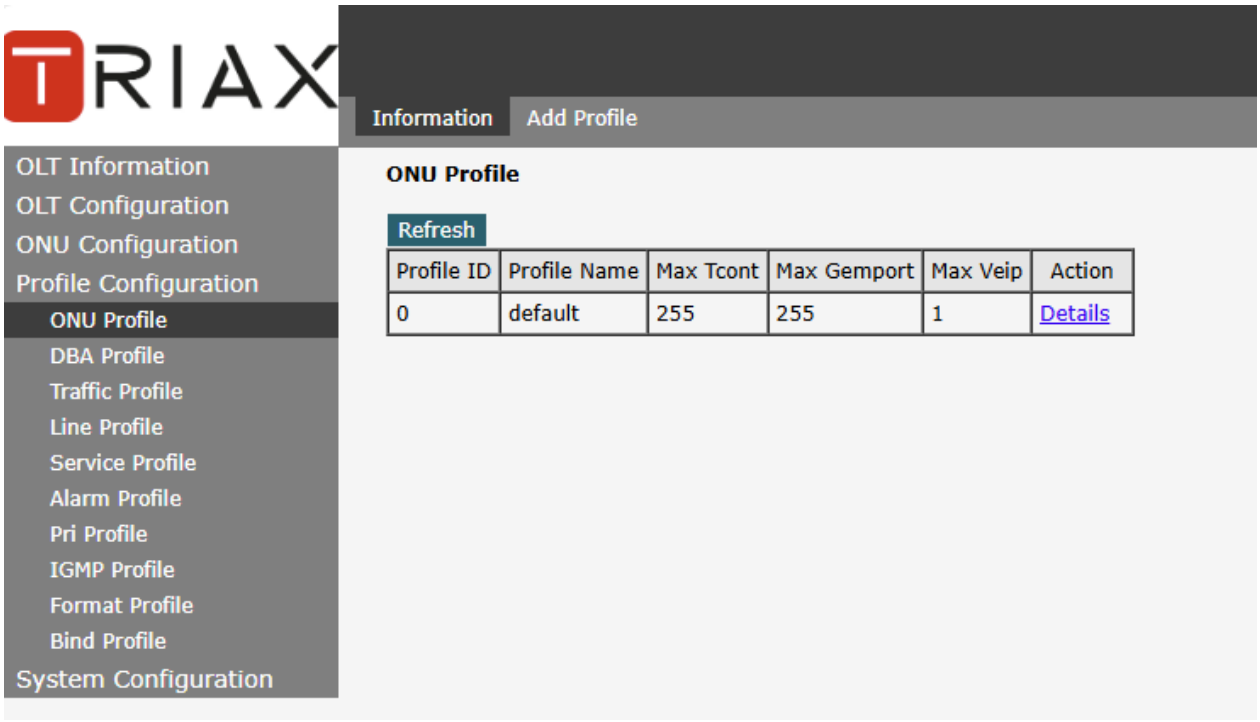


Figure 5.1-1: ONU profile list

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.

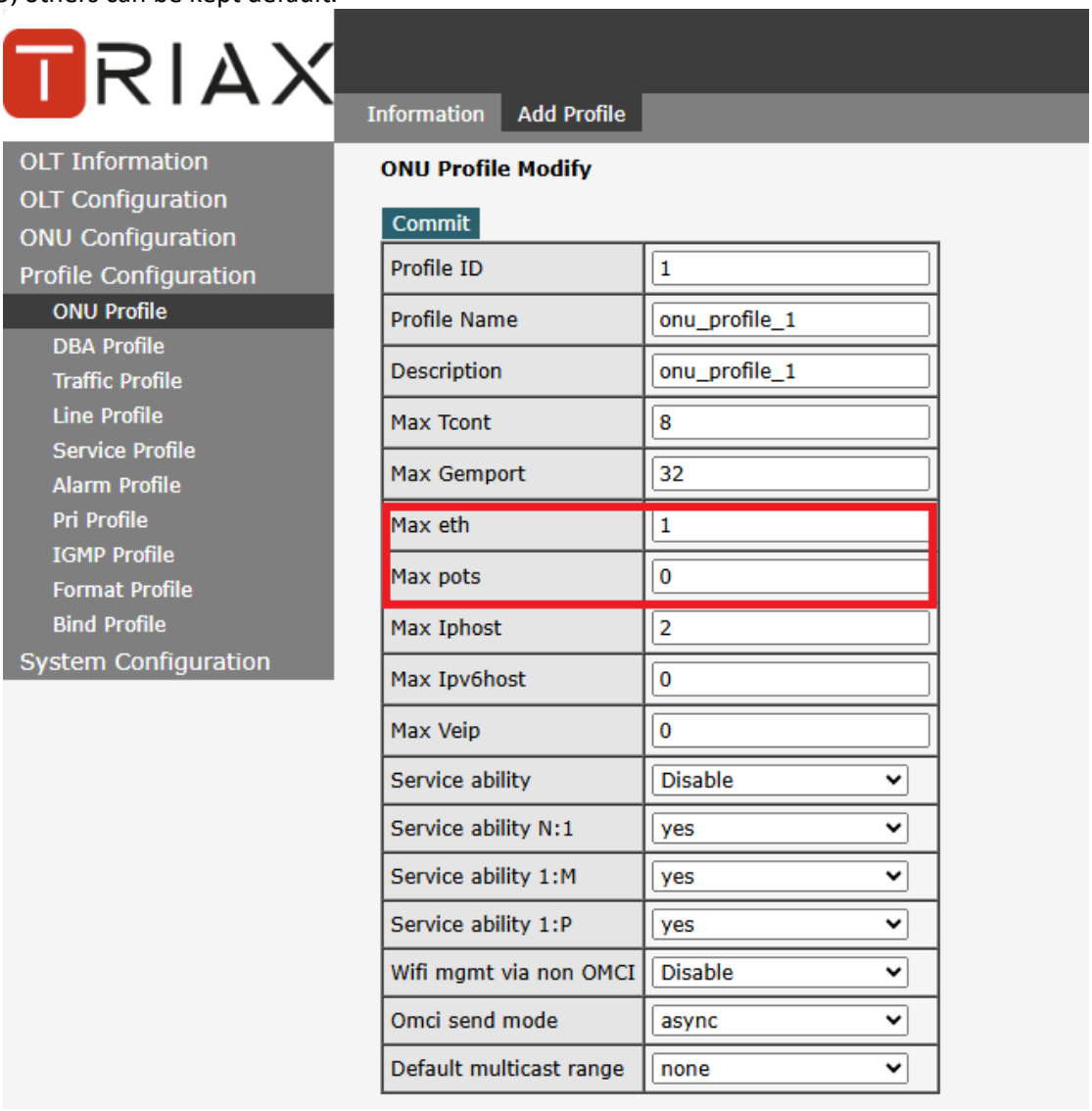


Figure 5.1-2: Add SFU profile

- 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.

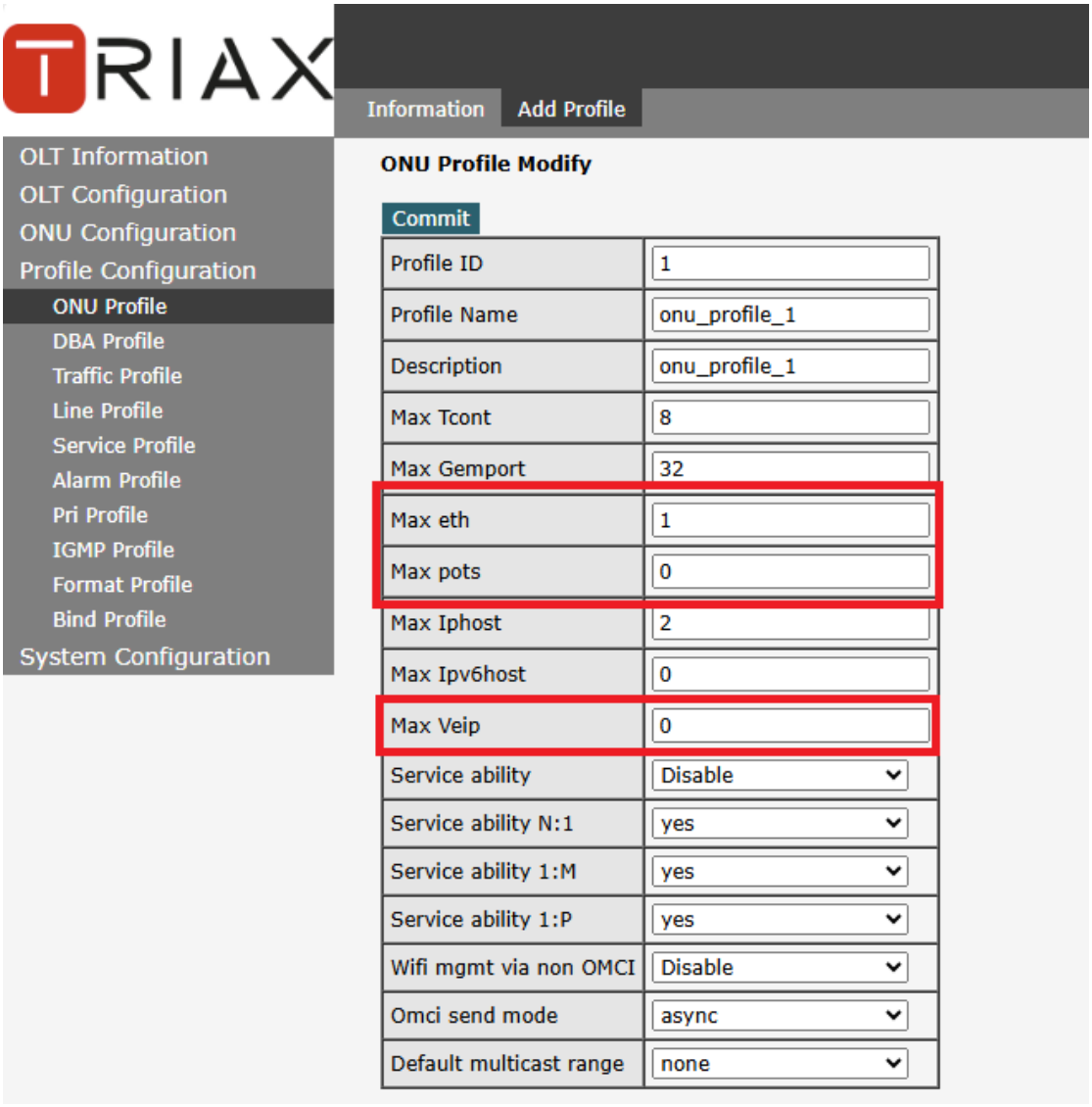


Figure 5.1-3: Add HGU profile

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.

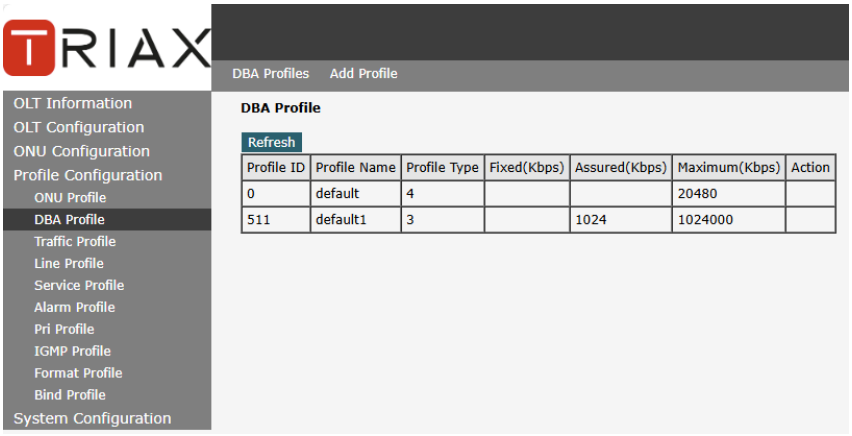


Figure 5.2-1: DBA profile list

5.2.2 Add profile

Profile Configuration→DBA Profile → Add profile

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

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

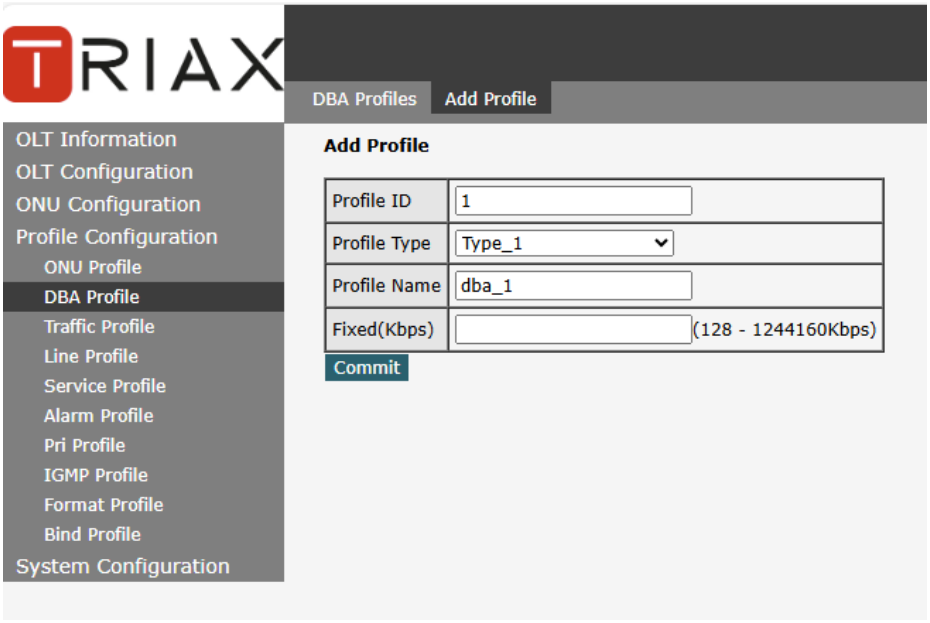


Figure 5.2-2: Add a DBA profile

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.

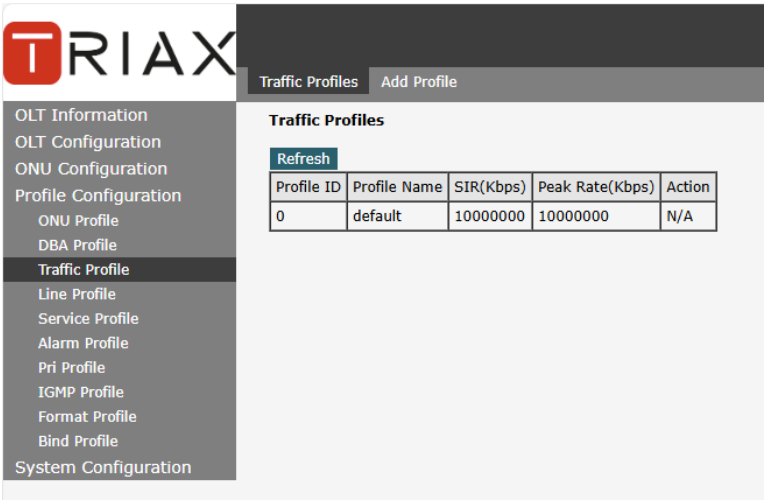


Figure 5.3-1: Traffic Profile list

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

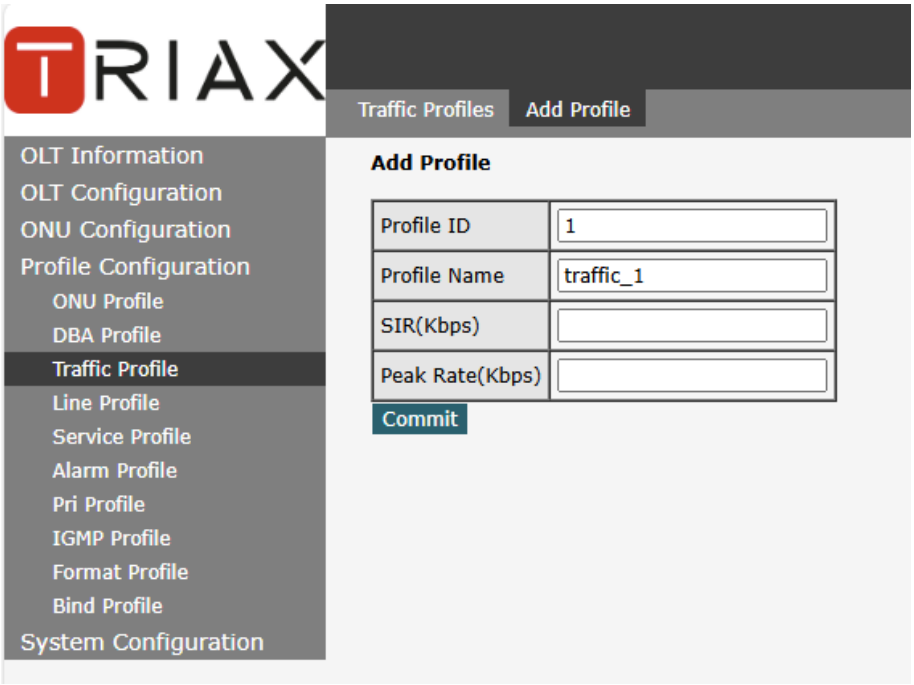


Figure 5.3-2: Add a traffic Profile

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.

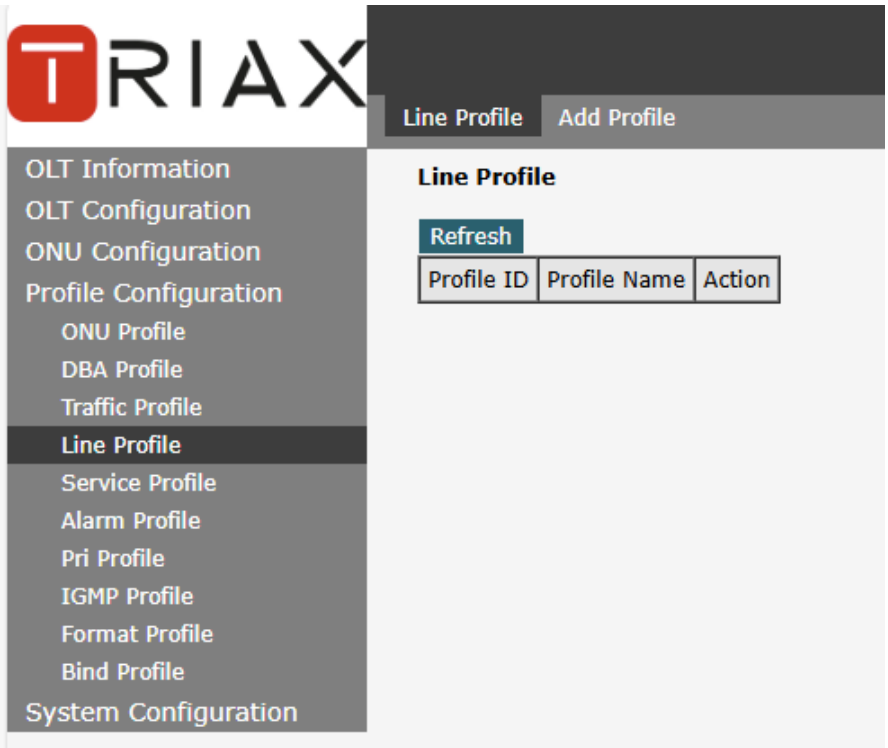


Figure 5.4-1: Line Profile list

5.4.2 Add profile

Profile Configuration→Line profile→Add profile

Create a new line profile.

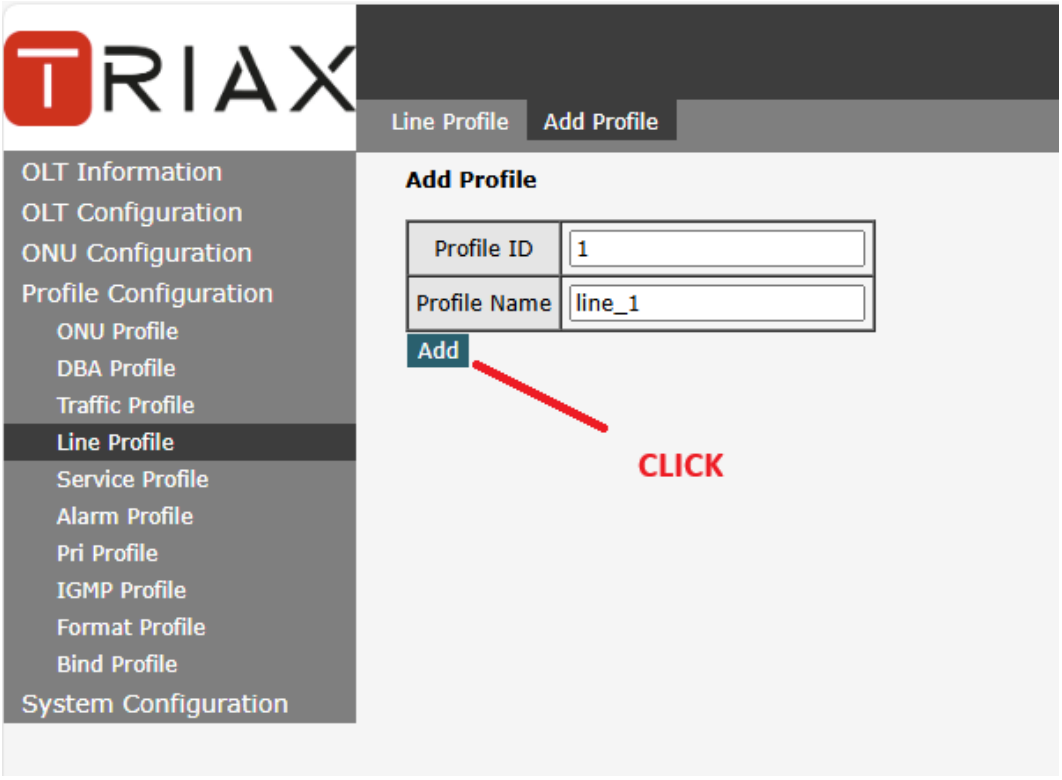


Figure 5.4-2: Add Line Profile

Modify the line profile parameters.

Figure 5.4-3: Modify Line Profile

5.4.2.1 Tcont

Add tcont ID and bind DBA profile.

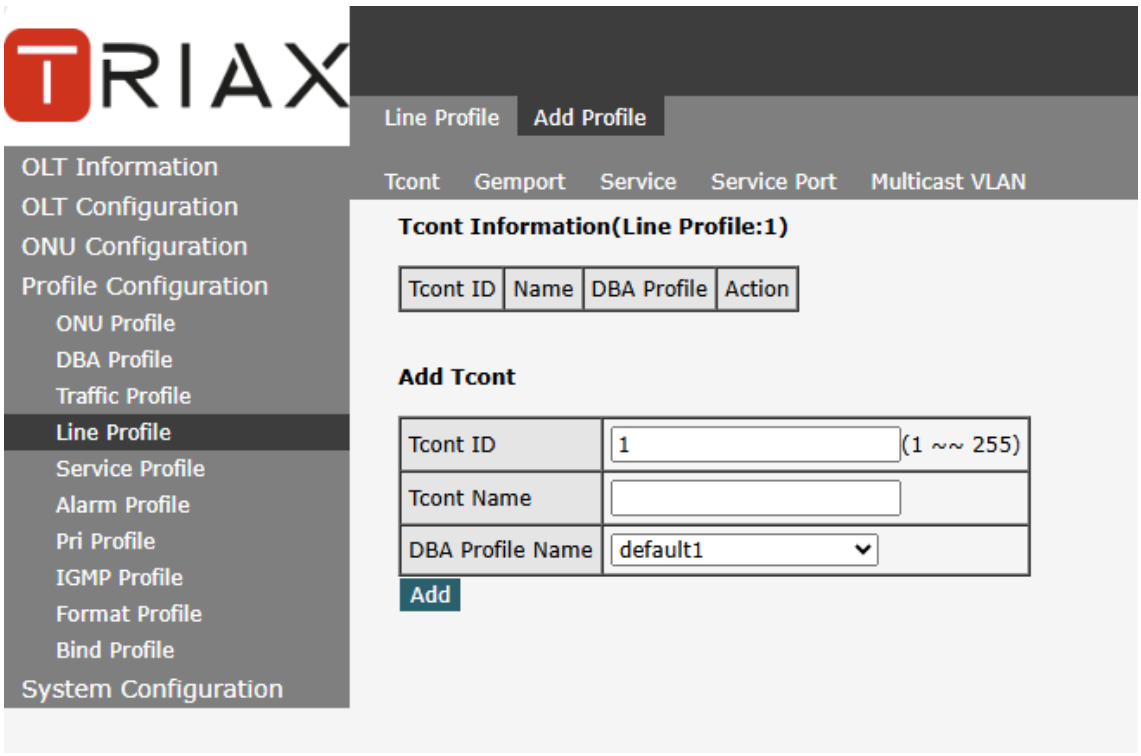


Figure 5.4-4: Add Tcont

5.4.2.2 Gemport

Add gemport ID and bind tcont ID.

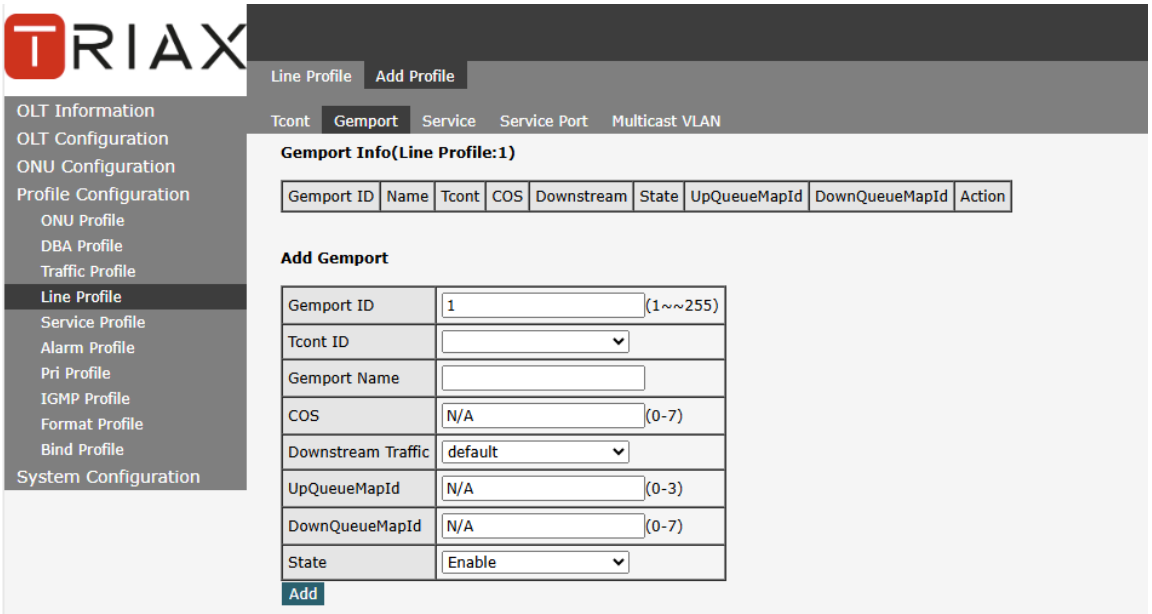


Figure 5.4-5: Add Gemport

5.4.2.3 Service

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

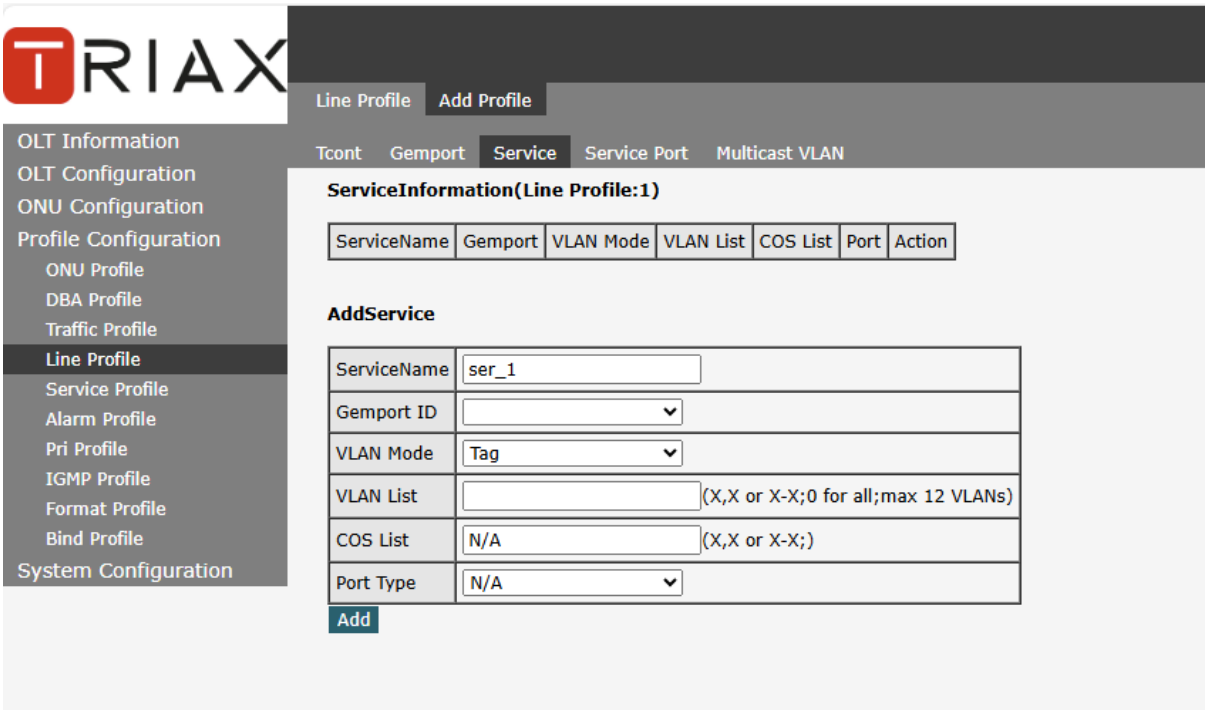


Figure 5.4-6: Add Service

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.

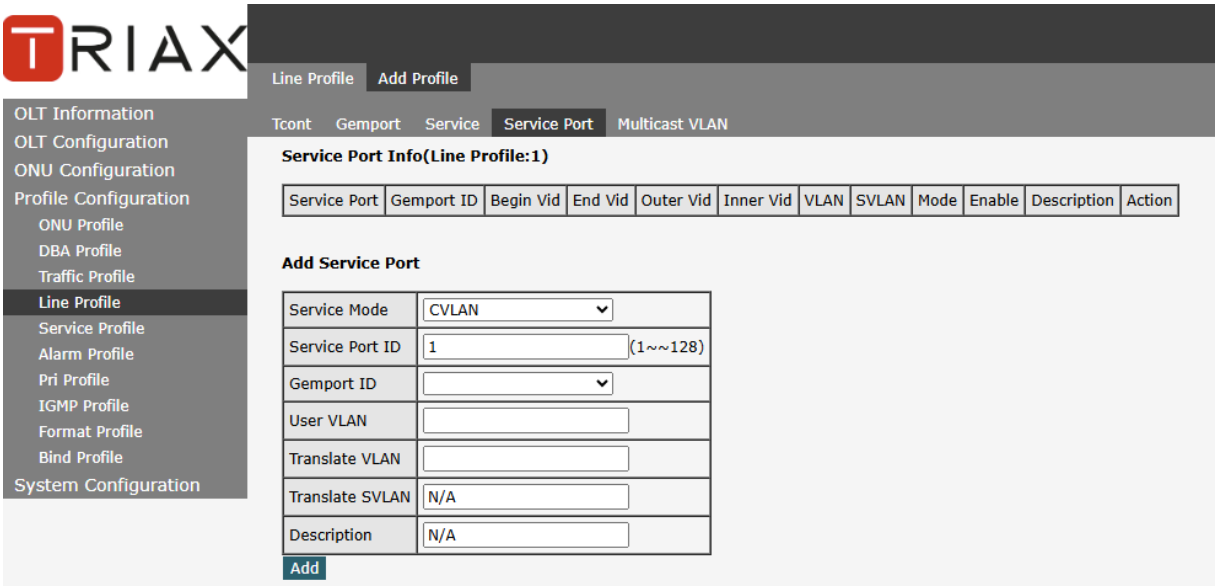


Figure 5.4-7: Add Service Port

5.4.2.5 Multicast Vlan

Set the Multicast VLAN of ONU.

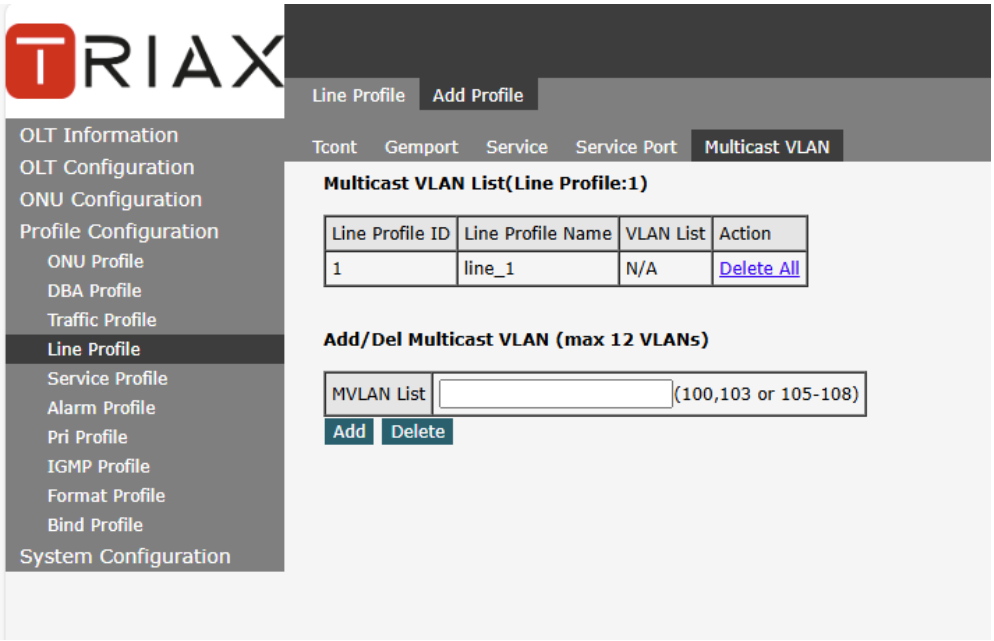


Figure 5.4-8: Configure Multicast VLAN

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.

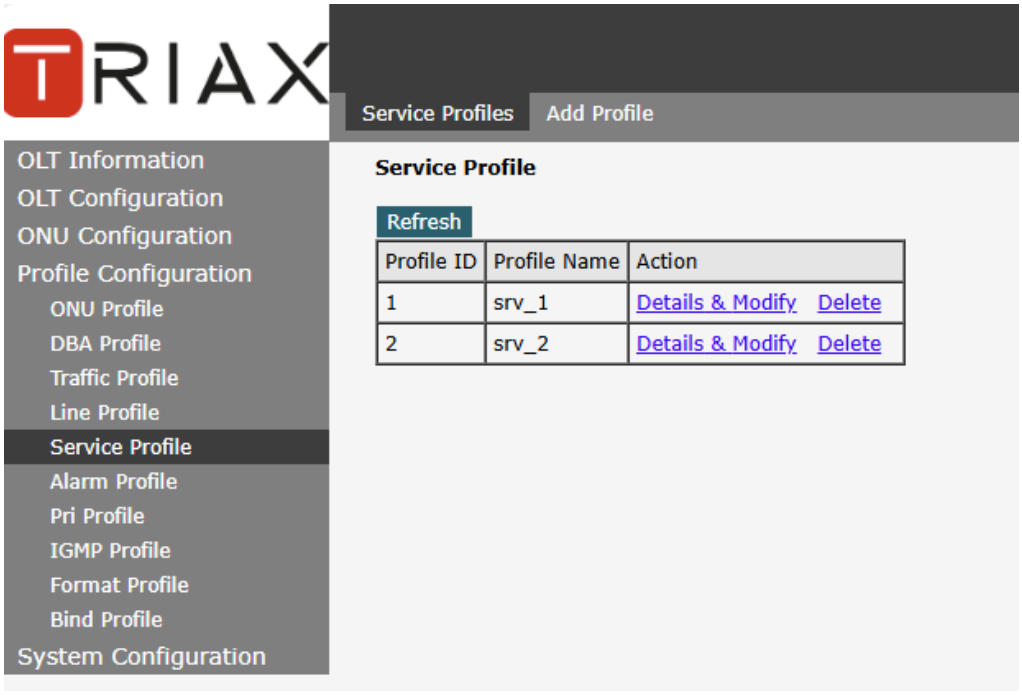


Figure 5.5-1: Service Profile List

5.5.2 5.5.2 Add profile

Profile Configuration→Service Profile →Add Profile

Add a new service profile.

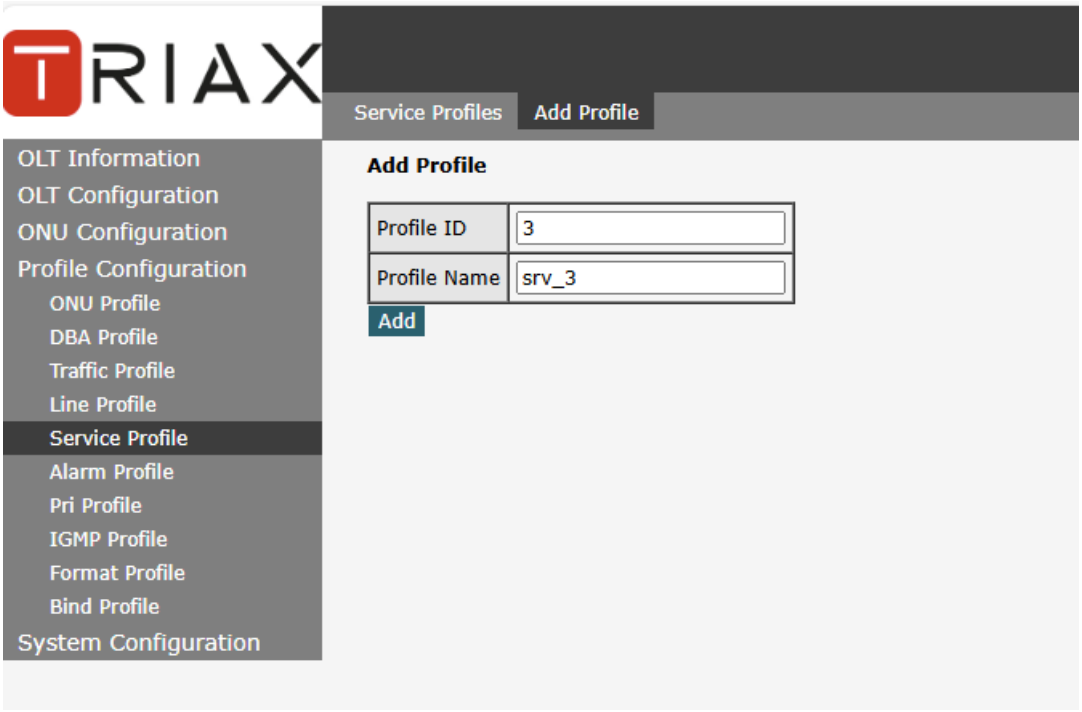


Figure 5.5-2: Add Service profile

Figure 5.5-3: Modify Service Profile

5.5.2.1 PortVlan

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

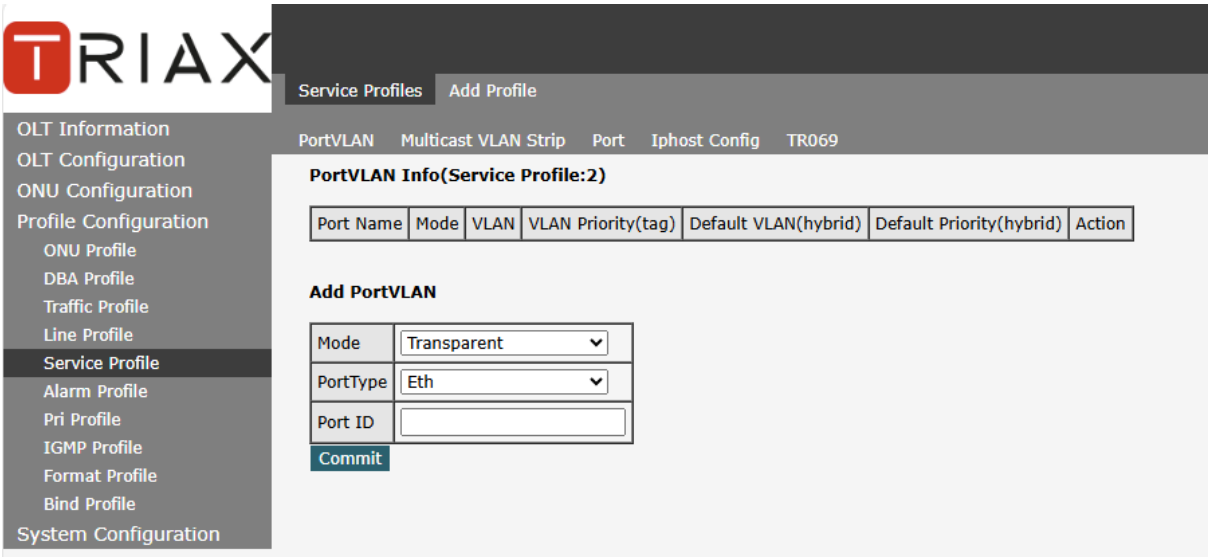


Figure 5.5-4: Port VLAN mode

5.5.2.2 Multicast Vlan Strip

Set the multicast VLAN mode of ONU's port.

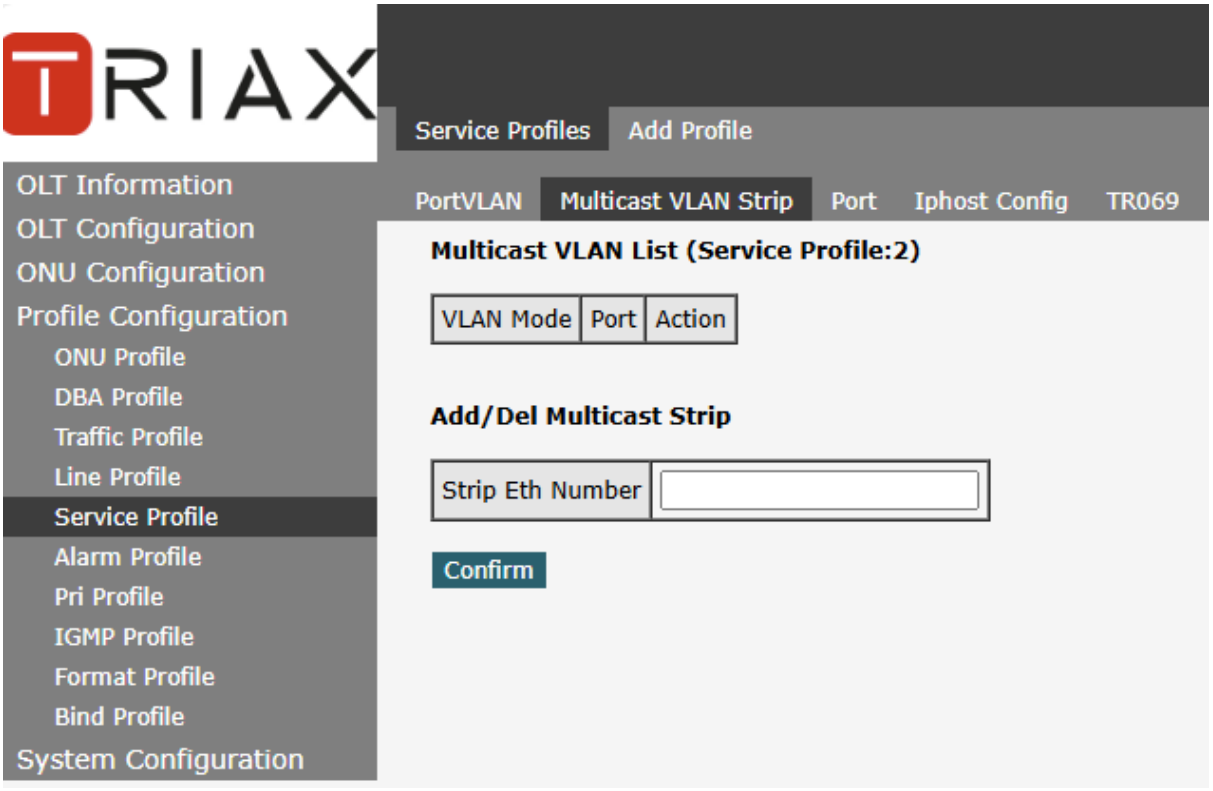


Figure 5.5-5: Port Multicast VLAN Mode

5.5.2.3 Iphost Config

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

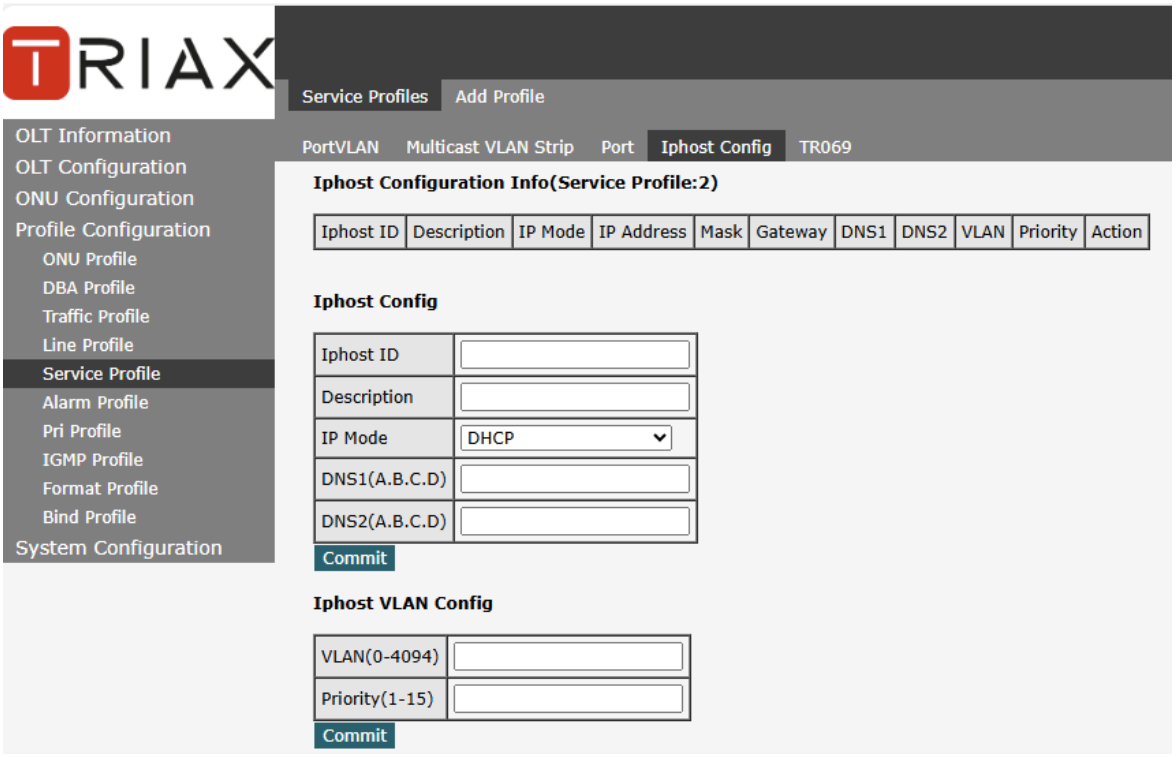


Figure 5.5-6: Add IPhost

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.

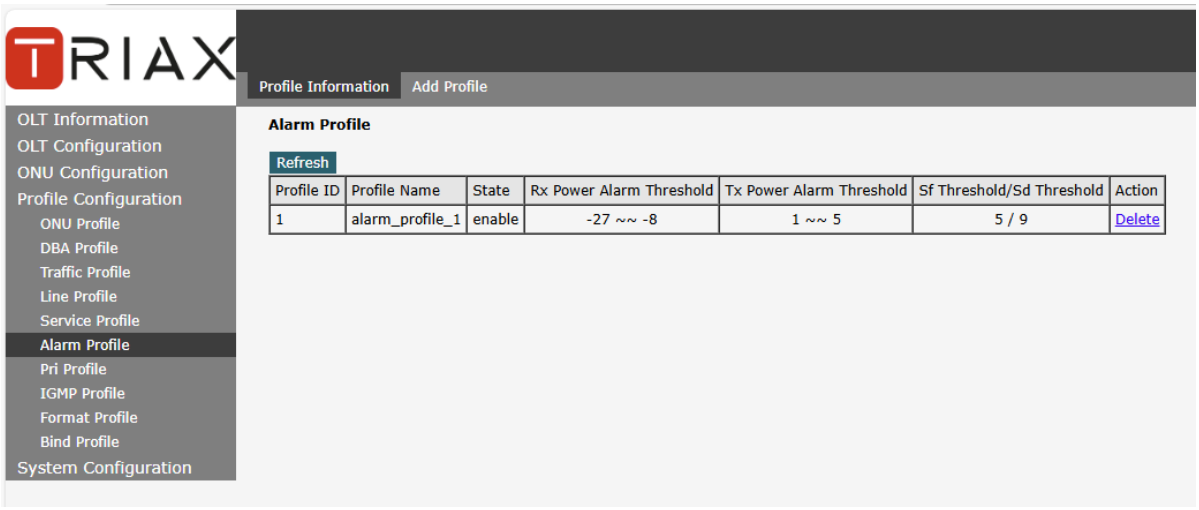


Figure 5.6-1: Alarm Profile List

5.6.2 Add Profile

Profile Configuration→Alarm Profile →Add profile

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

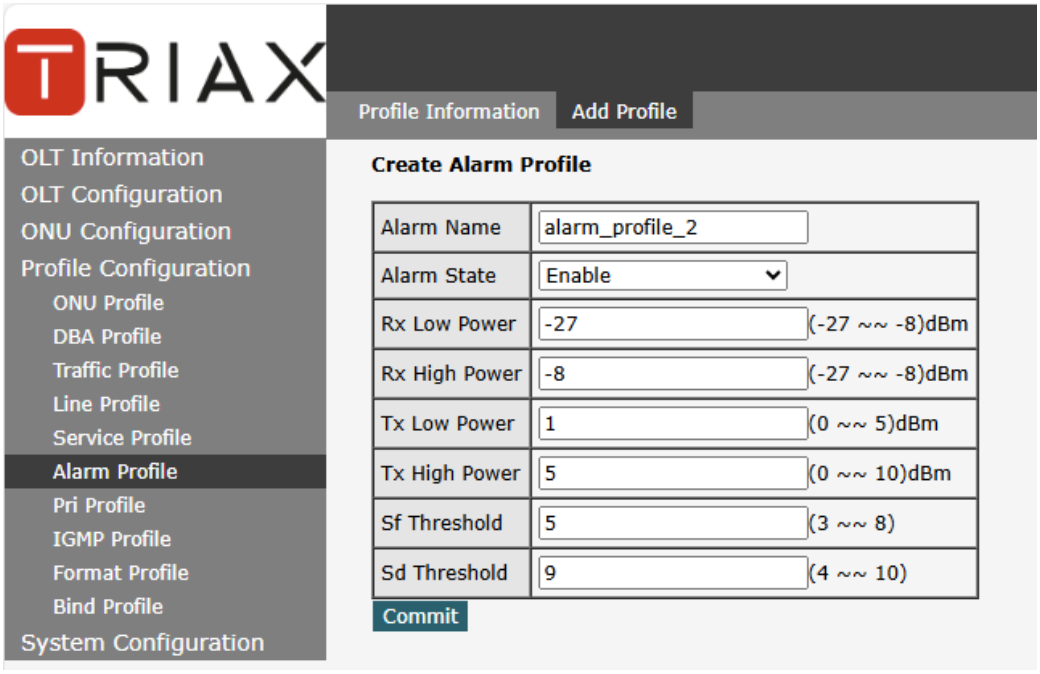


Figure 5.6-2: Add Alarm Profile

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.

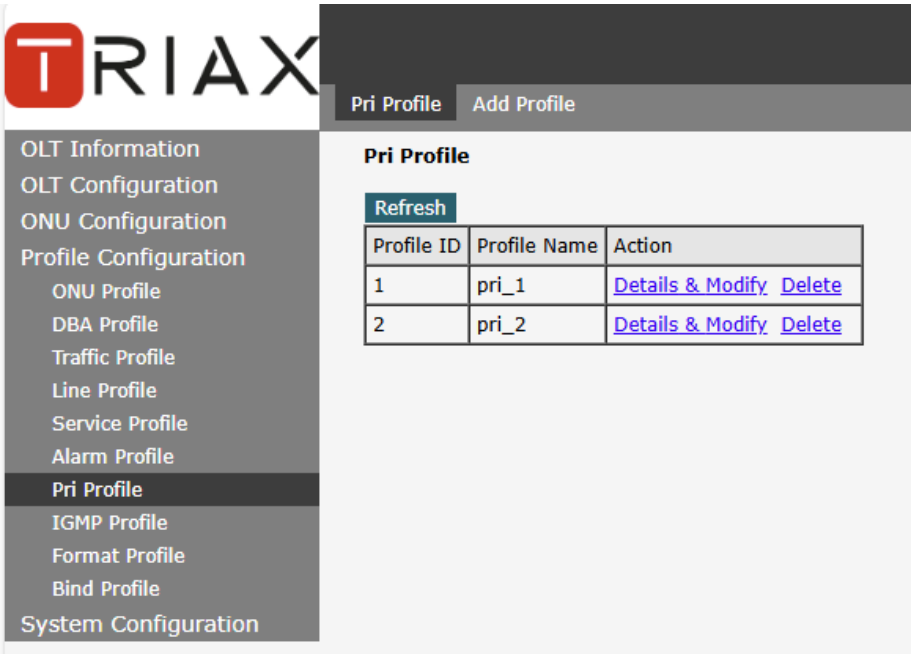


Figure 5.7-1: Pri Profile

5.7.2 Add Profile

Profile Configuration→Pri Profile →Add profile

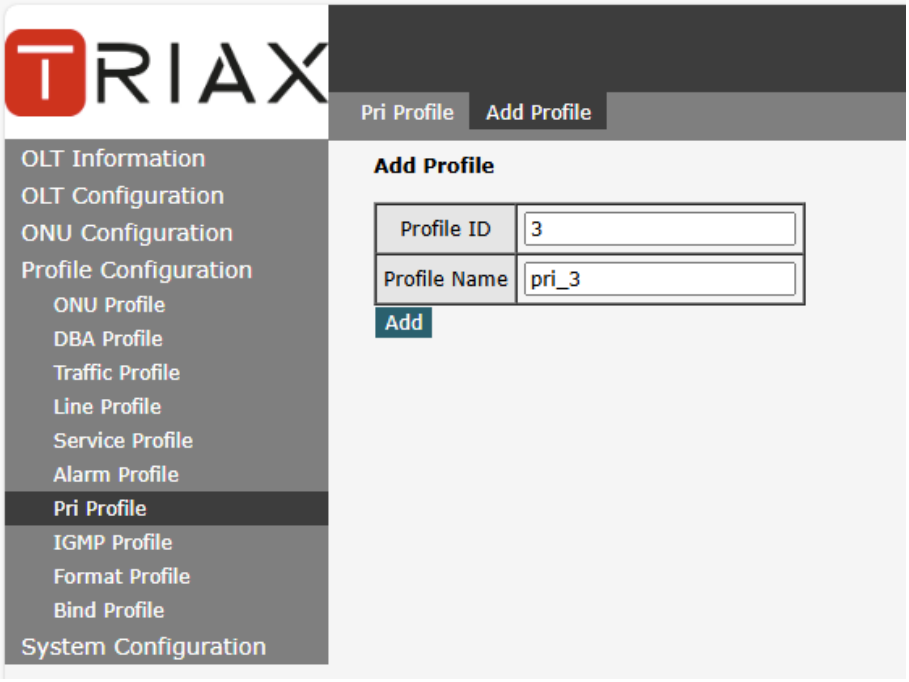


Figure 5.7-2: Add Private Profile

5.8 Bind Profile

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

Profile Configuration→Bind Profile

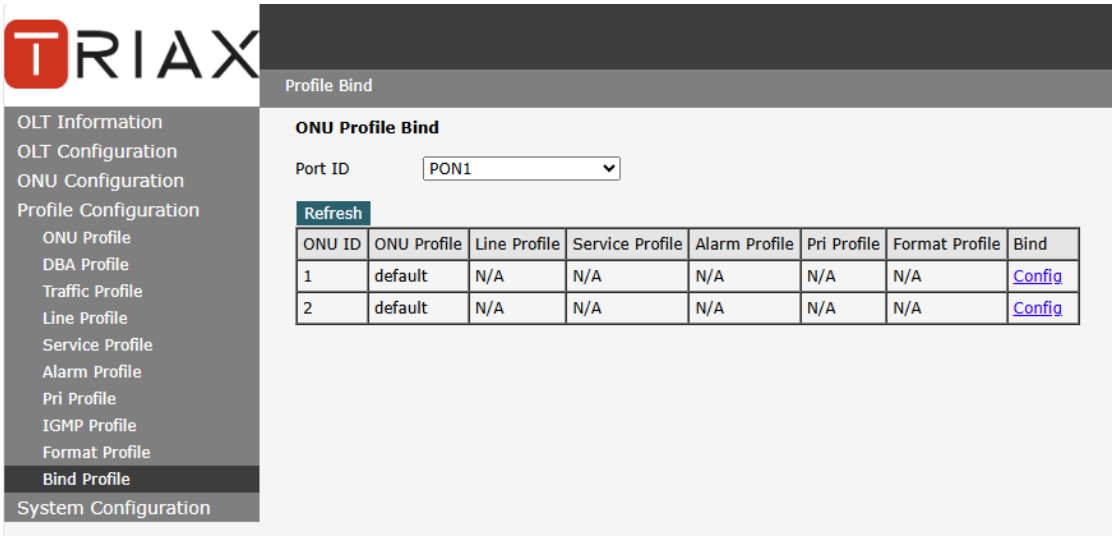


Figure 5.8-1: Bind profile

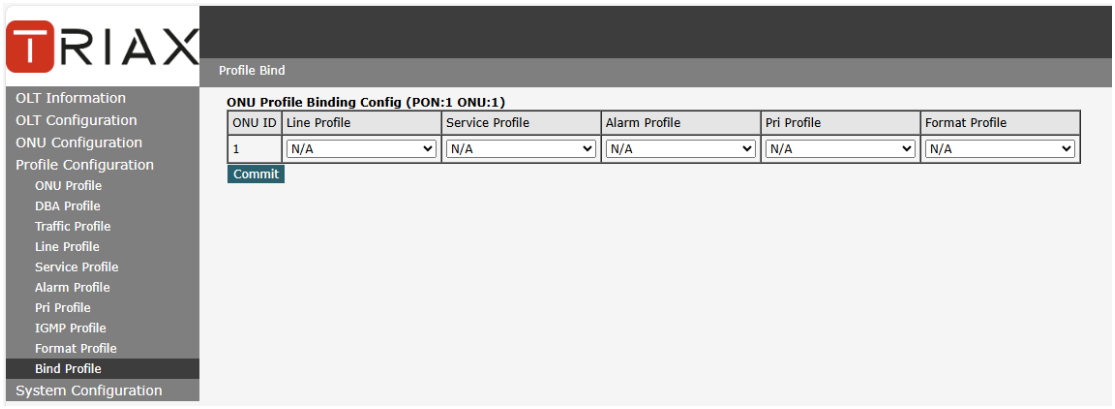


Figure 5.8-2: Select Profile

5.9 IGMP Profile

5.9.1 IGMP Profile

Profile Configuration→IGMP Profile→IGMP Profile

An IGMP Profile defines the multicast settings that will be applied to ports or VLANs for IPTV services. It controls how the OLT handles IGMP (Internet Group Management Protocol) messages from subscribers and how multicast streams are delivered.

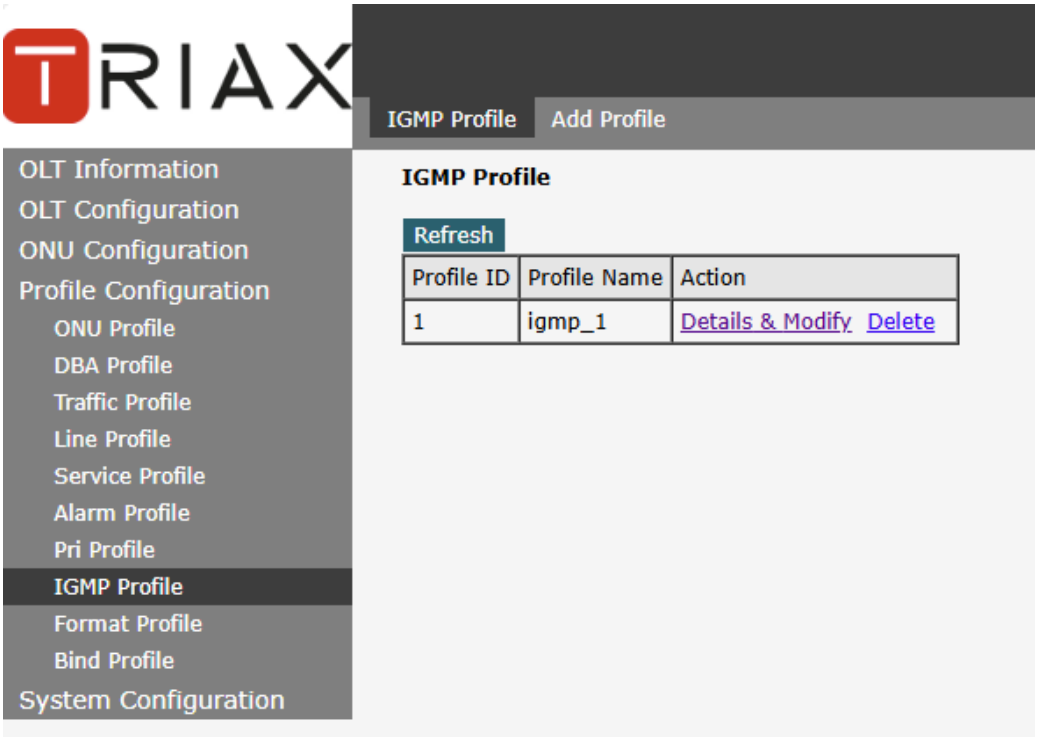


Figure 5.9.1: IGMP Profile

5.9.2 Add Profile

Profile Configuration→IGMP Profile→Add Profile

The IGMP profile sets how multicast IPTV traffic is handled. You can choose the IGMP version, mode (Snooping/Proxy), Fast Leave, upstream/downstream tag handling, rate limits, robustness, proxy IP, query intervals, and how unmatched multicast groups are treated. These settings control stream delivery, channel switching, and network efficiency.

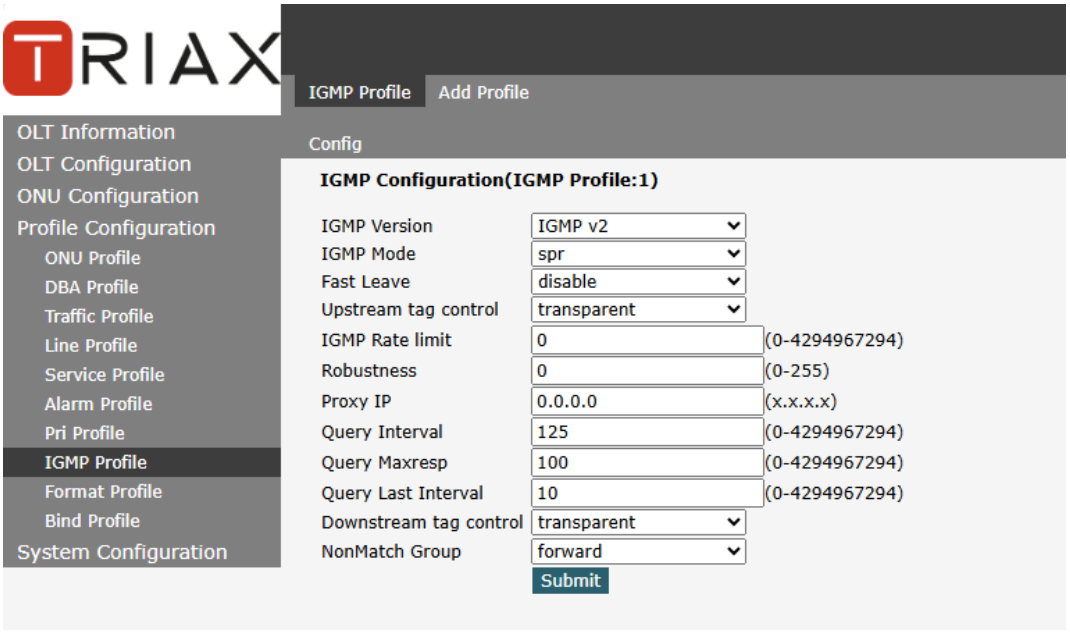


Figure 5.9.2: IGMP Add Profile

5.10 Format Profile

The Format Profile defines how subscriber information is inserted into DHCP, PPPoE, or other packets for identification and management.

5.10.1 Format Profile

Profile Configuration→Format Profile→Format Profile

The Format Profile defines how subscriber information is inserted into DHCP, PPPoE, or other packets for identification and management.

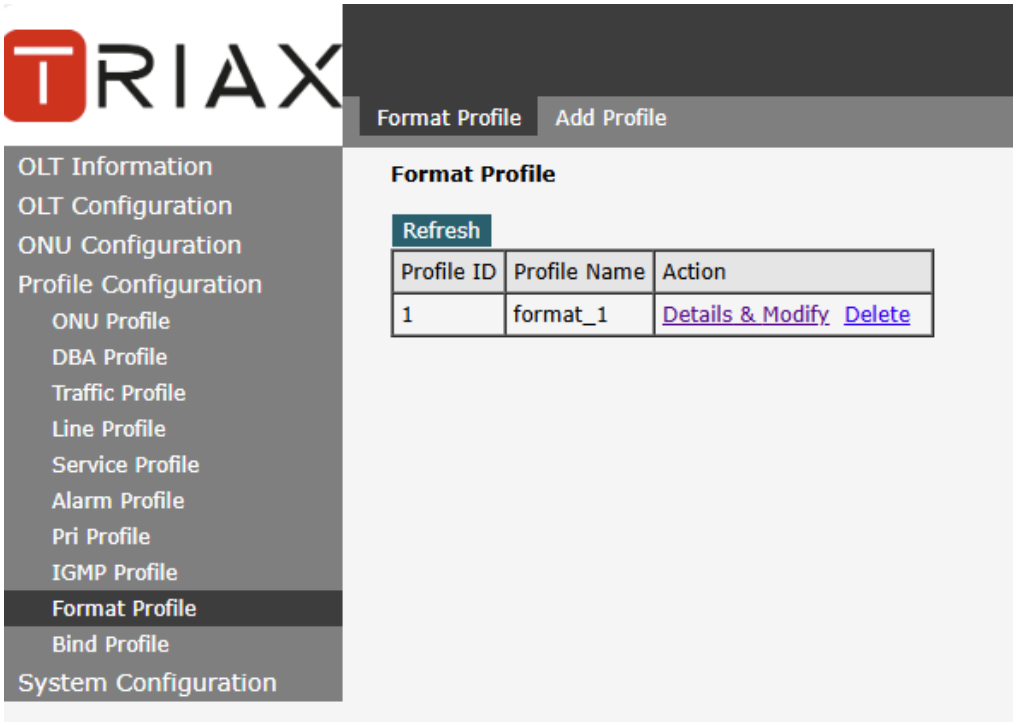


Figure 5.10.1: Format Profile

5.10.2 Add Profile

Profile Configuration→ Format Profile→Add Profile

The Format Profile defines how subscriber information is added to packets for identification. You can enable/disable options like Option82, Option18, Option37, or PPPoE Plus, choose a format type (custom), and configure Circuit ID/Remote ID (e.g., CVLAN) to track subscribers accurately.

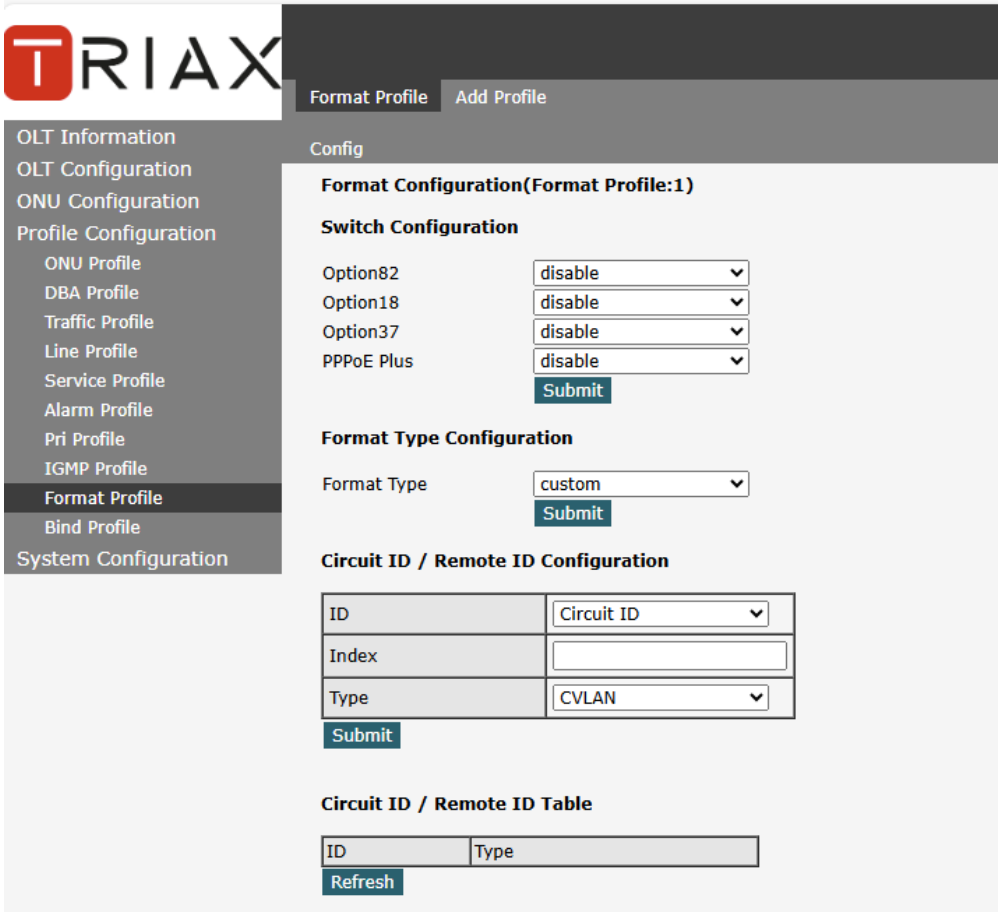


Figure 5.10.2: Format Add Profile

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.

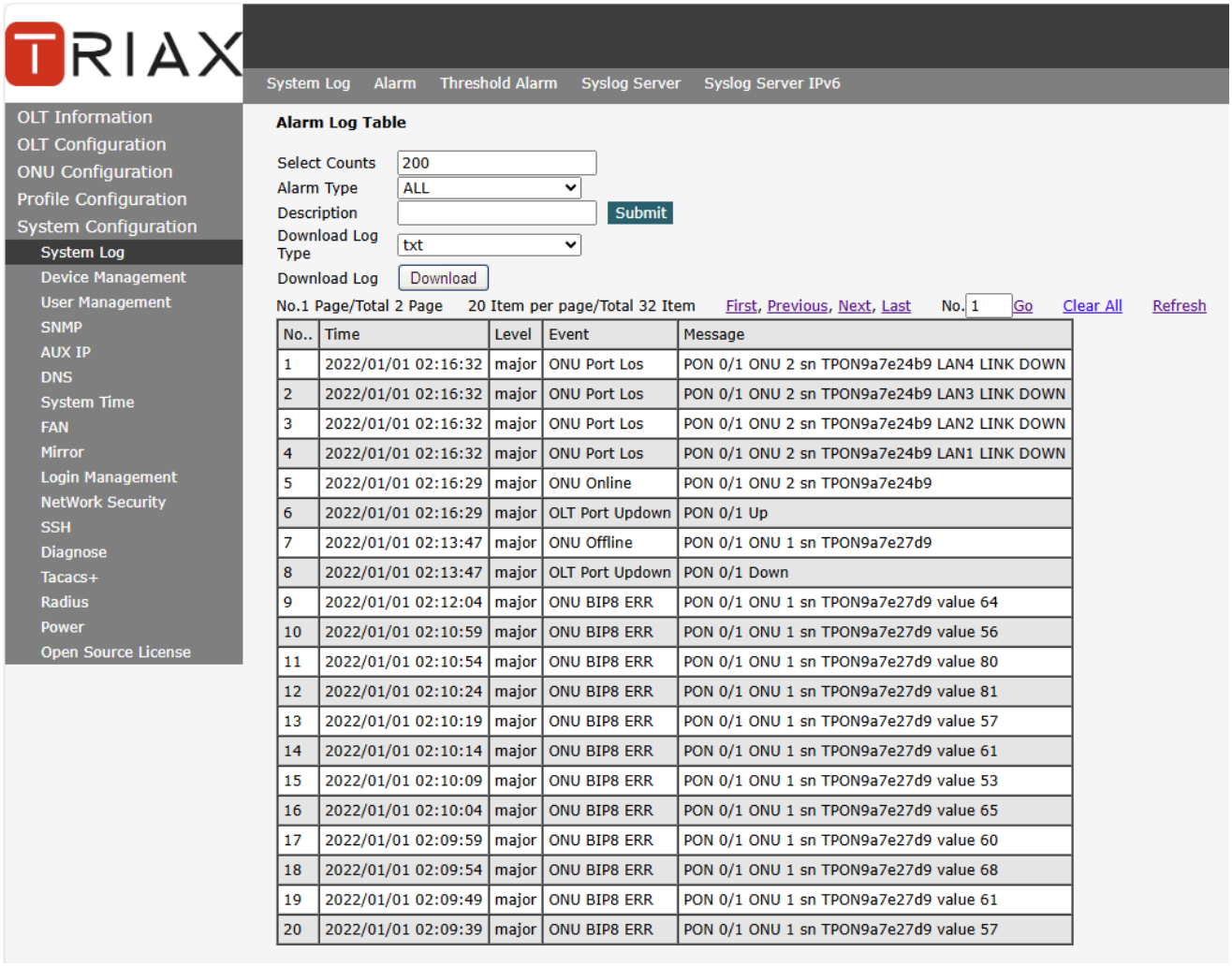
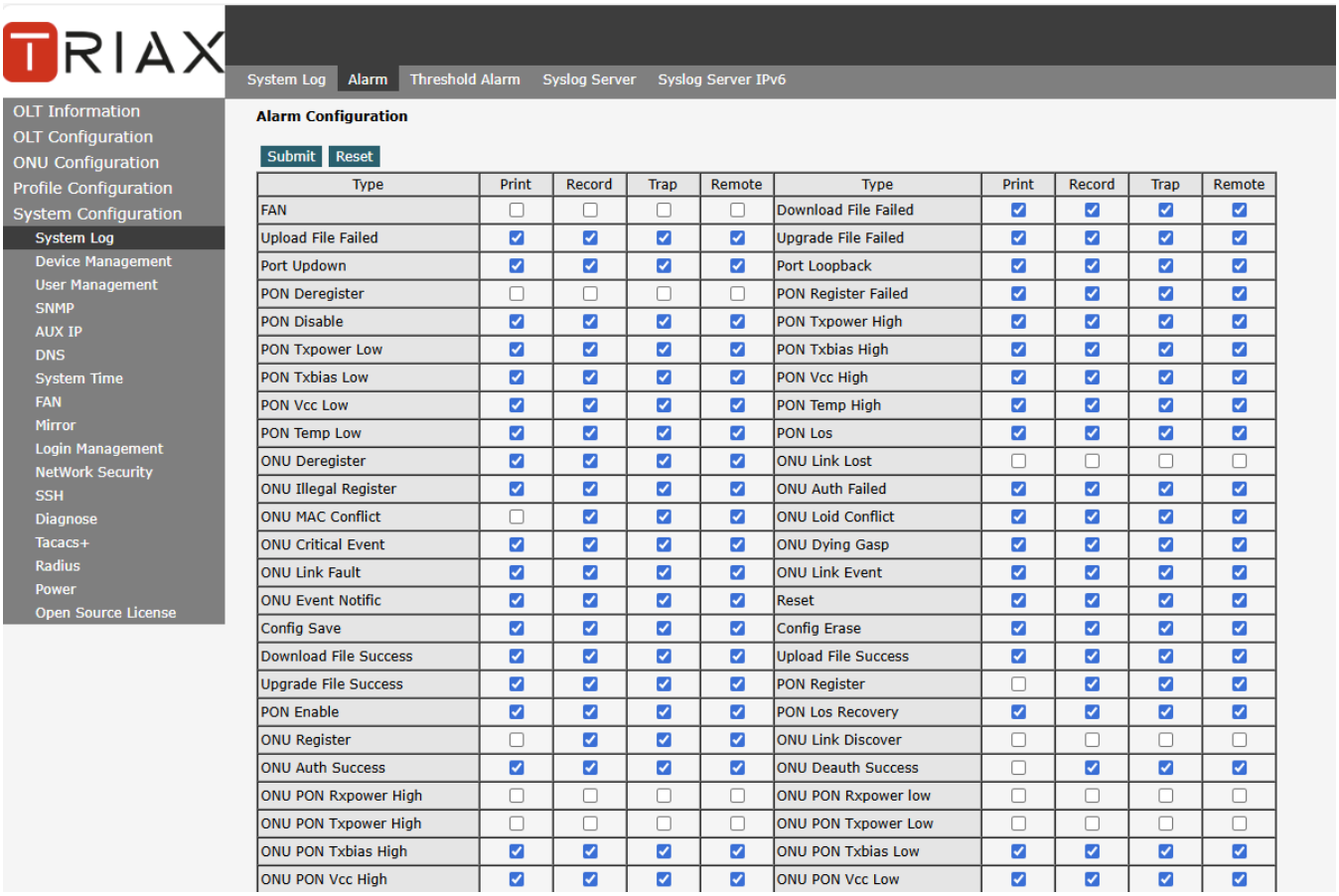


Figure 6.1-1: System Log

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**".



Type	Print	Record	Trap	Remote	Type	Print	Record	Trap	Remote
FAN	☐	☐	☐	☐	Download File Failed	☑	☑	☑	☑
Upload File Failed	☑	☑	☑	☑	Upgrade File Failed	☑	☑	☑	☑
Port Updown	☑	☑	☑	☑	Port Loopback	☑	☑	☑	☑
PON Deregister	☐	☐	☐	☐	PON Register Failed	☑	☑	☑	☑
PON Disable	☑	☑	☑	☑	PON Txpower High	☑	☑	☑	☑
PON Txpower Low	☑	☑	☑	☑	PON Txbias High	☑	☑	☑	☑
PON Txbias Low	☑	☑	☑	☑	PON Vcc High	☑	☑	☑	☑
PON Vcc Low	☑	☑	☑	☑	PON Temp High	☑	☑	☑	☑
PON Temp Low	☑	☑	☑	☑	PON Los	☑	☑	☑	☑
ONU Deregister	☑	☑	☑	☑	ONU Link Lost	☐	☐	☐	☐
ONU Illegal Register	☑	☑	☑	☑	ONU Auth Failed	☑	☑	☑	☑
ONU MAC Conflict	☐	☑	☑	☑	ONU Loid Conflict	☑	☑	☑	☑
ONU Critical Event	☑	☑	☑	☑	ONU Dying Gasp	☑	☑	☑	☑
ONU Link Fault	☑	☑	☑	☑	ONU Link Event	☑	☑	☑	☑
ONU Event Notific	☑	☑	☑	☑	Reset	☑	☑	☑	☑
Config Save	☑	☑	☑	☑	Config Erase	☑	☑	☑	☑
Download File Success	☑	☑	☑	☑	Upload File Success	☑	☑	☑	☑
Upgrade File Success	☑	☑	☑	☑	PON Register	☐	☑	☑	☑
PON Enable	☑	☑	☑	☑	PON Los Recovery	☑	☑	☑	☑
ONU Register	☐	☑	☑	☑	ONU Link Discover	☐	☐	☐	☐
ONU Auth Success	☑	☑	☑	☑	ONU Deauth Success	☐	☑	☑	☑
ONU PON Rxpower High	☐	☐	☐	☐	ONU PON Rxpower low	☐	☐	☐	☐
ONU PON Txpower High	☐	☐	☐	☐	ONU PON Txpower Low	☐	☐	☐	☐
ONU PON Txbias High	☑	☑	☑	☑	ONU PON Txbias Low	☑	☑	☑	☑
ONU PON Vcc High	☑	☑	☑	☑	ONU PON Vcc Low	☑	☑	☑	☑

Figure 6.1-2: Alarm

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

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.

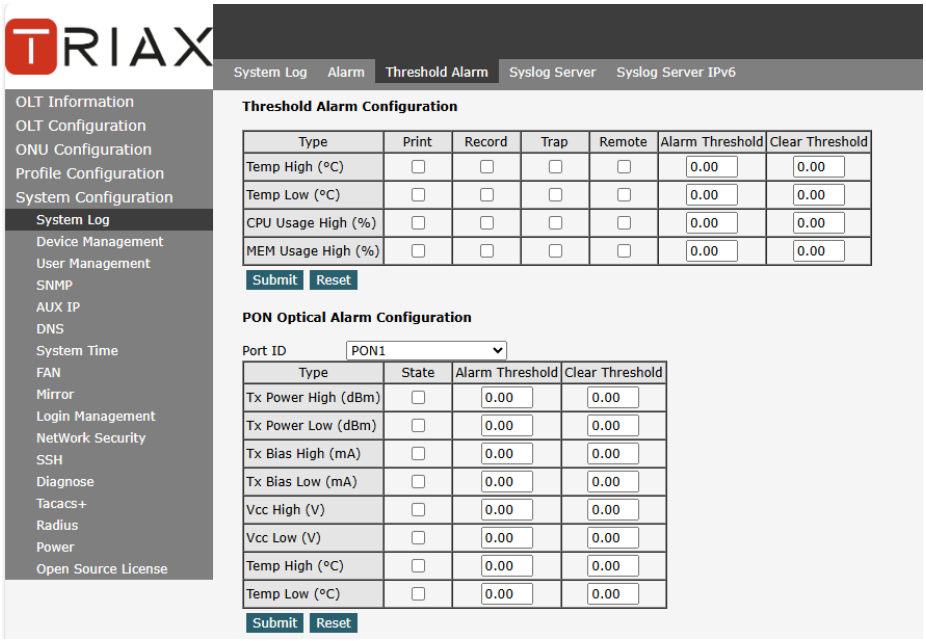


Figure 6.1-3: Threshold Alarm

6.1.4 Syslog Server

System Configuration→System Log →Syslog Server

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

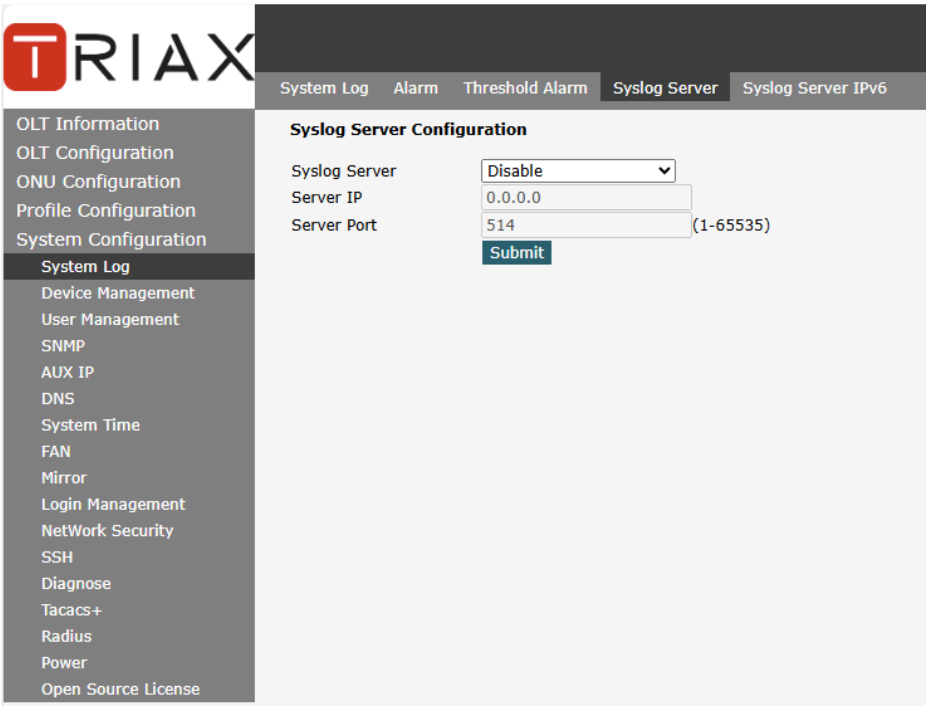


Figure 6.1-4: Syslog Server

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.

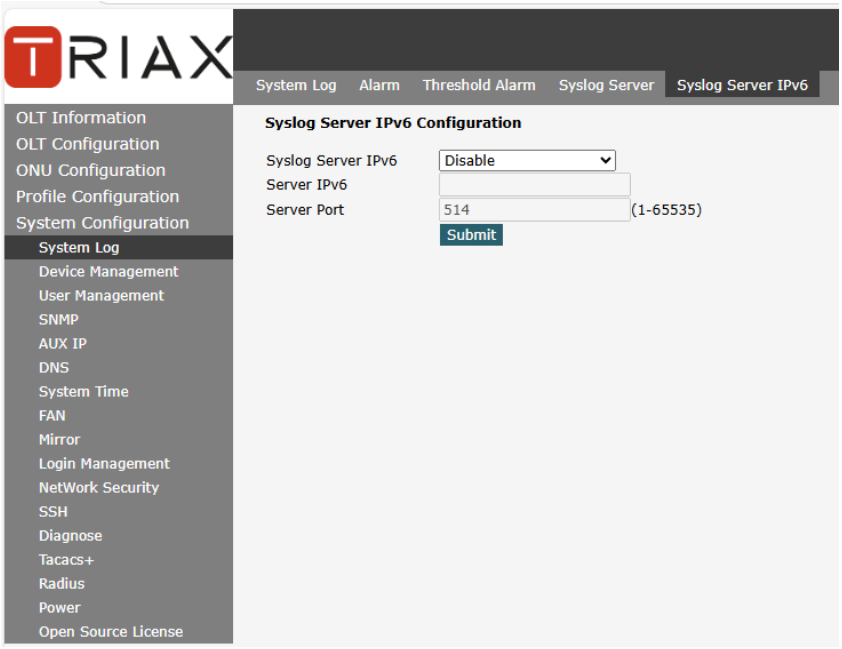


Figure 6.1-5: Syslog Server IPv6

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.

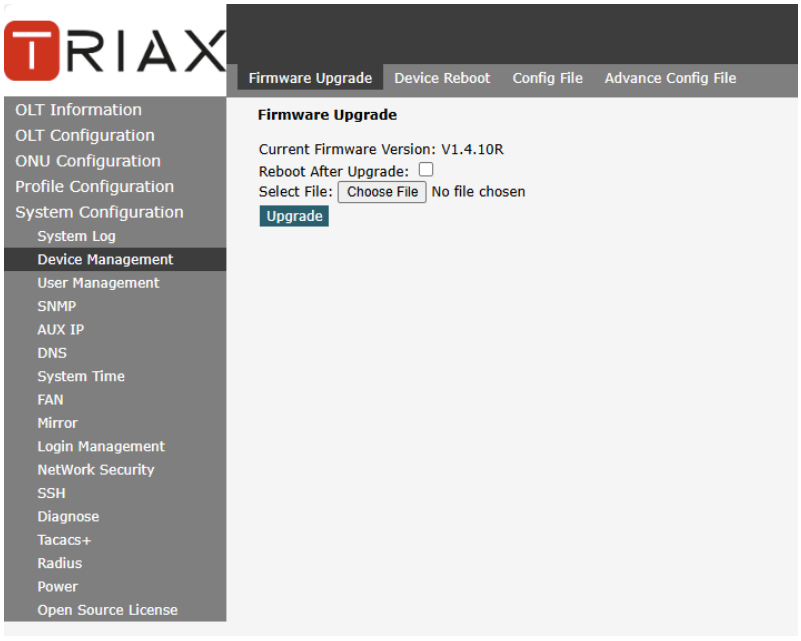


Figure 6.2-1: Firmware Upgrade

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.

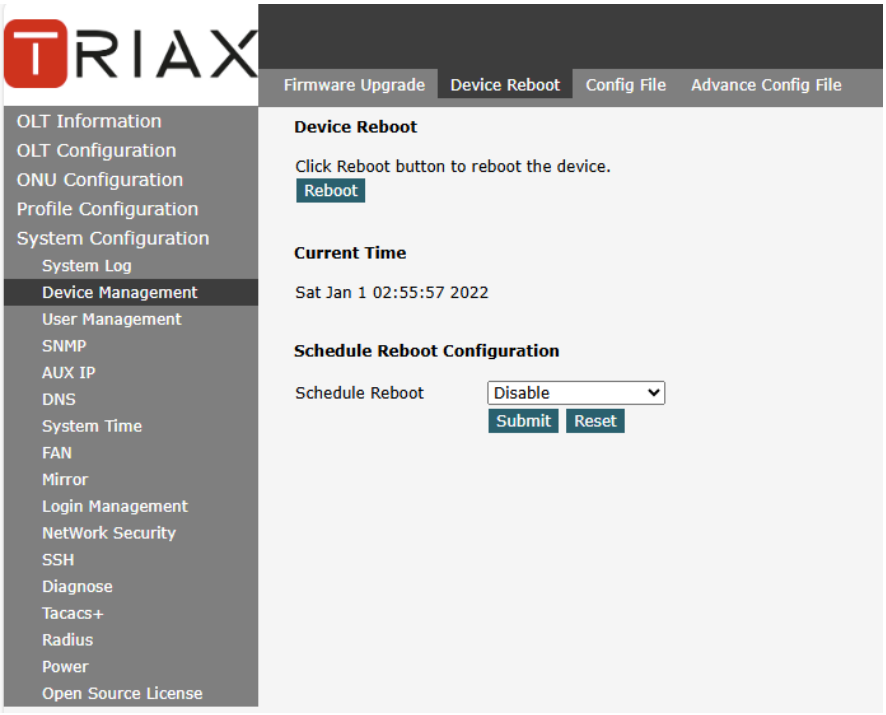


Figure 6.2-2: Device Reboot

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.

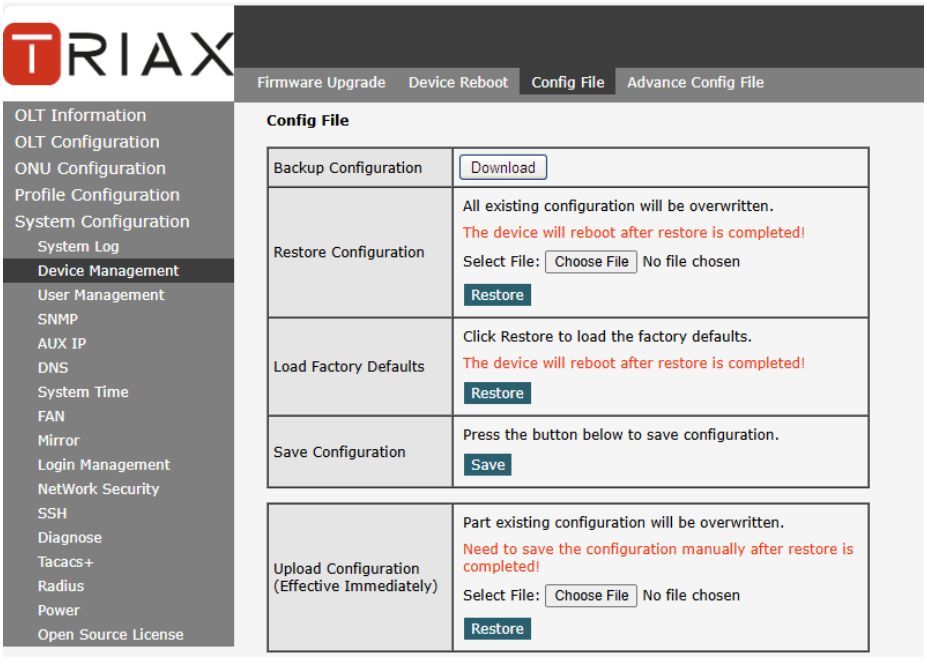


Figure 6.2-3: File Configuration

6.3 User Management

System Configuration→User management

Two types of users 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.

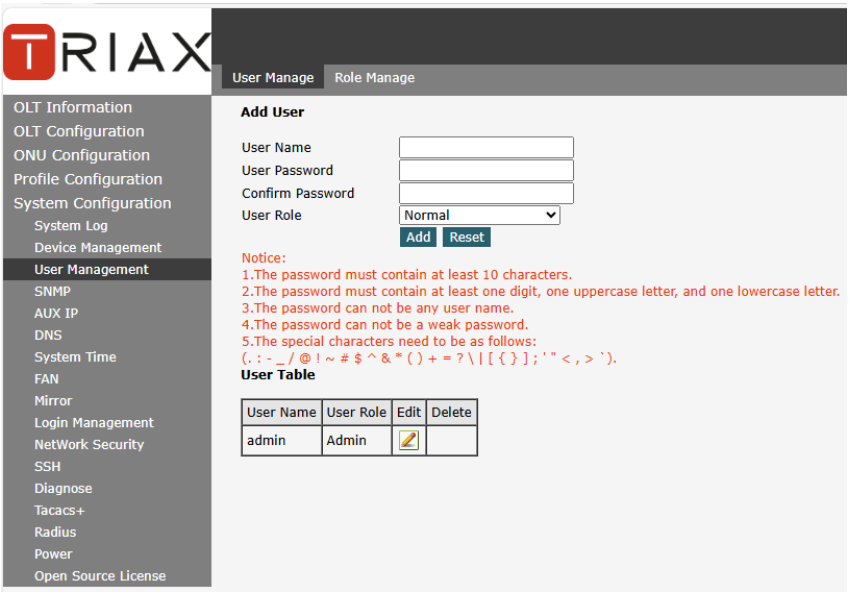


Figure 6.3-1: User Manage

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.

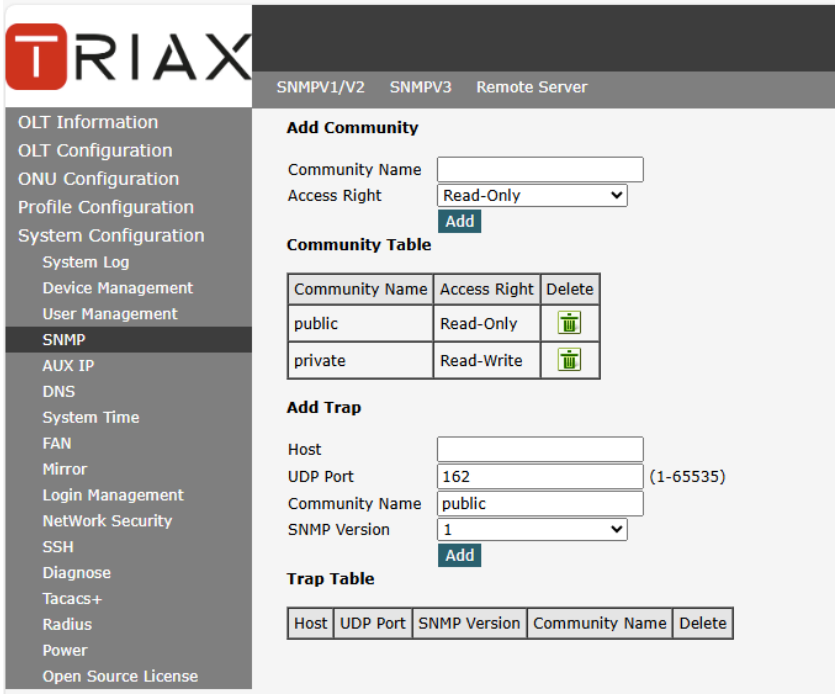


Figure 6.4-1: SNMP V1/V2

6.4.2 SNMP V3

System Configuration → SNMP →SNMP V3

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

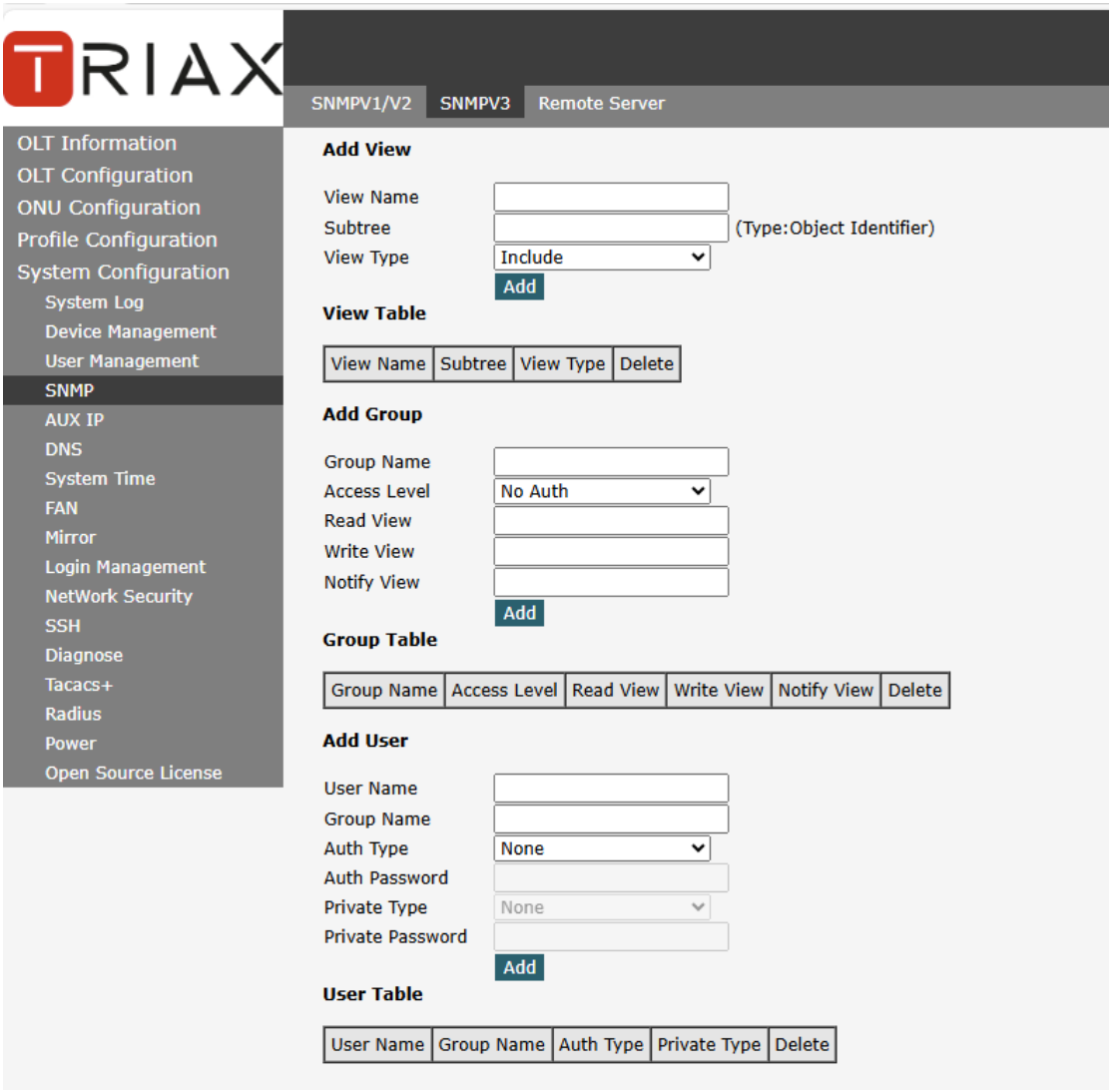


Figure 6.4-2: SNMP V3

6.4.3 Remote Server

System Configuration → SNMP →Remote Server

Configure the IP address of your SNMP network management server.

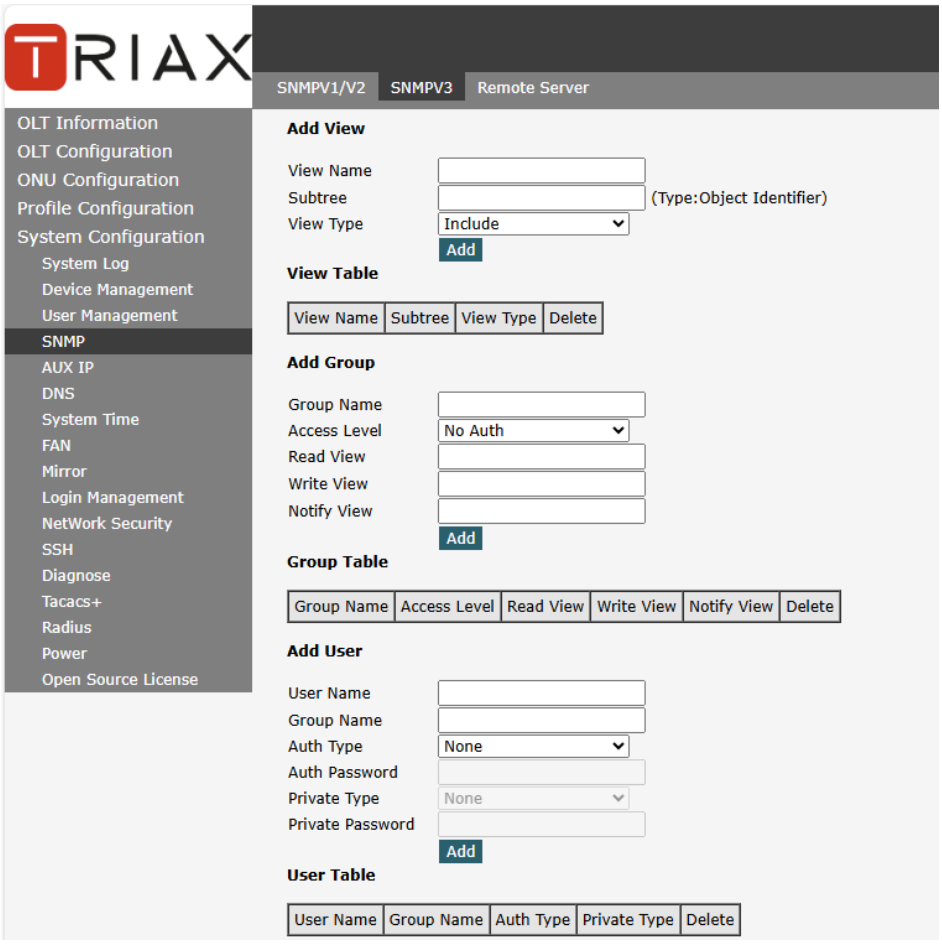


Figure 6.4-4: Remote Server

6.5 AUX IP

6.5.1 AUX IP

System Configuration → AUX IP→ AUX IP

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

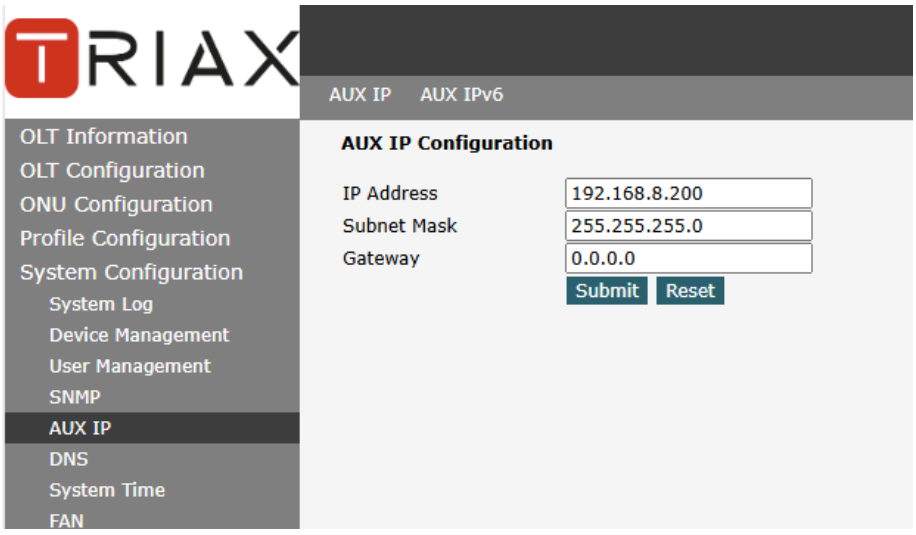


Figure 6.5-1: AUX IP

6.5.2 AUX IPv6

System Configuration → AUX IP → AUX IPv6

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

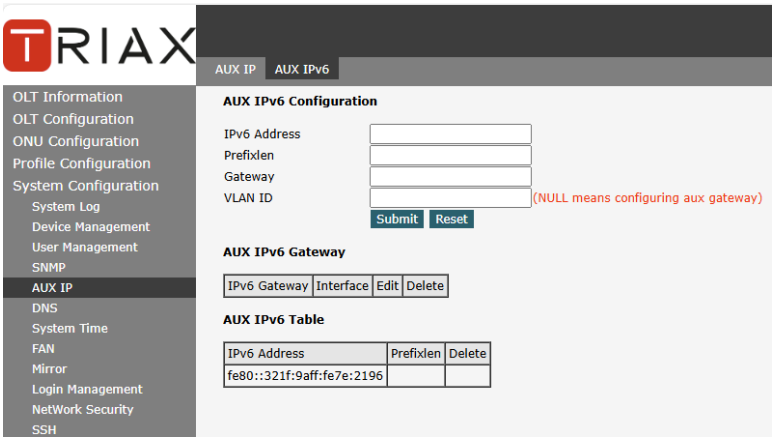


Figure 6.5-2: AUX IPv6

6.6 DNS

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

6.6.1 IPv4 DNS

System Configuration → DNS → IPv4 DNS

This page is used to configure IPv4 DNS.

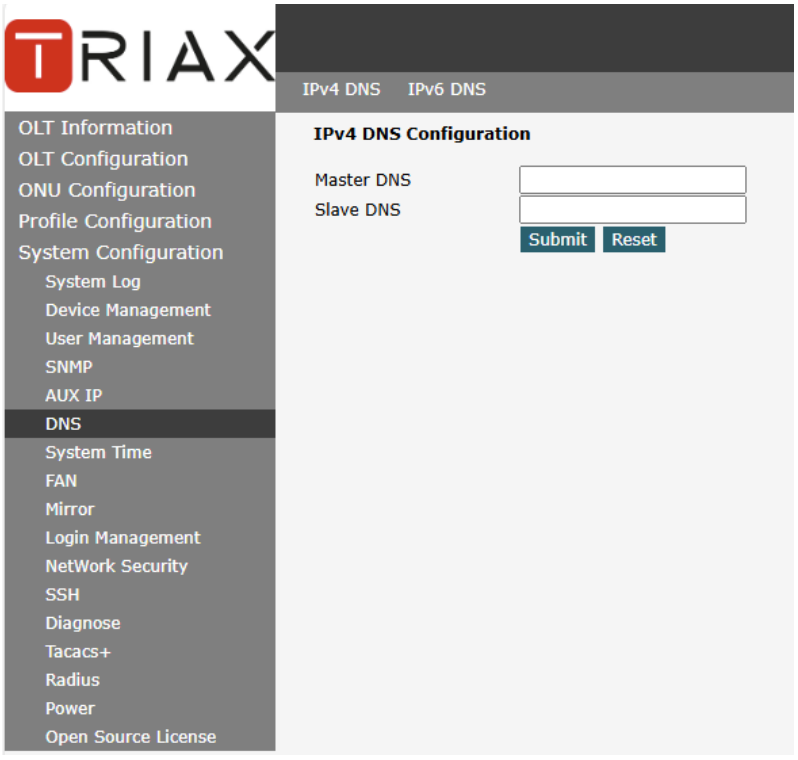


Figure 6.6-1: IPv4 DNS

6.6.2 IPv6 DNS

System Configuration → DNS → IPv6 DNS

This page is used to configure IPv6 DNS.

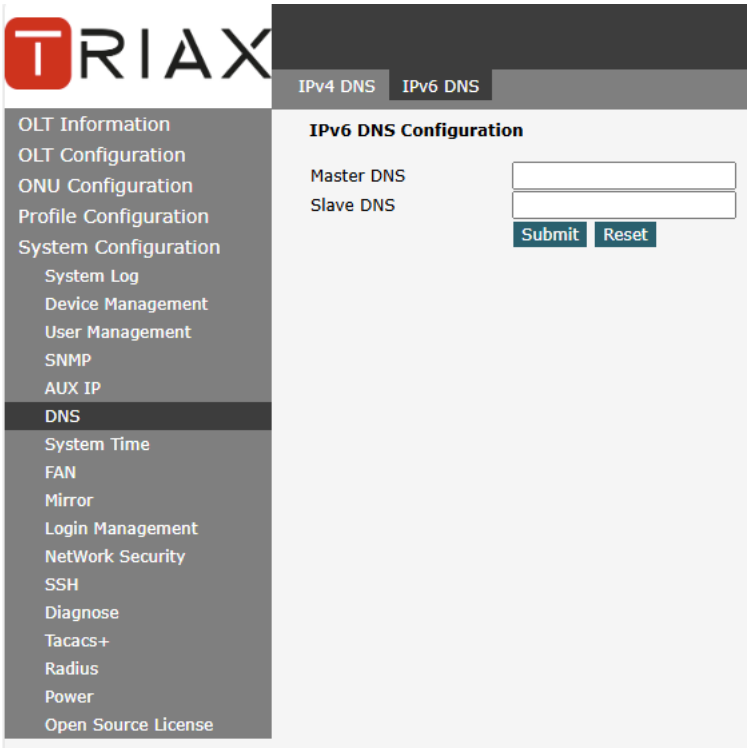


Figure 6.6-2: IPv6 DNS

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.

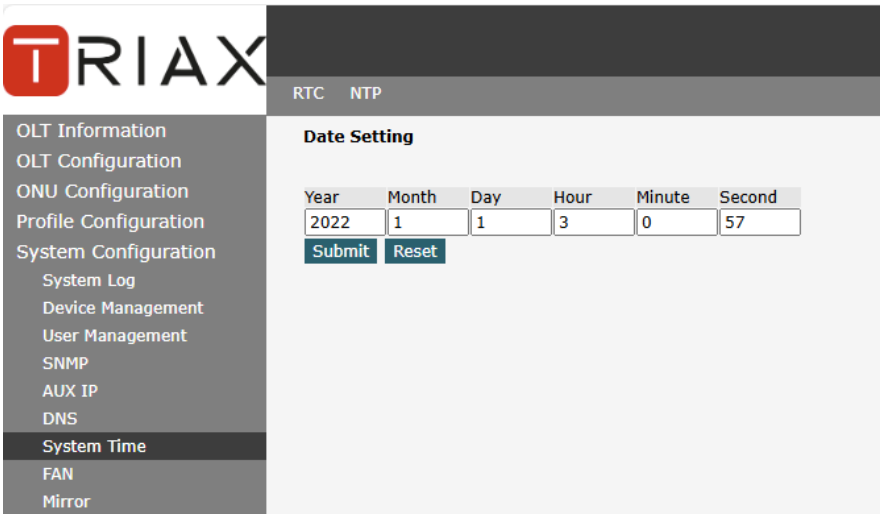


Figure 6.7-1: RTC Setting

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.

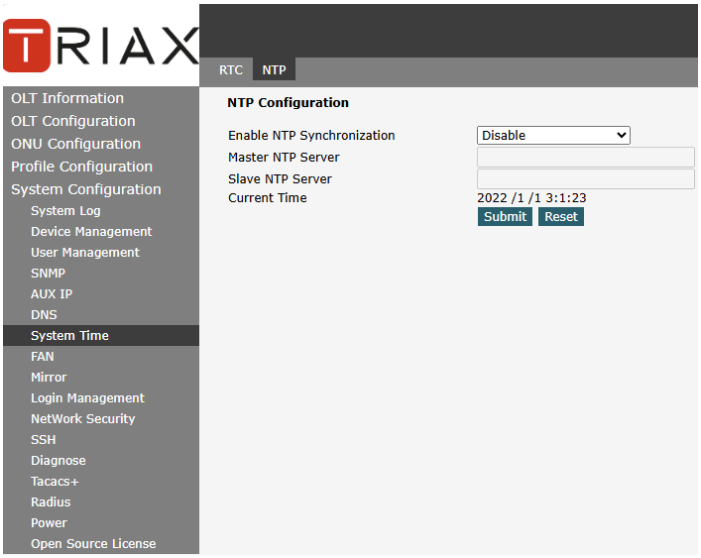


Figure 6.7-2: NTP Configuration

6.8 FAN

System Configuration → FAN

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

This configuration will not be saved after reboot.

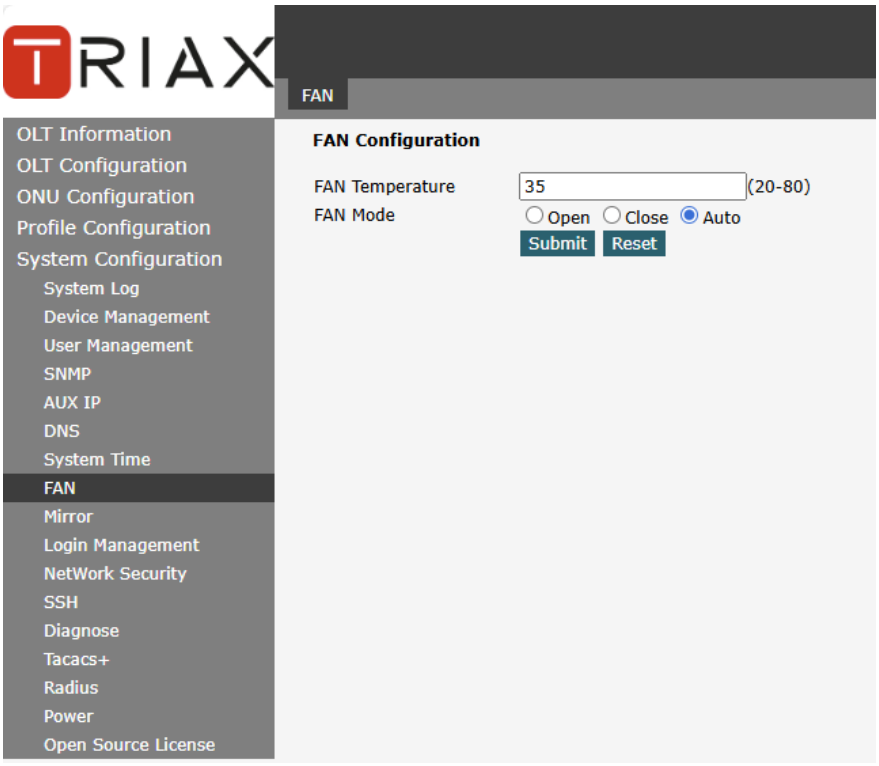


Figure 6.8-1: FAN Configuration

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.

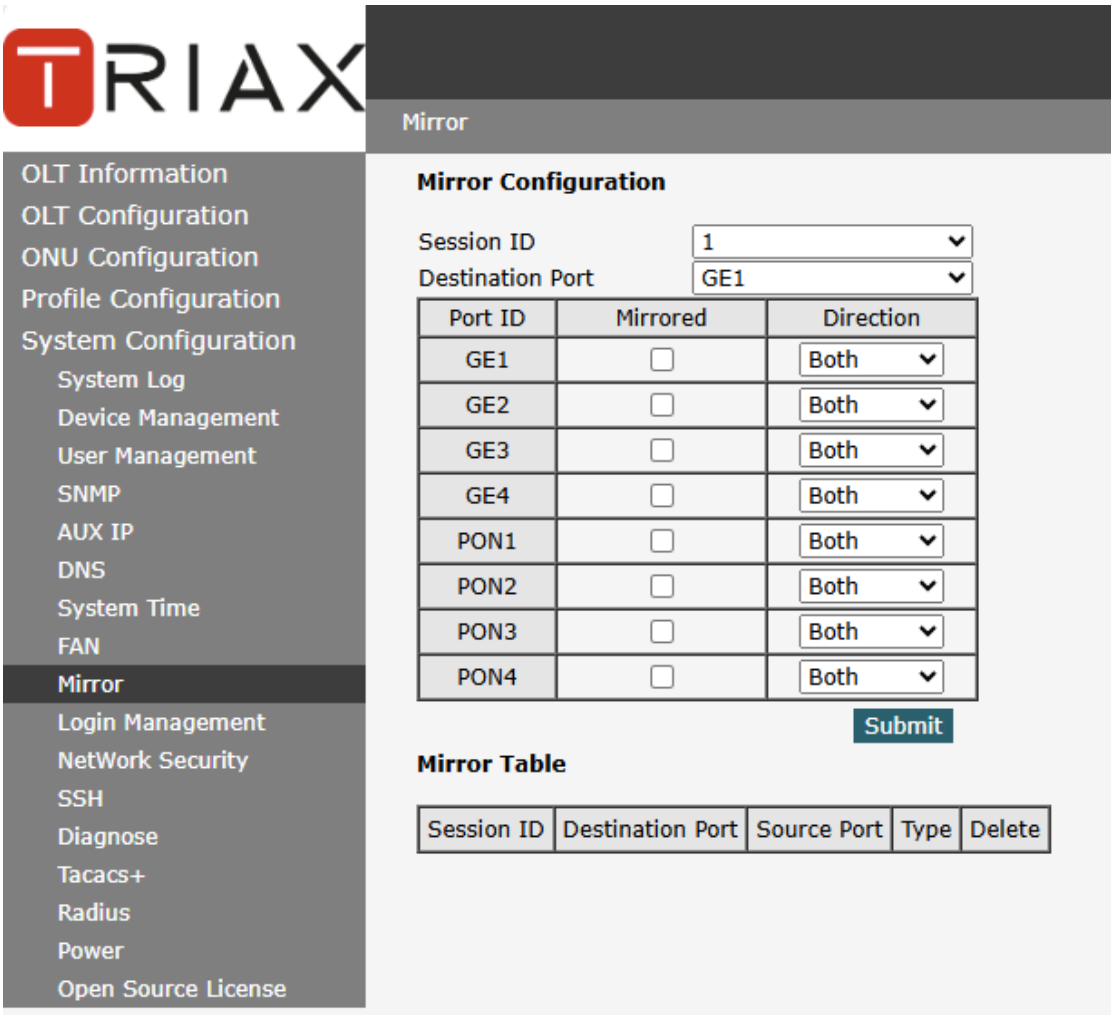


Figure 6.9-1: Mirror Configuration

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.

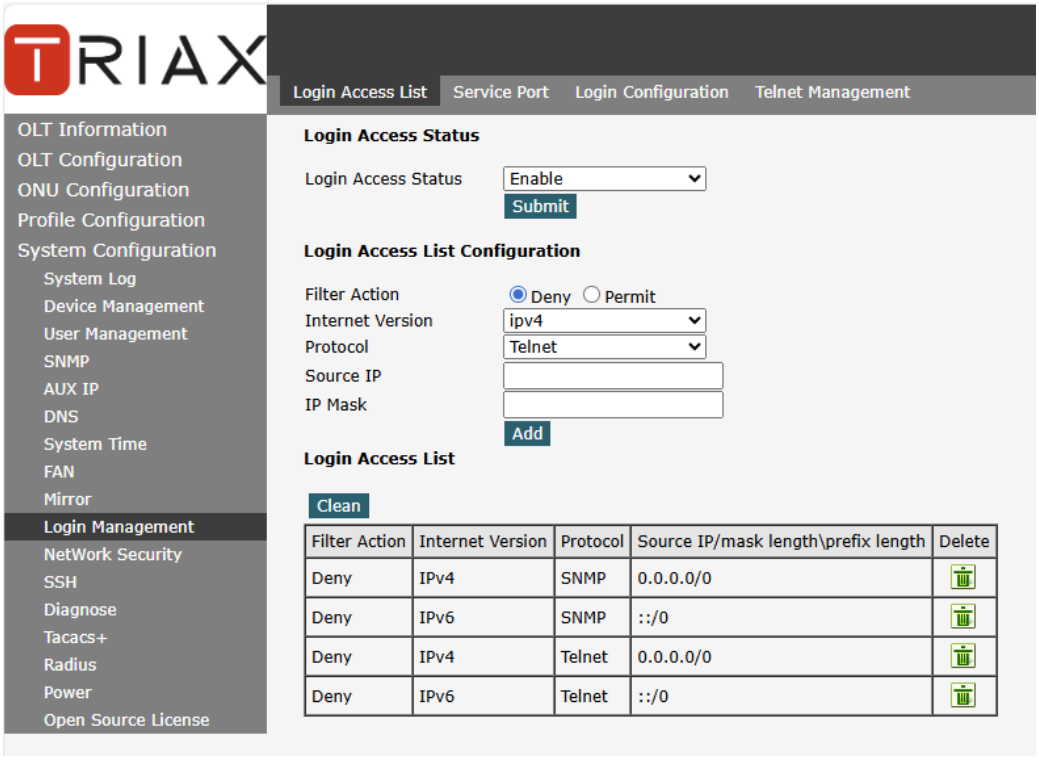


Figure 6.10-1: Login Access List Configuration

6.10.2 Service Port

System Configuration → Login Management→ Service Port

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

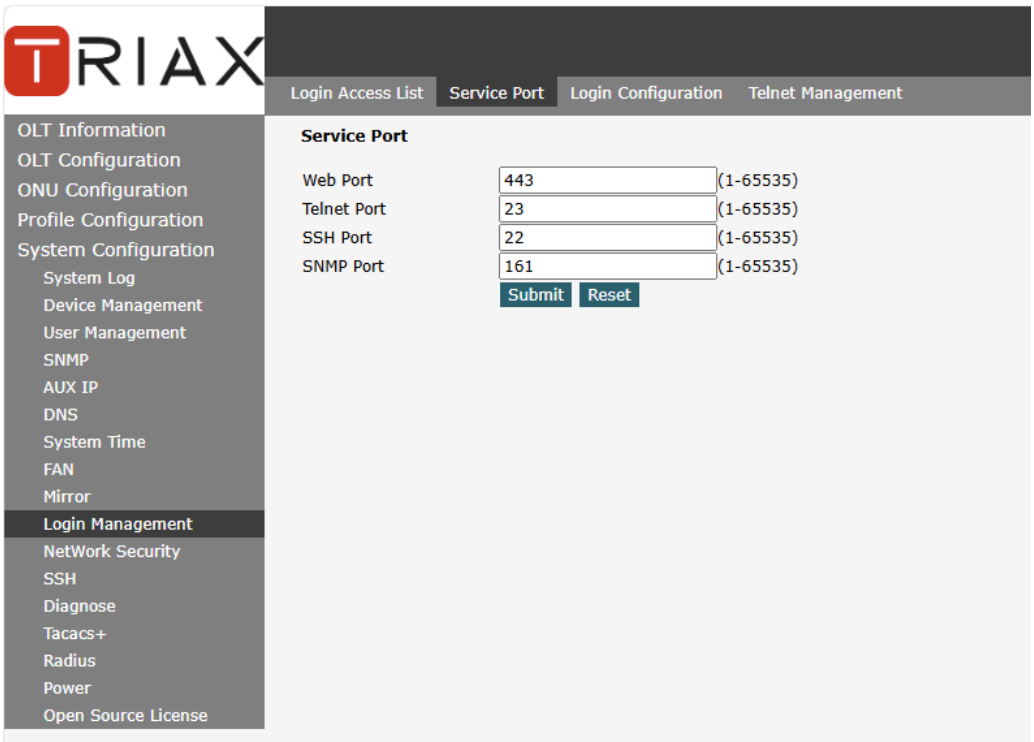


Figure 6.10-2: Service Port Configuration

6.10.3 Login Timeout

System Configuration → Login Management→ Login Timeout

This page is used to set web timeout.

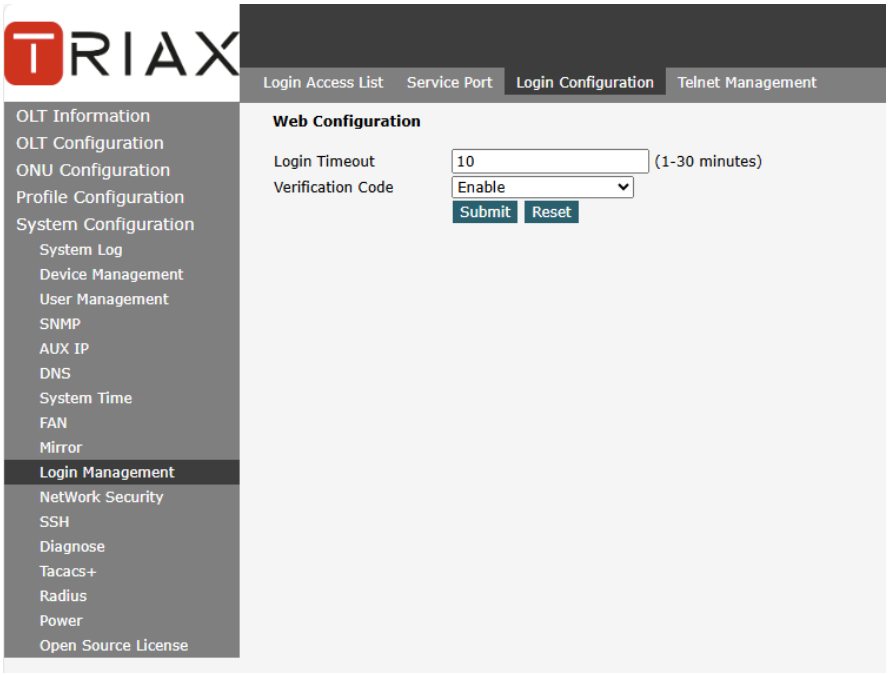


Figure 6.10-3: Login Timeout Configuration

6.11 Net Work Security

System Configuration → Net Work Security

This page is used to set up OLT's network security level.

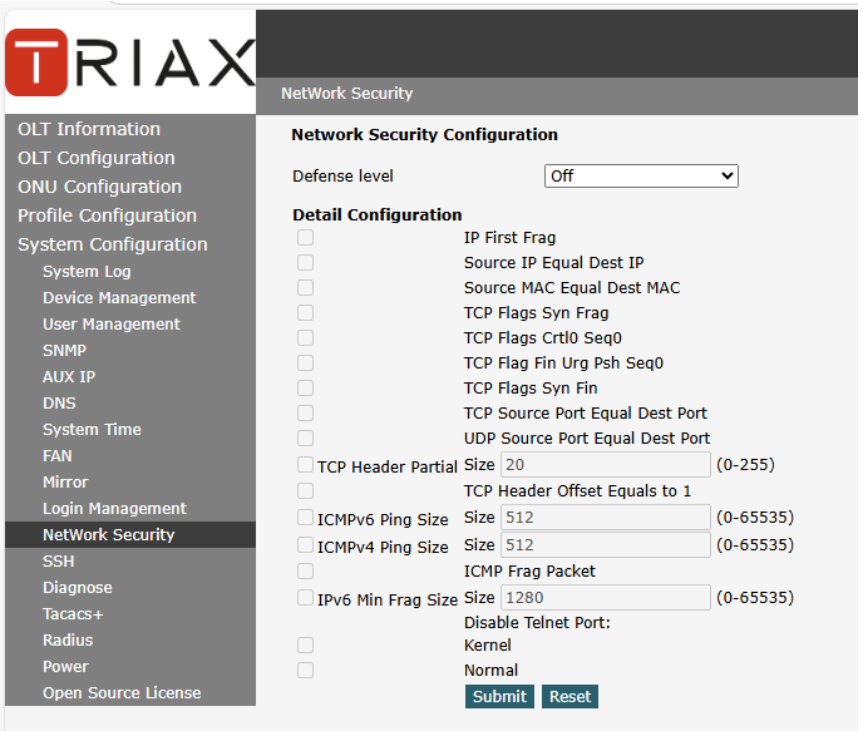


Figure 6.11-1: Net Work Security Setting

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 State

System Configuration → SSH→ SSH State

This page displays current connections that have established by SSH protocol.

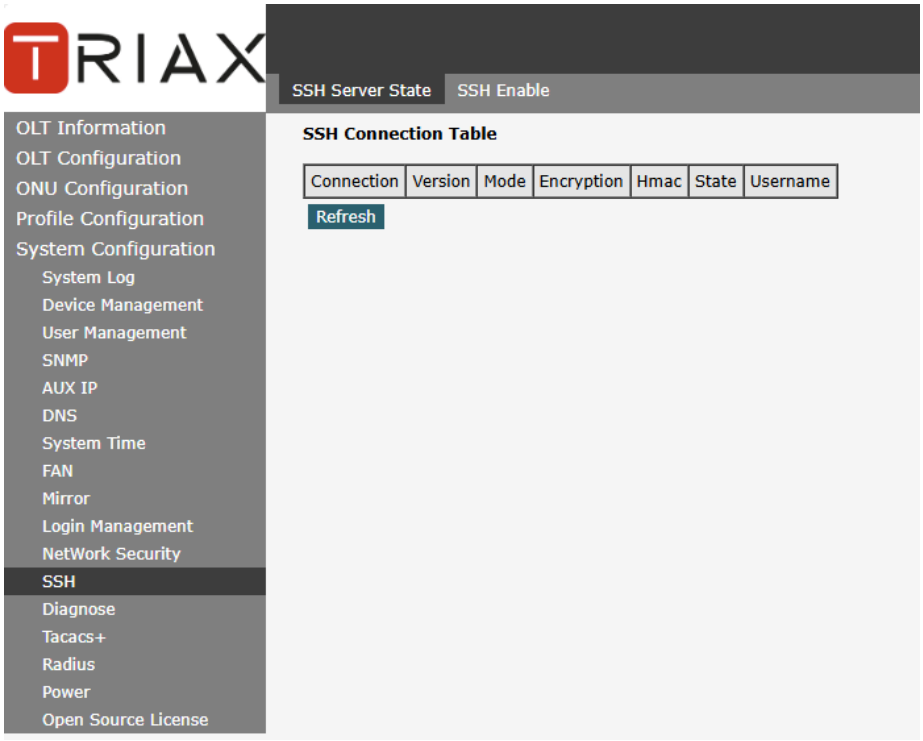


Figure 6.12-1: SSH State

6.12.2 SSH Enable

System Configuration → SSH→ SSH Enable

This page is used to configure SSH protocol related parameters.

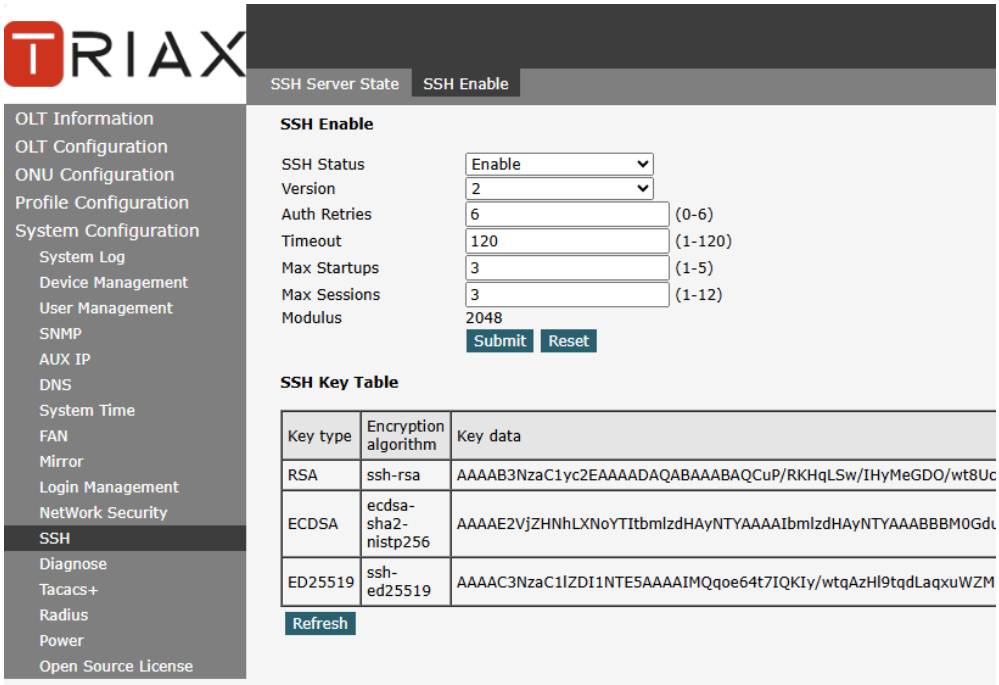


Figure 6.12-2: SSH Global Configuration

6.13 Diagnose

6.13.1 Ping Diagnose

System Configuration → Diagnose→ Ping Diagnose

This interface is used to diagnose network connectivity.

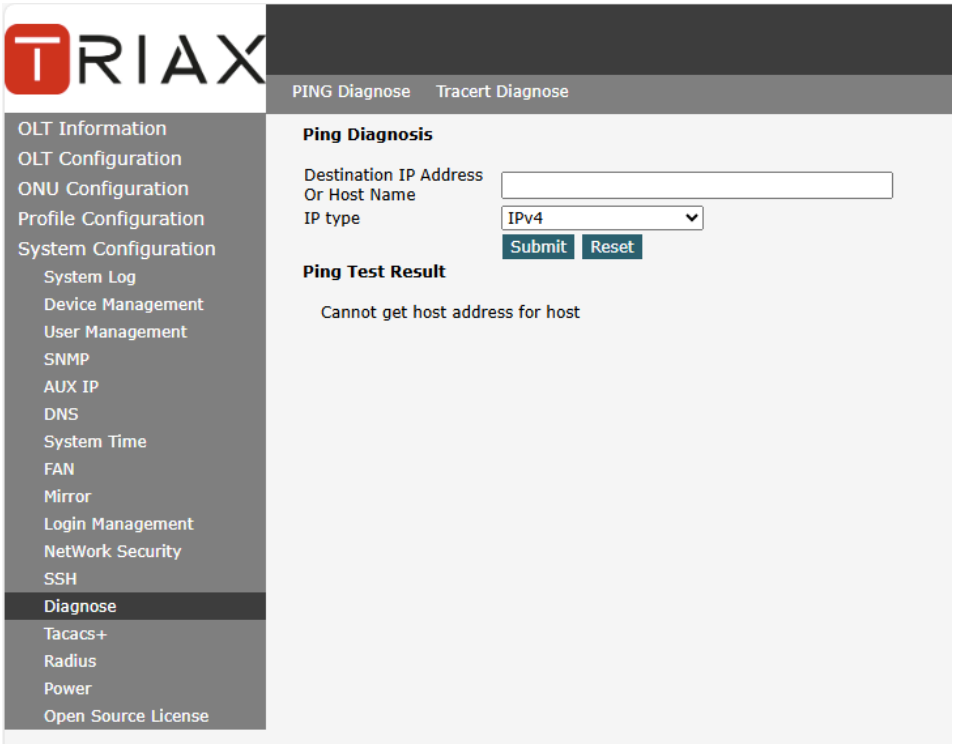


Figure 6.13-1: Ping Diagnose Configuration

6.13.2 Tracert Diagnose

System Configuration → Diagnose→ Tracert Diagnose

This interface is used to track and diagnose routing and forwarding.

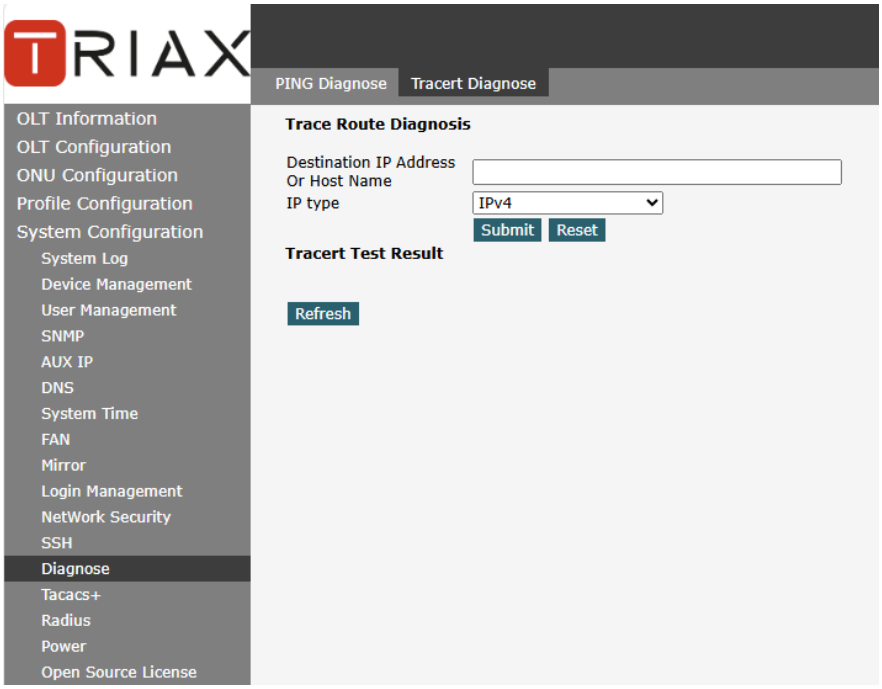


Figure 6.13-2: Tracert Diagnose Configuration

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.

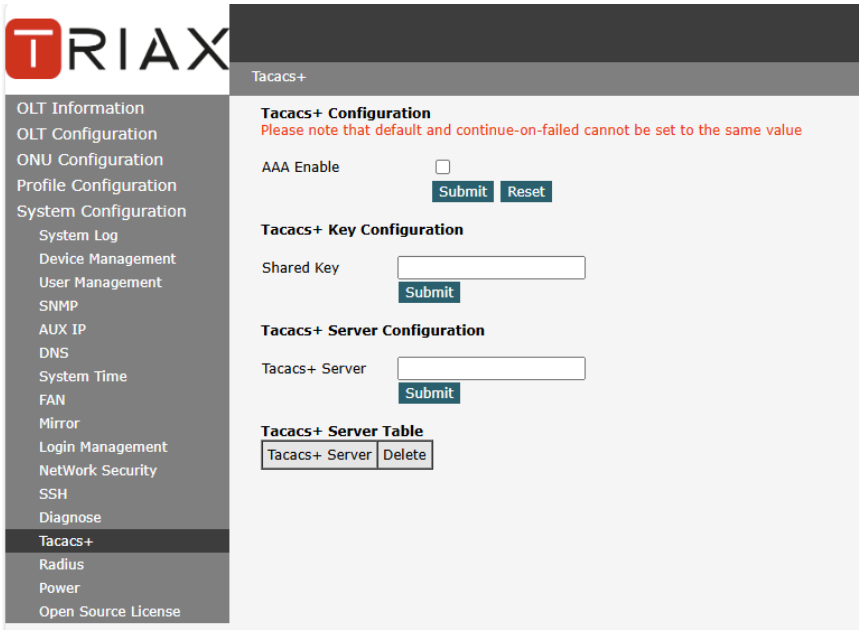


Figure 6.14-1: Tacacs+ Configuration

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.

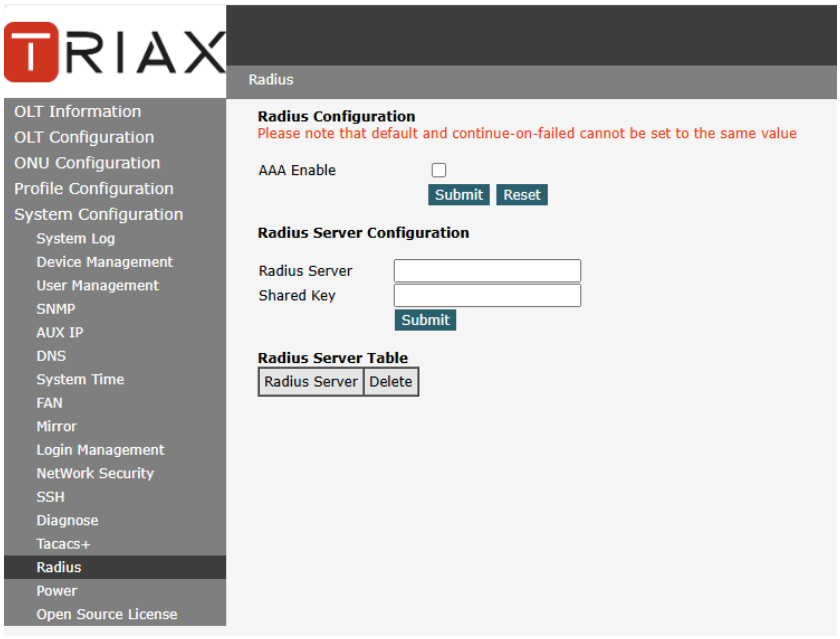


Figure 6.15-1: Radius Configuration

6.16 Power

The Power interface provides monitoring and management of the OLT's power and backup systems. It displays real-time status of the main power supply and rechargeable battery, including charging mode, operational state, and any faults. This allows administrators to ensure continuous device operation and quickly respond to power-related issues.

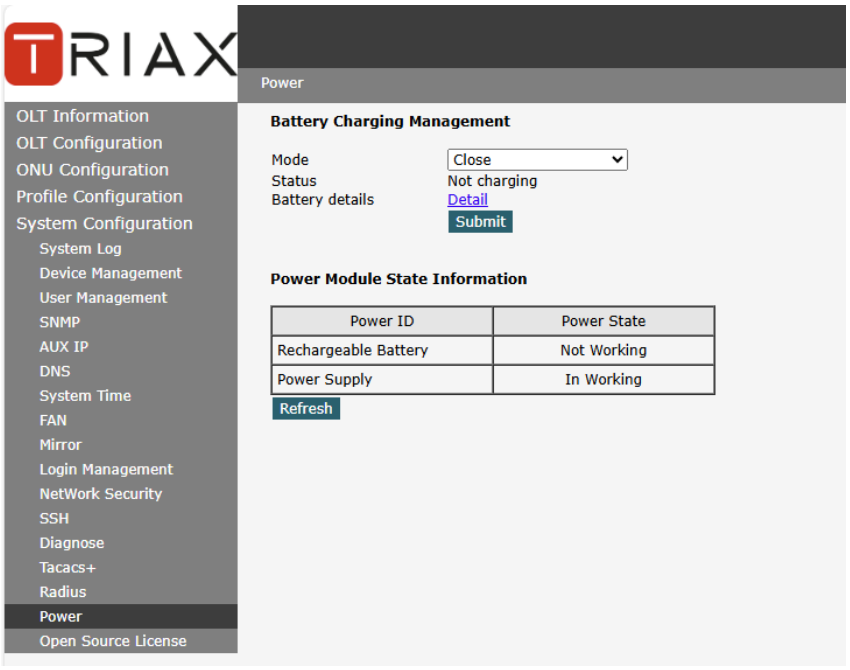


Figure 6.16-1: Power

7 Technical Specifications

TOLT - 4422			
ART. Number	308500		
	Product Description	Accessories	Power Configuration
	4*GPON	GPON SFP C++++ MODULE X 4	2*AC
	2*RJ45		
	2*SFP/SFP+		
Chassis	Rack	1U 19 Inch Standard Box	
	QTY	4	
Uplink Port	RJ45(GE)	2	
	SFP(GE)/SFP+(10GE)	2	
	QTY	4	
GPON Port	Physical Interface	SFP Slots	
	Max splitting ratio	1:128	
Management Ports		1*10/100/1000BASE-T out-band port 1*CONSOLE port	
		1*USB2.0	
Backplane Bandwidth (Gbps)		104	
Port Forwarding Rate (Mpps)		47.616	
PON Port Specification	Transmission Distance	20KM	
	GPON port speed	Upstream 1.244Gbps, Downstream 2.488Gbps	
	Wavelength	TX 1490nm, RX 1310nm	
	Connector	SC/UPC	
	Fibre Type	9/125µm SMF	
	Supported PON module level	Class B+, C, C+, C++, C+++, C++++	
Power Supply	AC	Working Voltage Range: 100~240V, Rated Voltage: 110V/220V	
Management Mode		EMS, WEB, SNMP, Telnet, CLI	

8 EU Declaration of Conformity

The product Declaration of Conformity can be downloaded from the product page at www.triax.com

9 Conditions of warranty

TRIAX UK warrants the product as being free from defects in material and workmanship for a period of 24 months starting from the date of production indicated on it. See note below.

If during this period of warranty, the product proves defective, under normal use, due to defective materials or workmanship, TRIAX UK, at its sole option, will repair or replace the product. Return the product to your local dealer for reparation.

THE WARRANTY IS APPLIED ONLY FOR DEFECTS IN MATERIAL AND WORKMANSHIP AND DOES NOT COVER DAMAGE RESULTING FROM:

- Misuse or use of the product outside of its specifications,
- Installation or use in a manner inconsistent with the technical or safety standards in force in the country where the product is used,
- Use of non-suitable accessories (power supply, adapters...),
- Installation in a defective system,
- External cause beyond the control of TRIAX UK such as drop, accidents, lightning, fire, …

THE WARRANTY IS NOT APPLIED IF

- Production date or serial number on the product is illegible, altered, deleted or removed.
- The product has been opened or repaired by a non-authorized person.

NOTE

Date of production can be found in the product's serial number code. The format is "YYWW123456 (YEAR, WEEK, 123456 product unique number), e.g. 2532000020 = year 2025 week 32, product No.20 of this batch.

TRIAX UK | Treorchy | RCT | CF42 6DL | UK