
AirLive
ONU-10XG(S)-1004-10G
USER MANUAL

airlive®

Contents

Chapter 1	Product Introduction.....	1
1.1	Product Description.....	1
1.2	Special features	2
1.3	Technical parameters	2
1.4	Application chart	3
1.5	Panel description	3
Chapter 2	Quick Installation	6
2.1	Standard Packing Contents.....	6
2.2	Quick Installation.....	6
2.3	Set up Connection	7
Chapter 3	Configuration.....	8
3.1	Login	8
3.2	Status.....	9
3.2.1	Device Info	9
3.2.2	WAN Info.....	9
3.2.3	PON Info	11
3.2.4	User Info.....	13
3.3	Network.....	16
3.3.1	WAN.....	16
3.3.2	LAN.....	18
3.3.3	MTU	21
3.3.4	Binding Settings	22
3.3.5	TR069.....	22
3.3.6	Qos.....	26
3.3.7	Time.....	30
3.3.8	Route.....	30
3.4	Security.....	33
3.4.1	URL Filtering	33

3.4.2 Firewall.....	33
3.4.3 Login Privilege	34
3.4.4 MAC Filtering	34
3.4.5 IP/Port Filtering.....	35
3.5 Application.....	38
3.5.1 Multicast Setting.....	38
3.5.2 Advance NAT.....	40
3.5.3 Others	42
3.6 Management	46
3.6.1 User Manage.....	46
3.6.2 Device Manage.....	46
3.6.3 Log Manage.....	50
3.6.4 Other Manage	51
3.7 Diagnostics.....	53
3.7.1 Network diagnostics	53
3.7.2 Loopback Test	53
Chapter 4 Examples.....	55
4.1 Internet service.....	55
4.1.1 Requirement	55
4.1.2 Steps	55
4.2 IPTV service.....	57
4.2.1 Requirement	57
4.2.2 Steps	57
4.3 Internet and IPTV service mixed.....	61
4.3.1 Requirement	61
4.3.2 Steps	61
4.4 Update image	65
Chapter 5 FAQ	67

Chapter 1 Product Introduction

1.1 Product Description

The 10G PON AirLive ONU-10XG(S)-1004-10G developed by AirLive comes in two models a XG-PON and XGS-PON, providing multiple rate Ethernet ports of 10GE/GE. It enables fast and stable networking for multiple devices, ensuring a seamless user experience within homes and effortlessly meeting the demands of 4K/8K, VR, and other services. It offers home and enterprise users an ultimate experience of 10G ultra-high-speed internet connection.

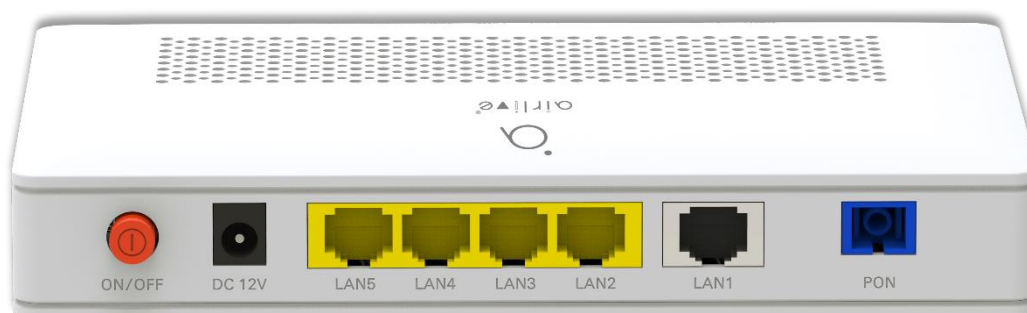


Figure 1-1-1: AirLive ONU-10XG(S)-1004-10G

There are three specifications available for this ONU, 10G-EPON, XG-PON or XGS-PON optional.

Product	Specification
XG/XGS-PON ONU	1*10GE+4GE+1USB3.0 XG-PON ONU
	1*10GE+4GE+1USB3.0 XGS-PON ONU

1.2 Special features

- Plug and play, integrated auto detecting, auto configuration, and auto firmware upgrade technology.
- Integrated TR069 remote configuration and maintenance function.
- Support rich VLAN, DHCP Server/Relay and IGMP/MLD snooping multicast feature.
- Support NAT, Firewall function.
- Support IPv4 and IPv6 dual stack.
- The WAN port supports bridge, router and bridge/router mixed mode.

1.3 Technical parameters

Technical items	Descriptions
PON interface	10G-XG/XGS-PON connector, SC single-mode/single-fiber. XG(S)-PON: uplink 2.5/10Gbps, downlink 10Gbps;
Wavelength	XG/XGS: Tx 1270nm, Rx 1577nm
Optical interface	SC/UPC connector
Interface	1*10GE, Auto-negotiation, RJ45 ports 4*GE, Auto-negotiation, RJ45 ports 1*USB3.0
LED	PWR, PON, LOS, WAN, LAN1~5, USB
Operating condition	Operating temp:-10 ~ +55°C Operating humidity:5 ~ 95% (non-condensed)
Storing condition	Storing temp: -40 ~ +70°C Storing humidity: 5 ~ 95% (non-condensed)
Power supply	DC 12V, 1A, external AC-DC power adaptor
Power consumption	12W
Dimension	180mm*120mm*34.5mm (L*W*H)
Net weight	285.5g

1.4 Application chart

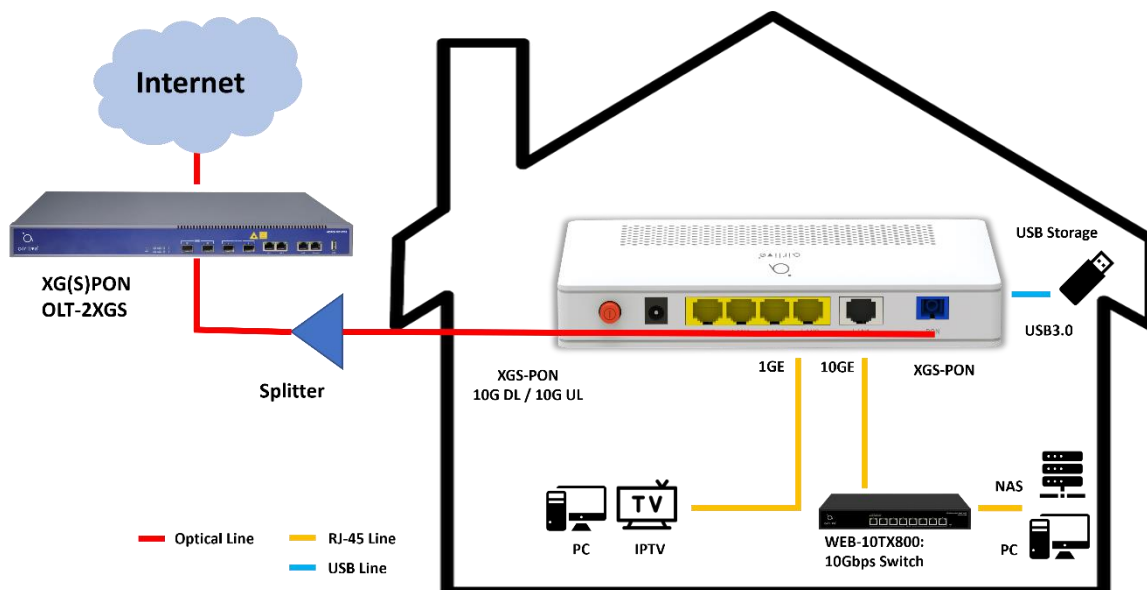


Figure 1-4-1: Application chart, when using XG-Pon it will be 10G DL/2.5G UL

1.5 Panel description

Interface panel

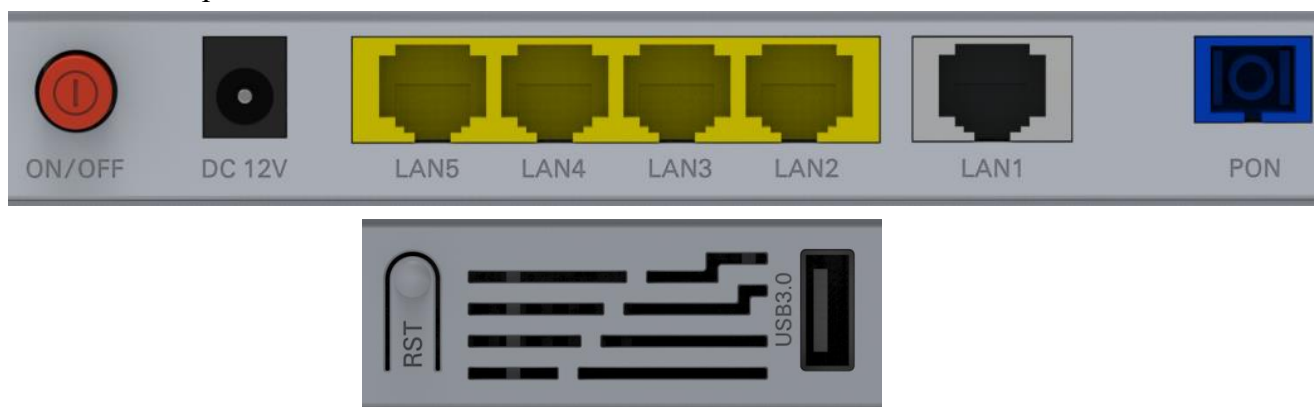


Figure 1-5-1: Interface panel

Name	Function
ON/OFF	Power switch.
DC 12V	Connect with power adapter. DC 12V, 1A.

LAN1-5	The silver LAN1 is 10GE port and the yellow LAN2-5 are 1GE port. Connect PC or other devices to GE port by Cat5 cable, RJ-45 connector and connect to 10GE port by Cat6a cable, RJ-45 connector.
PON	Connect to OLT by SC type fiber connector, single mode optical fiber cable.
RST	Press RST button over 10 seconds, ONU restores factory default and reboots.
USB 3.0	External USB port, connect to USB storage device.

Indication Panel



Figure 1-5-2: Indication panel

Name	Status	Function
PWR	On	Device is powered up.
	Off	Device is powered down.
PON	On	Device is registered to PON system.
	Off	Device is not registered to PON system.
	Blink	Device is registering.
LOS	Off	Device has received optical signal.
	Blink	Device does not receive optical signal.
WAN	On	WAN connection is up.
	Off	WAN connection is down.
	Blink	Data passing WAN connection.

LAN1-5	On	Port is connected properly (LINK).
	Off	Port is not connected properly.
	Blink	Port is sending or/and receiving data (ACT).
USB	On	USB device is connected, but without ongoing data transmission.
	Off	Device is powered off or USB device is not connected.
	Blink	USB is with ongoing data transmission.

Chapter 2 Quick Installation

2.1 Standard Packing Contents

When you receive our products, please check carefully to make sure that our products do not have some defects or not. If something is wrong after shipping, please contact carrier; other damage or lack of some parts, please contact with dealer.

Contents	Description
XG or XGS-PON ONU	1 pc
Power Adapter	1 pc
Installation Guide	1 pc
Network cable	1 pc

2.2 Quick Installation

1. Connecting the optical fiber cable to the unit.
 - a) Remove the protective cap of the optical fiber.
 - b) Clean the end of the optical fiber with an optical fiber end cleaner.
 - c) Remove the protective cap of the ONU optical interface (PON interface). Connect the fiber to the PON port on the unit.

Note: When measuring the optical power before connecting to the ONU, it is recommended to use a PON Inline Power Meter. While connecting, please note:

- Keep the optical connector and the optical fiber clean.
 - Make sure there are no tight bends in the fiber and that the bending diameter is greater than 6cm. Otherwise, the optical signal loss may be increased, to the extent that signal may be unavailable.
 - Cover all optic ports and connectors with a protective cap to guard against dust and moisture when the fiber is not used.
2. Apply power to the unit.
 3. After the ONU is power ON, Indicators should light up as for normal operation. Check whether the PON interface status LED is (PON/LOS) is continuously on. If it is, the connection is normal: otherwise there is either a problem with the physical connection or the optical level at either end. This may be caused by either too much or too little attenuation over the optical fiber. Please refer to the Layout Description section of this installation manual for normal LED activity.

4. Check all signal levels and services on all the ONU communication ports.

Unit Installation Adjustment

Installing the ONU on a horizontal surface (Bench top)

Put the ONU on a clean, flat, sturdy bench top. You must keep the clearance for all sides of the unit to more than 10cm for heat dissipation.

Installing the ONU on a vertical surface (Hanging on a wall)

You can install the ONU on a vertical surface by using the mounting holes on the bottom of the ONU chassis and two flat-head wood screws.

- a) Insert the screws into the wall. The screw positions must be in the same horizontal line and the distance between them must be 165mm. Reserved at least 6mm between the screw caps and the wall.
- b) Hang the ONU on the screws through the mounting holes.

2.3 Set up Connection

Set up wired connection

Connect PC with ONU Ethernet port by RJ-45 CAT5/CAT6A cable.

Chapter 3 Configuration

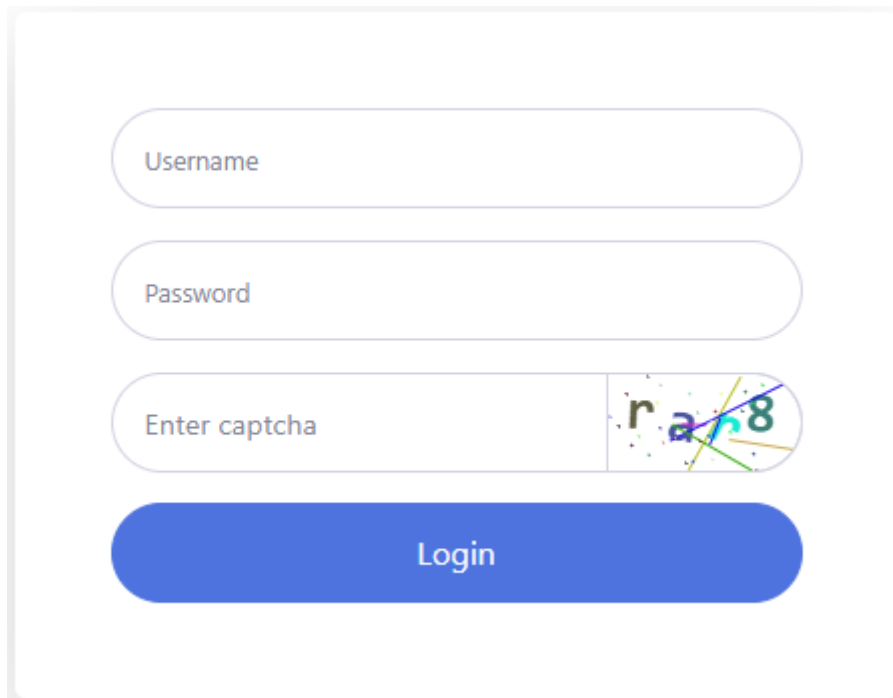
After finishing the basic connection configuration, you can use its basic function. In order to satisfy individuation service requirements, this chapter provides you with the parameter modification and individuation configuration description.

3.1 Login

The device is configured by the web interface. The following steps will enable you to login:

- 1、Conform “2.2 Quick Installation” to install;
- 2、The device default IP is 192.168.1.1;
- 3、Open web browser, type the device IP in address bar;
- 4、Entry of the username and password will be prompted. Enter the default login User Name and Password:

The default login User Name of administrator is “admin”, and the default login Password is “stdONU101”.



The image shows a web interface for logging in. It features three input fields: 'Username', 'Password', and 'Enter captcha'. The 'Enter captcha' field contains a captcha image with the characters 'ra78'. Below these fields is a blue 'Login' button.

Figure 3-1-1: Login

3.2 Status

This part shows the main information of the product.

3.2.1 Device Info

This page shows the device basic information, such as device model, device SN, hardware version, and firmware version, PON S/N, CPU usage, memory usage and quick guide.

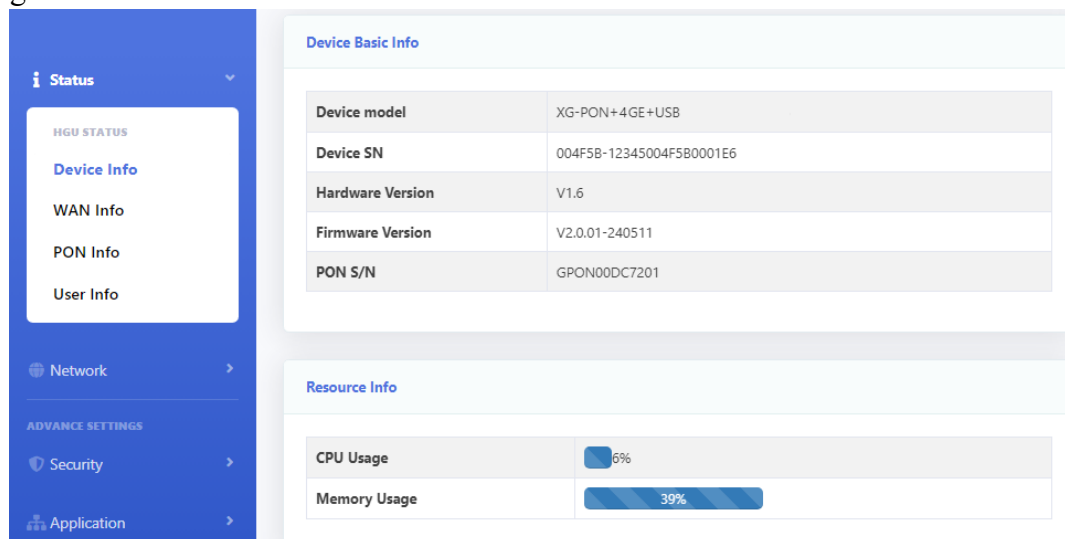


Figure 3-2-1: Device Information

3.2.2 WAN Info

This page shows the device wan information, such as IPv4/IPv6 WAN info, and Remote Manage Info.

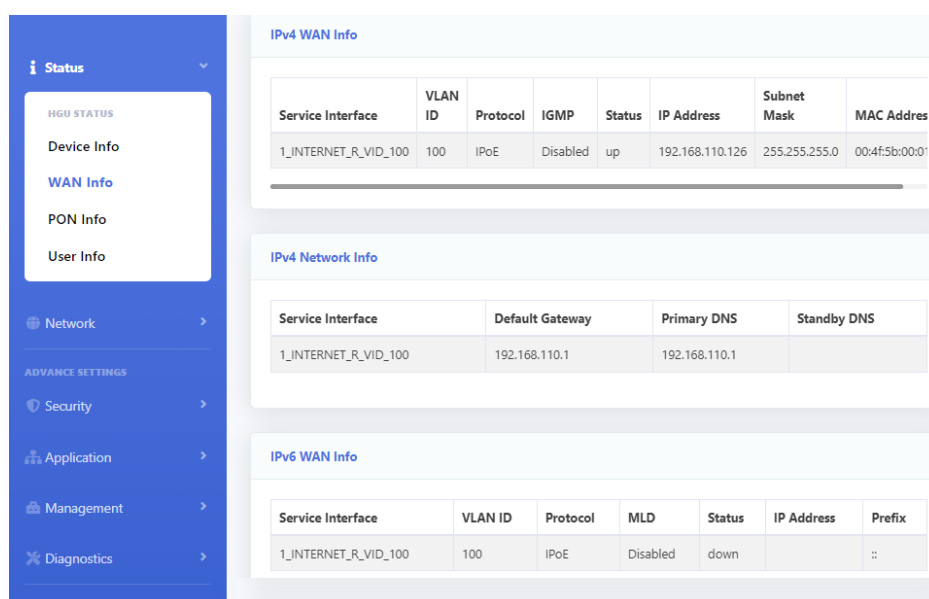


Figure 3-2-2: WAN info

3.2.2.1 IPv4 Connection Info

This page shows IPv4 WAN connection information that you have configured.

IPv4 WAN Info							
Service Interface	VLAN ID	Protocol	IGMP	Status	IP Address	Subnet Mask	MAC Address
1_INTERNET_R_VID_100	100	IPoE	Disabled	up	192.168.110.126	255.255.255.0	00:4f:5b:00:01

IPv4 Network Info			
Service Interface	Default Gateway	Primary DNS	Standby DNS
1_INTERNET_R_VID_100	192.168.110.1	192.168.110.1	

Figure 3-2-3: IPv4 WAN Information

3.2.2.2 IPv6 Connection Info

This page shows IPv6 WAN connection information that you have configured.

IPv6 WAN Info						
Service Interface	VLAN ID	Protocol	MLD	Status	IP Address	Prefix

IPv6 Network Info			
Service Interface	Default Gateway	Primary DNS	Standby DNS

Figure 3-2-4: IPv6 WAN Information

3.2.2.3 TR069 Status

This page shows the request status and configuration status of TR069 connection.

Remote Manage Info	
Connection	no inform
ACS connect request state	NONE
ACS config state	ACS not set

Figure 3-2-5: TR069 connection Status

3.2.3 PON Info

This page shows the PON information, including connection information, FEC information, temperature, voltage, current, optical power, and statistics of the packet on send or receive direction.

Status	
<ul style="list-style-type: none"> HGU STATUS Device Info WAN Info PON Info User Info 	
<ul style="list-style-type: none"> Network 	
ADVANCE SETTINGS <ul style="list-style-type: none"> Security Application Management Diagnostics 	

Connect information	
PON MODE	XGS-PON
Connect state	Initial State (O1)
FEC Upstream Status	Disable
FEC Downstream Status	Enable

Laser Device Info	
Tx Power	-inf dBm
Rx Power	-inf dBm
Temperature	51.078125 °C
Voltage	3.320300 V
Bias Current	0.000000 mA
PON Alarm Info	

Figure 3-2-6: PON Info

3.2.3.1 Connect information

This page shows the PON connection information and FEC information.

Connect information	
PON MODE	XGS-PON
Connect state	Initial State (O1)
FEC Upstream Status	Disable
FEC Downstream Status	Enable

Figure 3-2-7: Connection Info

3.2.3.2 Laser Device Info

This page shows the laser device information, including temperature, voltage, current, optical power.

Laser Device Info	
Tx Power	-inf dBm
Rx Power	-inf dBm
Temperature	51.078125 °C
Voltage	3.320300 V
Bias Current	0.000000 mA
PON Alarm Info	

Figure 3-2-8: Laser Device Info

3.2.3.3 Link Performance Info

This page shows statistics of the packet on send or receive direction.

Link Performance Info	
Tx Bytes	0
Rx Bytes	0
Tx Frame	0
Rx Frame	0
Tx Unicast Frame	0
Rx Unicast Frame	0
Tx Multicast Frame	0
Rx Multicast Frame	0
Tx Broadcast Frame	0
Rx Broadcast Frame	0
Rx FEC Error Frame	0
Rx HEC Error Frame	0
Tx Lose Frame	0
Tx PAUSE Control Frame	0
Rx PAUSE Control Frame	0

Figure 3-2-9: Link Performance Info

3.2.4 User Info

This page shows the user information for LAN, including LAN IP, LAN packets and DHCP clients.

The screenshot displays the user interface for the AirLive ONU-10XG(S)-1004-10G. On the left is a blue navigation sidebar with sections for 'Status' (containing HGU STATUS, Device Info, WAN Info, PON Info, and User Info), 'Network', 'ADVANCE SETTINGS' (containing Security and Application), and 'Management'. The main content area is divided into two sections: 'LAN Interface' and 'LAN Send and Recv'.

LAN Interface

IP Address	MAC Address
192.168.1.1	00:4f:5b:00:01:e6

LAN Send and Recv

Interface	Status	Rate	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dr (S)
LAN1	Up	2500Mb	210888	42929360	0	0	125024	93679248	0	0
LAN2	Down	-	0	0	0	0	0	0	0	0
LAN3	Down	-	0	0	0	0	0	0	0	0
LAN4	Down	-	0	0	0	0	0	0	0	0

Figure 3-2-10: User info

3.2.4.1 LAN Interface

This page shows LAN address and LAN gateway.

The screenshot shows the 'LAN Interface' section of the user interface. It contains a table with two columns: 'IP Address' and 'MAC Address'.

IP Address	MAC Address
192.168.1.1	00:4f:5b:00:01:e6

Figure 3-2-11: LAN Interface

3.2.4.2 LAN Interface Statistics

This page shows the statistics of received or sent packets of the LAN interface.

LAN Send and Recv										
Interface	Status	Rate	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dropped (Send)
LAN1	Down	-	0	0	0	0	19939	1605516	0	0
LAN2	Up	100Mb	13106	1435171	0	0	12659	1180872	0	0
LAN3	Down	-	0	0	0	0	0	0	0	0
LAN4	Down	-	0	0	0	0	0	0	0	0
LAN5	Down	-	0	0	0	0	0	0	0	0

Figure 3-2-12: LAN Interface Statistics

3.2.4.3 Active DHCP Clients

This page shows the lease information of the DHCP server.

Active DHCP Clients			
Device Name	MAC Address	IP Address	Lease Time

Figure 3-2-13: Active DHCP Clients

3.3 Network

3.3.1 WAN

This page is used to set up WAN connections, create a bridge or routing type WAN, and set the NAT type.

The screenshot displays the WAN Config page. On the left is a navigation menu with 'Status', 'Network', and 'Security' sections. Under 'Network', there are sub-sections for 'NETWORK SETTINGS' (WAN, LAN, MTU) and 'OTHERS' (Binding, TR069, QoS, Time, Route). The main content area is titled 'WAN Config' and contains the following fields:

- Connectin Name: Add New Wan
- Mode: Bridge
- IP Version: IPv4/IPv6
- Enabled Vlan:
- MTU: 1500
- ServiceMode: INTERNET
- Disable LAN DHCP:
- Bind Port: LAN_1, LAN_2, LAN_3, LAN_4, LAN_5

A blue 'Submit' button is located at the bottom of the configuration area. Below the WAN Config section, a 'NAT Config' section is partially visible.

Figure 3-3-1:WAN

3.3.1.1 WAN Config

This page allows you to add or modify WAN connections. You can't add any WAN connection if you have configured eight connections.

The screenshot shows the WAN Config interface with the following settings:

- Connectin Name:** Add New Wan (dropdown)
- Mode:** Bridge (dropdown)
- IP Version:** IPv4/IPv6 (dropdown)
- Enabled Vlan:**
- MTU:** 1500 (input field)
- ServiceMode:** INTERNET (dropdown)
- Disable LAN DHCP:**
- Bind Port:**
 - LAN_1
 - LAN_2
 - LAN_3
 - LAN_4
 - LAN_5

A blue **Submit** button is located at the bottom of the form.

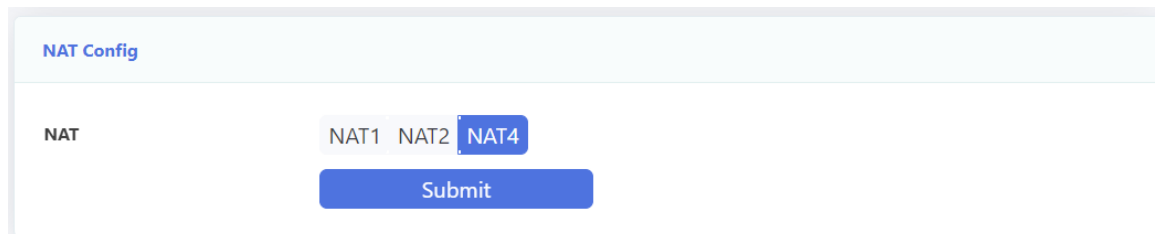
Figure 3-3-2:WAN config

Parameters	Illustration
Connection Name	This is the list table of WAN connection name. If you want to create a new WAN connection, please select “Add New Wan” and input other parameters at the same time and then click “Submit” button. If you want to edit WAN connection, please select the wan connect name you want to edit and change parameters and then click “Submit” button. If you want to delete one connection, please select the wan connection you want to delete and then click “Delete” button.
Mode	Bridge: The LAN ports you have selected in this WAN connection and PON port are in the bridge mode. Route: The LAN ports you have selected in this WAN connection and PON port are in the route mode.
IP Version	IPv4: WAN connections use IPv4 protocol. IPv6: WAN connections use IPv6 protocol. IPv4 / IPv6: WAN connections use both IPv4 and IPv6 protocol.
IP Mode	DHCP: Automatically obtain an IP address from your ISP Static: Set the IP address manually PPPoE: Select this option if your ISP uses PPPoE
Enable VLAN	unchecked: In this wan connection, the packets transmitted by the PON port without VLAN tag. checked: In this wan connection, the packets transmitted by the

	PON port with VLAN tag. VLAN ID: input the VLAN ID you want to set. 802.1p: select the port priority you want to set.
MTU	MTU: max transfer unit. Default Value: 1492 in route PPPoE mode, 1500 in other modes.
NAT	checked: enable NAT function unchecked: disable NAT function
Request DNS	Enable: DHCP server assigns DNS. Disable: set DNS manually.
Service Mode	Service mode indicates what the wan connection is used for.
Disable LAN DHCP	Checked: LAN DHCP will not work at the port which binds with the WAN. Unchecked: LAN DHCP will work at the port which binds with the WAN.
Bind Port	Showing which LAN port the wan connection has included.

3.3.1.2 NAT Config

This page allows you to set NAT type.



The screenshot shows a web interface for NAT configuration. At the top, there is a header 'NAT Config'. Below it, the word 'NAT' is displayed on the left. In the center, there are three tabs: 'NAT1', 'NAT2', and 'NAT4'. The 'NAT4' tab is highlighted with a blue border, indicating it is the active configuration. Below the tabs is a blue 'Submit' button.

Figure 3-3-3:NAT config

3.3.2 LAN

This page allows you to set up LAN, including IP, enable DHCP server, and reserve IP address for specific devices.

Figure 3-3-4: LAN

3.3.2.1 IPv4 LAN Configuration

This page allows you to do some LAN settings, such as LAN IP address, DHCP server.

Figure 3-3-5: IPv4 configuration

Parameters	Illustration
IP Address	LAN IP address.
Subnet Mask	LAN IP mask.

Disable DHCP Server	DHCP Server is disabled.
Enable DHCP Server	Enable ONU DHCP server. Start IP Address: The start IP address of address pool. End IP Address: The end IP address of address pool. Lease Time: Lease time of the IP address. LAN DNS Mode: Select the mode to obtain DNS.

3.3.2.2 Reserve IP Address List

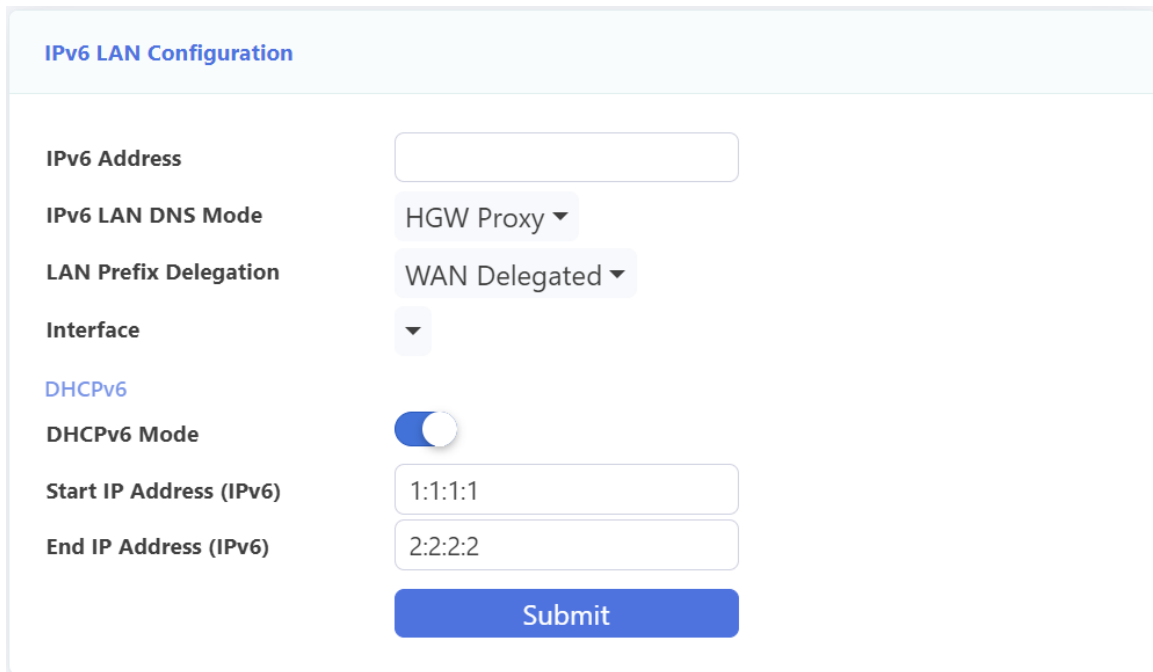
This page allows you to add a reserved IP address in the DHCP server. Click “Add” button to configure IP address you want to reserve. If you want to delete one reserve IP configuration, select the reserve IP address you want to delete and then click “Delete Selected” button.

The screenshot shows a web interface for managing reserved IP addresses. At the top, there is a header bar with the text "Reserve IP Address List". Below this is a table with two columns: "MAC Address" and "IP Address". Below the table, there are two buttons: a teal "Add" button and a red "Delete Selected" button.

Figure 3-3-6:Reserve IP

3.3.2.3 IPv6 LAN Configuration

This page allows you to configure LAN IPv6 address, LAN IPv6 DNS, IPv6 prefix and IPv6 DHCP server. When IPv6 DHCP server is disabled, it is auto configure mode.

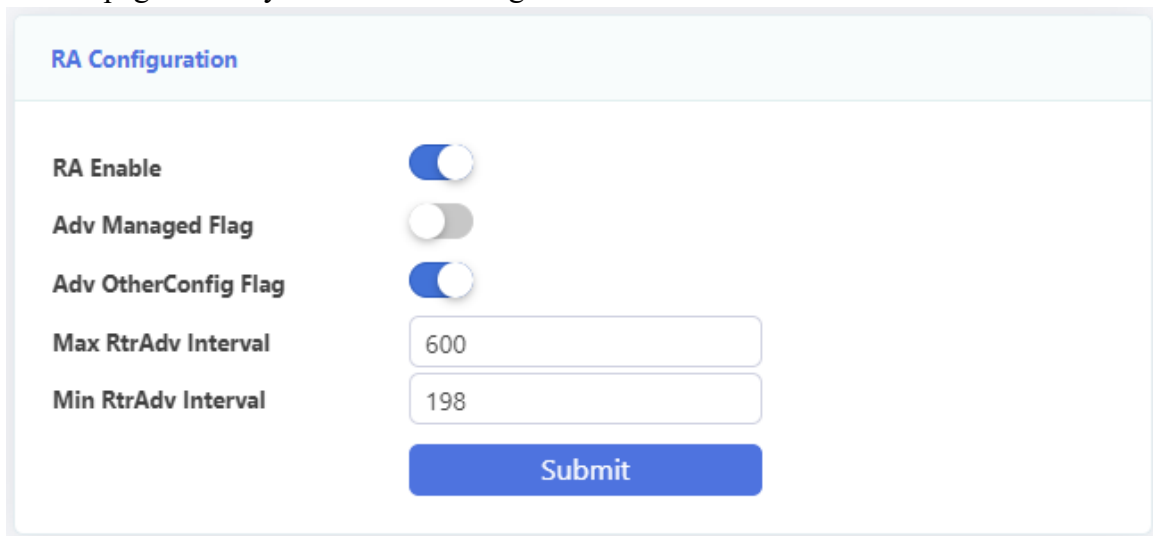


The screenshot shows the 'IPv6 LAN Configuration' page. It features several configuration options: 'IPv6 Address' (empty text box), 'IPv6 LAN DNS Mode' (dropdown menu set to 'HGW Proxy'), 'LAN Prefix Delegation' (dropdown menu set to 'WAN Delegated'), and 'Interface' (dropdown menu). Under the 'DHCPv6' section, 'DHCPv6 Mode' is a toggle switch that is turned on. Below this, 'Start IP Address (IPv6)' is set to '1:1:1:1' and 'End IP Address (IPv6)' is set to '2:2:2:2'. A blue 'Submit' button is located at the bottom of the configuration area.

Figure 3-3-7: IPv6 configuration

3.3.2.4 RA Configuration

This page allows you to do RA configuration.



The screenshot shows the 'RA Configuration' page. It includes the following settings: 'RA Enable' (toggle switch turned on), 'Adv Managed Flag' (toggle switch turned off), and 'Adv OtherConfig Flag' (toggle switch turned on). The 'Max RtrAdv Interval' is set to '600' and the 'Min RtrAdv Interval' is set to '198'. A blue 'Submit' button is positioned at the bottom of the configuration section.

Figure 3-3-8: RA configuration

3.3.3 MTU

This page allows you to set system MTU.

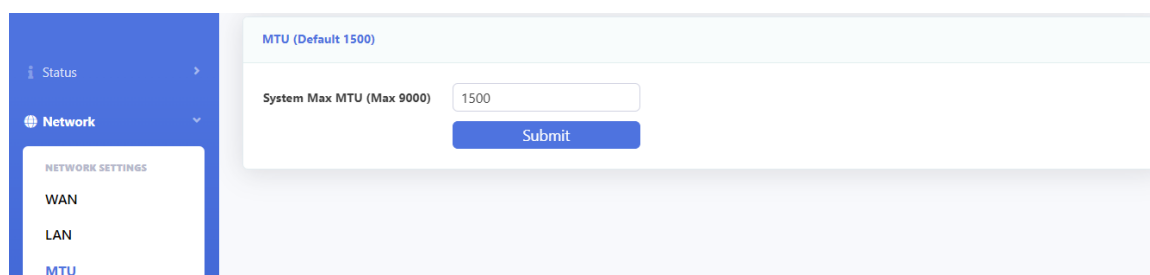


Figure 3-3-9: MTU

3.3.4 Binding Settings

This page is used to configure binding mode, which contains port binding and VLAN binding.

When using port binding, traffic of the LAN port will transmit to the WAN which binds this port; when using VLAN binding, traffic of the LAN port will transmit to the WAN which configured the same VLAN.

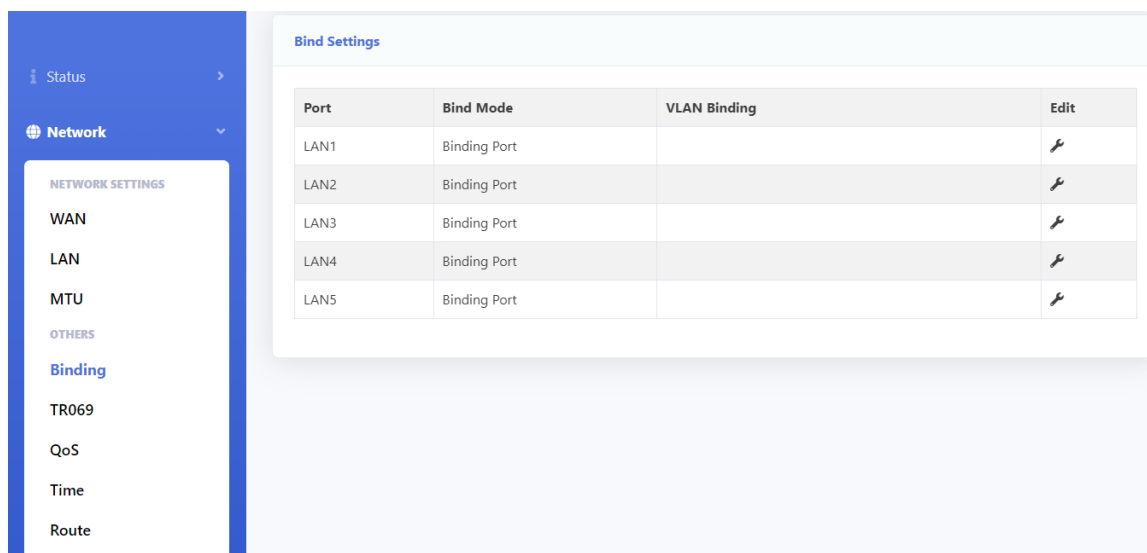


Figure 3-3-10: Binding Settings

3.3.5 TR069

This page allows you to configure Tr069-related parameters.

The screenshot displays the 'TR069 Client Configuration' interface. On the left, a blue sidebar contains a 'Network' menu with sub-items: NETWORK SETTINGS (WAN, LAN, MTU), OTHERS (Binding, TR069, QoS, Time, Route), ADVANCE SETTINGS (Security, Application, Management). The main panel is divided into three sections: 'TR069 Client Configuration', 'LOID Config', and 'PonPwd Config'. The TR069 section includes:

- EnableTR069**: A toggle switch that is currently turned on.
- Server URL**: A text input field containing 'http://'.
- Username**: A text input field containing 'username'.
- Password**: A password input field with masked characters and a visibility icon.
- Enable Certificate**: A toggle switch that is currently turned off.
- Periodic Report**: A toggle switch that is currently turned on.
- Periodic Report Interval(s)**: A text input field containing '43200'.
- Connect Request Username**: An empty text input field.
- Connect Request Password**: A password input field with masked characters and a visibility icon.
- Submit**: A blue button at the bottom of the TR069 section.

 The LOID Config section includes:

- LOID**: A text input field containing '123456789'.
- Password**: A password input field with masked characters and a visibility icon.
- Submit**: A blue button at the bottom of the LOID Config section.

 The PonPwd Config section is currently empty.

Figure 3-3-11: TR069

3.3.5.1 ACS Client Configuration

This page allows you to configure ACS connection parameters.

This screenshot shows a detailed view of the 'TR069 Client Configuration' section. The fields and their states are:

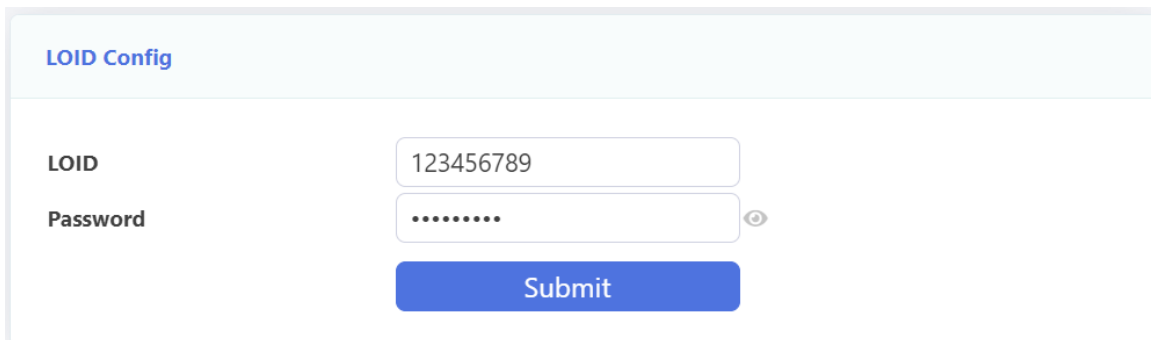
- EnableTR069**: Toggle switch (ON).
- Server URL**: Text input field (http://).
- Username**: Text input field (username).
- Password**: Password input field (masked).
- Enable Certificate**: Toggle switch (OFF).
- Periodic Report**: Toggle switch (ON).
- Periodic Report Interval(s)**: Text input field (43200).
- Connect Request Username**: Empty text input field.
- Connect Request Password**: Password input field (masked).
- Submit**: Blue button at the bottom.

Figure 3-3-12: ACS Client Configuration

Parameter	Illustration
Server URL	Server provider's ACS server.
Username	Authentication username for ONU connects to ACS server.
Password	Authentication password for ONU connects to ACS server.
Enable Certificate	Whether needs certificates or not.
Periodic Report	Switch of inform interval.
Periodic Report Interval	Reconnection interval. ONU will verify connection with ACS server when inform interval times up.
Connect Request Username	Authentication username for ACS connects to ONU.
Connect Request Password	Authentication password for ACS connects to ONU.

3.3.5.2 LOID Config

LOID is used for PON authentication.

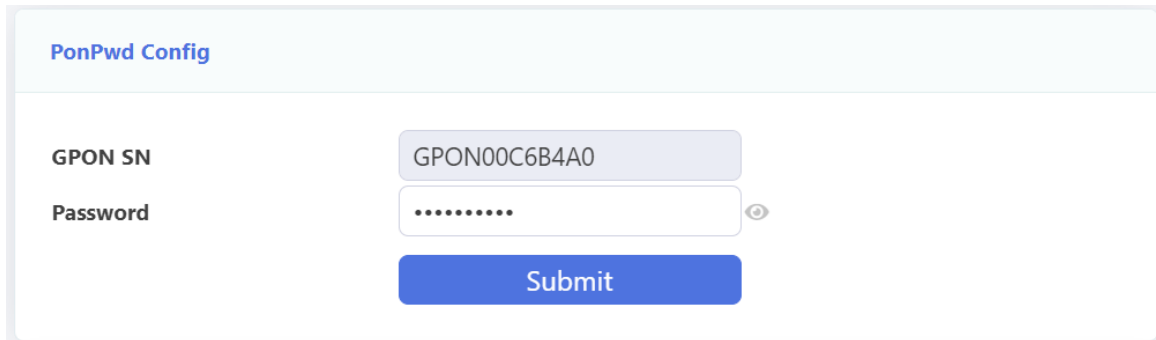


The screenshot shows a web interface for LOID configuration. At the top, the title "LOID Config" is displayed in blue. Below the title, there are two input fields. The first field is labeled "LOID" and contains the text "123456789". The second field is labeled "Password" and contains masked characters ".....". To the right of the password field is a small eye icon. Below these fields is a blue button labeled "Submit".

Figure 3-3-13: LOID configuration

3.3.5.3 PonPwd Config

GPON PLOAM Password is used for the registration and distribution of the new device, please do not change it. Restart the gateway if changing the Password causes business to malfunction.



PonPwd Config

GPON SN GPON00C6B4A0

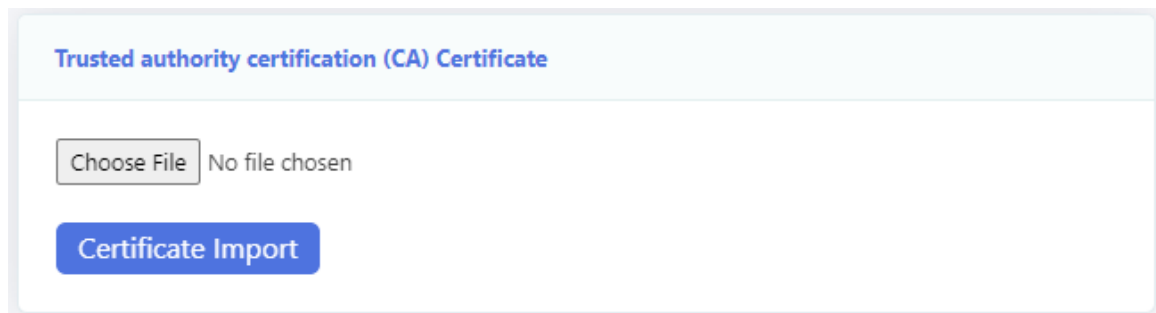
Password

Submit

Figure 3-3-14: Password configuration

3.3.5.4 CA Certificate

This page is used to upload CA certificate. Choose a CA certificate file and click “Certificate Import” button to upload.



Trusted authority certification (CA) Certificate

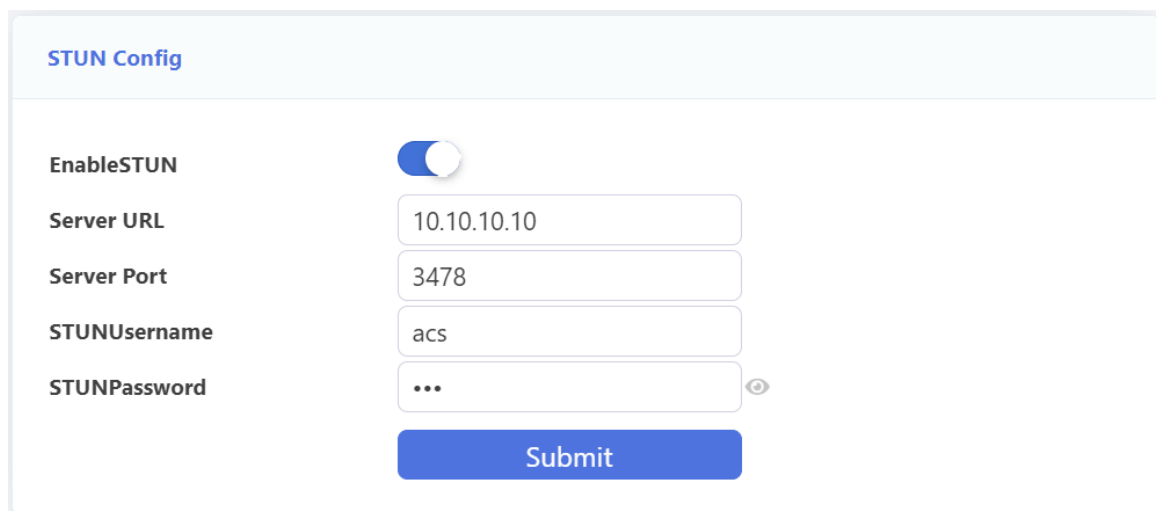
Choose File No file chosen

Certificate Import

Figure 3-3-15: Upload CA certificate

3.3.5.5 STUN

This page is used to set the STUN server parameter. It can make your ONU to connect the ACS pass through NAT.



STUN Config

EnableSTUN

Server URL 10.10.10.10

Server Port 3478

STUNUsername acs

STUNPassword ...

Submit

Figure 3-3-16: STUN Config

3.3.6 Qos

This page allows you to configure QoS config, QoS Classification and QoS Traffic Control.

The screenshot displays the QoS configuration page. On the left is a navigation menu with 'Network' selected, containing sub-items like WAN, LAN, MTU, Binding, TR069, QoS, Time, and Route. The main content area is divided into two sections: 'QoS Config' and 'QoS Classification'.

QoS Config: Features a toggle for 'IP QoS' (turned on) and a dropdown for 'QoS Policy' (set to 'PRIO'). Below is a table with the following data:

Queue	PRIO
Q1	1
Q2	2
Q3	3
Q4	4

A 'Submit' button is located below the table.

QoS Classification: Shows a table with 16 columns: ID, Name, DSCP Mark, IP Priority, 802.1P Mark, LAN Port, Protocol, DSCP, Source IP/Subnet Mask, Source Port, Destination IP/Subnet Mask, DestinationPort, Source MAC, Destination MAC, 802.1P, IP Version, and Connect Type. An 'Add' button is positioned below the table header.

Figure 3-3-17: Qos

3.3.6.1 Qos Config

This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply greater precedence. If select WRR of policy, please input the weight of this queue. After configuration, please click 'Submit'.

This figure provides a closer look at the 'QoS Config' section. It includes the 'IP QoS' toggle switch, the 'QoS Policy' dropdown menu (set to 'PRIO'), and the queue configuration table. The table lists four queues (Q1, Q2, Q3, Q4) with their respective priorities (1, 2, 3, 4). A 'Submit' button is located at the bottom of the configuration area.

Figure 3-3-18: QoS Config

3.3.6.2 QoS Classification

This page is used to configure the QoS classification. Click on the "Add" button to add the network traffic control type rules.

ID	Name	DSCP Mark	IP Priority	802.1P Mark	LAN Port	Protocol	DSCP	Source IP/ Subnet Mask	Source Port	Destination IP/ Subnet Mask	DestinationPort	Source MAC	Destination MAC	802.1P	IP Version	Connect Type
Add																

Figure 3-3-19: QoS Classification

Add IP QoS Traffic Shaping Rule

IP protocol version IPv4 ▼

Flow control type name

Specify IP Priority Tags Queue 1 ▼

Specify DSCP Tag ▼

If the WAN port 802.1p is ena... ▼

ModE Selection General mode ▼

Physical LAN Port LAN1 ▼

Protocol ▼

DSCP Check ▼

802.1p Priority ▼

Source IP Address

The source subnet mask

Destination IP Address

The destination subnet mask

Source Port (port or port:port)

Figure 3-3-20: QoS rule

parameter	illustration
IP protocol version	Select IPv4 or IPv6.
Flow control type name	Input this rule name.
Specify IP Priority Tags	Select queue.
Specify DSCP Tag	Select DSCP tag.
If the WAN port 802.1p is enabled, set the 802.1p value	If 802.1p is set in the WAN, set the 802.1p value.

Mode Selection	Select the general mode or the application type.
Physical LAN Port	Select the physical LAN port to which this rule applies.
Protocol	Select Protocol.
DSCP Check	Select DSCP Check mark.
802.1p Priority	Input 802.1p Priority.
Source IP Address	Input source IP address.
The source subnet mask	Input the source subnet mask.
Destination IP Address	Input destination IP address.
The destination subnet mask	Input the destination subnet mask.
Source Port (port or port:port):	Input source port.
Destination Port (port or port:port):	Input destination port.
Source MAC (xx:xx:xx:xx:xx:xx)	Input source MAC.
Destination MAC (xx:xx:xx:xx:xx:xx)	Input destination MAC.

3.3.6.3 QoS Traffic Control

This page allows you to QoS traffic control, click the "Add" button to add network traffic control type rules.

QoS Traffic Control

Total Bandwidth Limit Enable

Total Bandwidth Limit

ID	Protocol	Source Port	DestinationPort	Source IP/ Subnet Mask	Destination IP/ Subnet Mask	Rate(kb/s)	IP Version	Direction
<input type="button" value="Add"/> <input type="button" value="Delete Selected"/>								

Figure 3-3-21: QoS Traffic Control

Figure 3-3-22: QoS Traffic Control Shaping Rule

parameter	illustration
Total Bandwidth Limit Enable	Select whether to enable the total bandwidth limit.
Total Bandwidth Limit	Input the total bandwidth that you want to limit.
IP Version	Select IPv4 or IPv6.
Direction	Select upstream or downstream.
Protocol	Select protocol.
Source IP	Input source IP address.
Source Mask	Input the source subnet mask.
Destination IP	Input destination IP address.
Destination Mask	Input the destination subnet mask.
Source Port	Input source port.
Destination Port	Input destination port.
Rate Limit	Input the limit rate.

3.3.7 Time

This page allows you to configure time related parameters of your router. After you have selected the check box, select the time server and time zone you want to set and then click the “Submit” button to save.

The screenshot shows the 'Time' configuration page. On the left is a navigation menu with 'Time' selected. The main content area is titled 'Time' and displays the current time as 'Sat Jan 3 00:01:48 CST 1970'. Below this are several settings: 'Enable SNTP Client Update' (checked), 'Time Zone Select' (Asia/Shanghai (GMT+08:00)), 'Enable Daylight Saving Time' (checked), 'NTP PrimaryTimeServer' (clock.fmt.he.net), 'NTP StandbyTimeServer' (clock.nyc.he.net), 'Sync Channel' (INTERNET), 'Sync with WAN' (unchecked), and 'Interval' (86400). A 'Submit' button is at the bottom.

Figure 3-3-23: Time server

3.3.8 Route

This page allows you to configure some route-related configurations.

The screenshot shows the 'Route' configuration page. On the left is a navigation menu with 'Route' selected. The main content area is titled 'RIP' and has 'RIP Enable' turned off. Below this is a section for 'Please input configuration' with fields for 'Interface' (br0), 'Receive Mode' (None), and 'Send Mode' (NONE). An 'Add' button is below these fields. A table below the 'Add' button has columns for 'Interface', 'Receive Mode', and 'Send Mode'. Below the table are 'Delete Selected' and 'Delete All' buttons. The 'Static Route' section below has a table with columns for 'Status', 'Destination', 'Subnet Mask', 'Gateway', 'Metric', and 'Interface'. Below the table are 'Add' and 'Show Routes' buttons.

Figure 3-3-24: Route

3.3.8.1 RIP Configuration

This page allows you to configure RIP function.

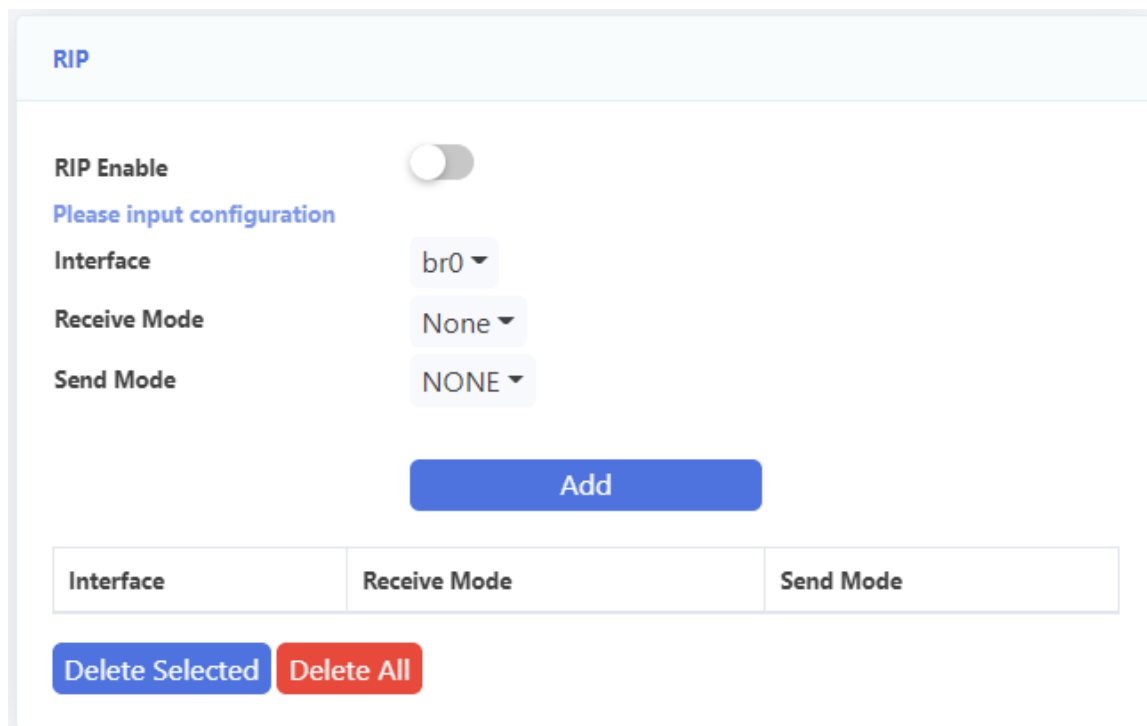


Figure 3-3-25: RIP configuration

Parameter	Illustration
RIP	RIP switch.
Interface	WAN connection for transmitting or receiving RIP messages.
Receive Mode	The version of RIP messages that have been received.
Send Mode	The version of RIP messages that have been sent.
RIP configuration table	RIP configuration that has been added.

3.3.8.2 Static route

This page allows you to configure static routing, click “Add” to configure routing rules.

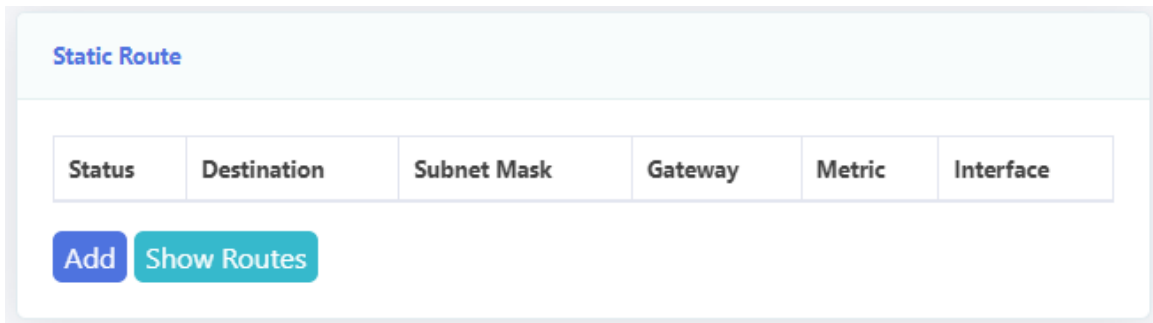


Figure 3-3-26: Static route

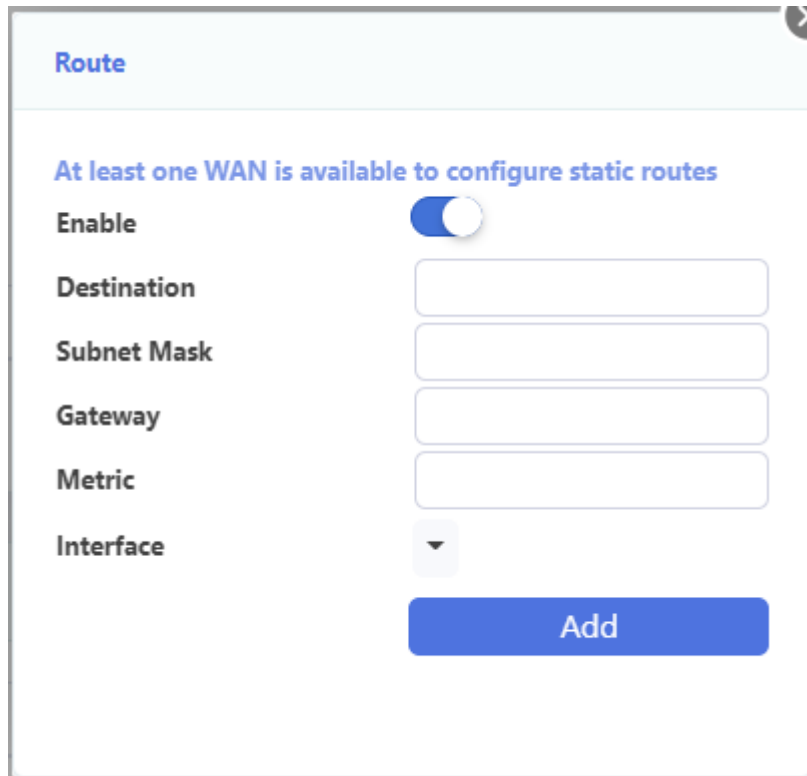


Figure 3-3-2: Static Route configuration

Parameter	Illustration
Enable	Switch of static route.
Destination	Destination network address.
Subnet Mask	Destination network mask.
Gateway	The gateway IP address.
Metric	It is used to determine the optimal route when searching for a route. Its value range is 0~16.
Interface	Select the wan interface you want to add static route

3.4 Security

3.4.1 URL Filtering

This page allows you to configure URL filter. URL filter is taking effect when the wan connection is in router mode. In other words, when the wan connection is in bridge mode, the URL filter cannot be taken effect.

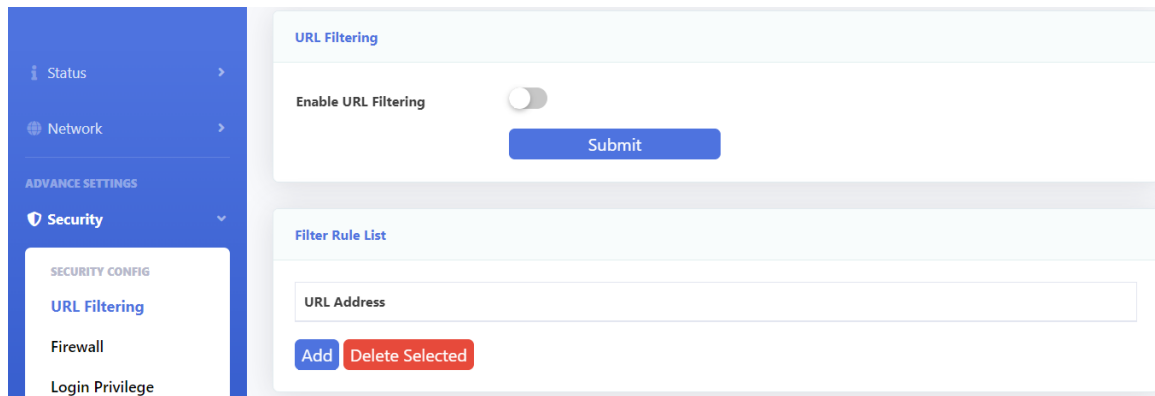


Figure 3-4-1: URL Filter

Parameter	Illustration
Enable URL Filtering	Enable or Disable URL Filter.
Filtering Mode	Black List: URL in the list will be forbidden and others will be accessed. White List: URL in the list will be accessed and others will be forbidden.
URL List	URL List you want to deal with (Drop or Access). Click “Add” button to add URL item to the list. Select “Delete” checkbox and then click “Delete Selected” button to remove URL address from the list.

3.4.2 Firewall

This page allows you to configure the firewall level and attack protection status. Firewall has two levels: Low and High.

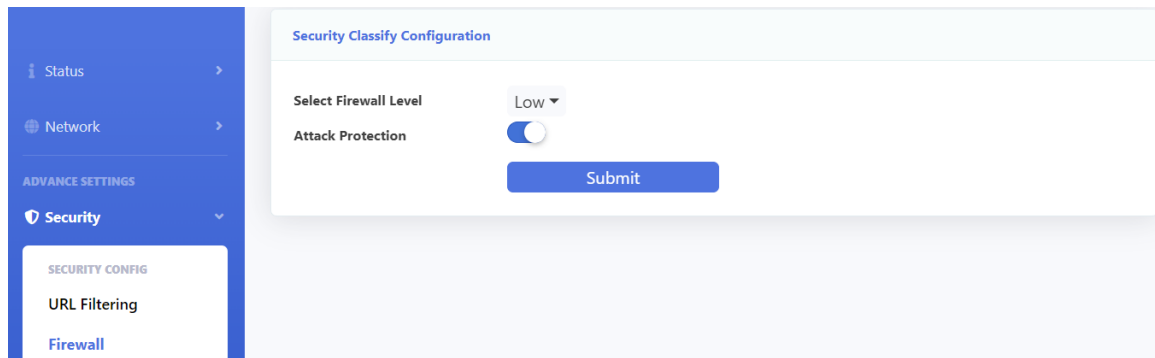


Figure 3-4-2: Security Classify

Parameter	Illustration
Firewall Level	Low: Protect nothing. High: Forbid ICMP Input, Forbid Port Scan, Denial of Service protections.

3.4.3 Login Privilege

This page is used to configure the access control and common ports on the upstream and downstream directions. By default, ONU can't be accessed from WAN side by telnet, web and so on.

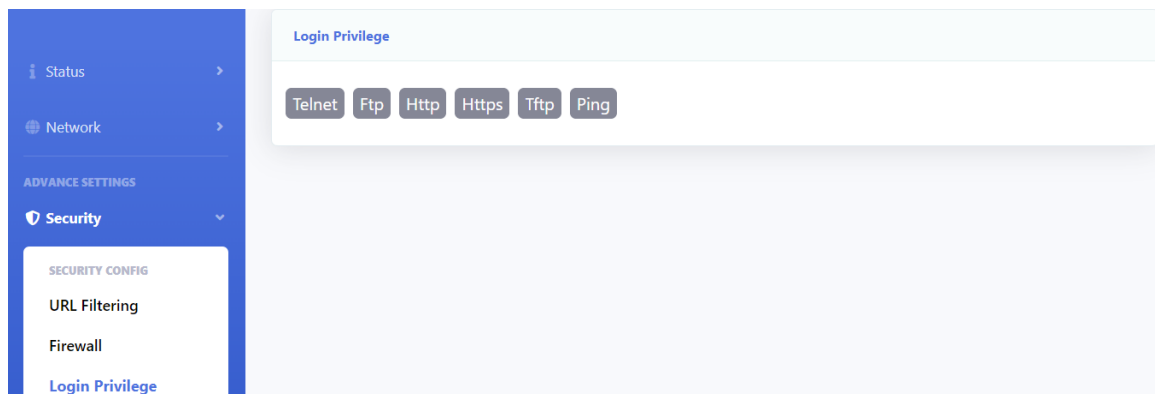


Figure 3-4-3: Login Privilege

3.4.4 MAC Filtering

This page allows you to configure MAC filter. Mac filter is different from URL filter, which is nothing to do with the wan connection mode. When packets input the LAN port, the packets will be dropped or accessed depends on the MAC filter rules.

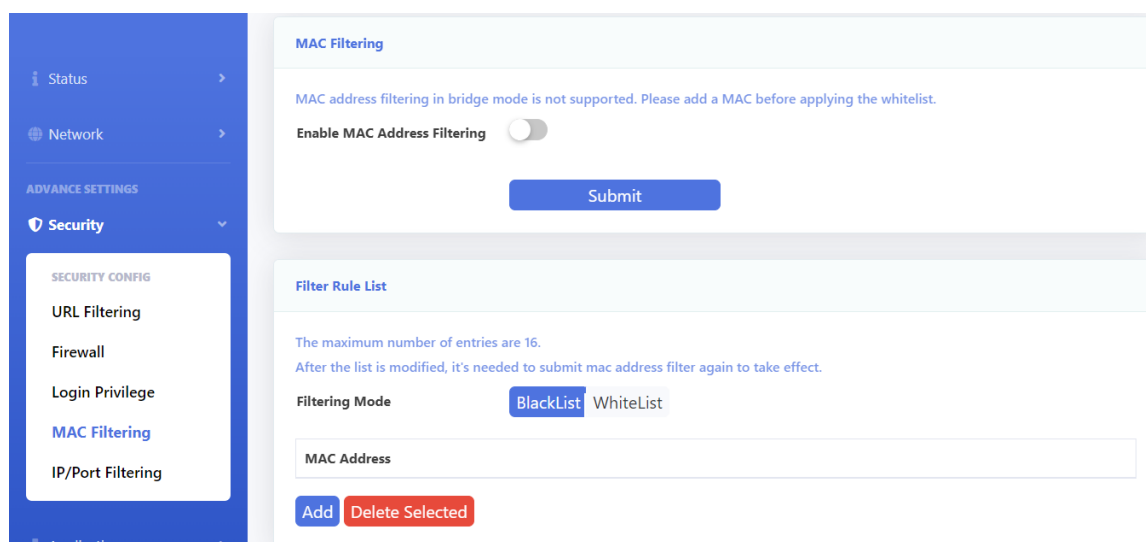


Figure 3-4-4: MAC Filtering

Parameter	Illustration
Enable Mac Address Filtering	unchecked: Disable Mac Filter. checked: Enable Mac Filter.
Filtering Mode	Black List: MAC Address in the list will be forbidden and others will be accessed. White List: Mac Address in the list will be accessed and others will be forbidden.
MAC Address	Input the MAC address and click the “Add” button to add MAC address to the table. Select “Delete” checkbox and then click “Delete Selected” button to remove MAC address from the table.

3.4.5 IP/Port Filtering

This page is used to configure port filter. Port filter includes many kinds of filters, such as IP filter, protocol filter and port filter. Black list and white list take effect simultaneously.

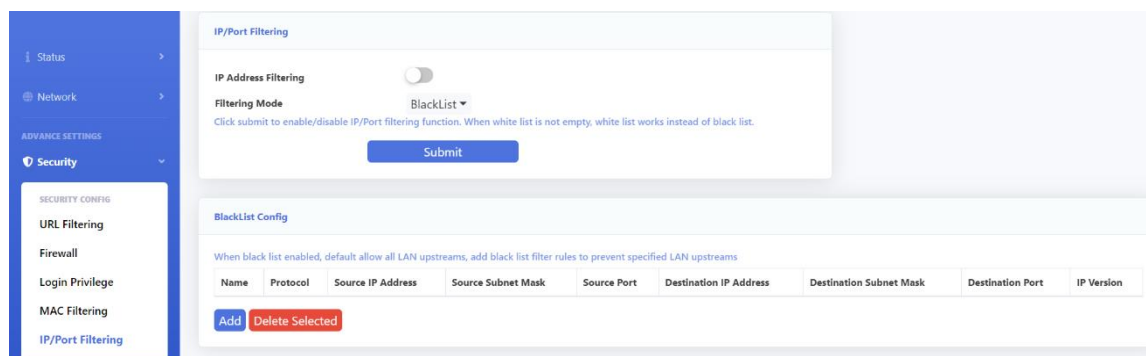


Figure 3-4-5: Ip / Port Filter

Figure 3-4-6: Port Filter -Incoming

Parameter	Illustration
IP Address Filtering	Switch of IP/port filtering.
Filter Mode	Black List: Rule in the list will be forbidden and others will be accessed. White List: Rule in the list will be accessed and others will be forbidden.
Filter Rule Settings	
Filter Name	Input filter name.
IP Version	IPv4 or IPv6.
Protocol	Input the protocol you want to configure in the rule.
Source IP Address	Input the source IP address you want to configure in the rule.
Source Subnet Mask	Input the mask of source IP address. Only need to configure

	when using single IP address.
Destination IP Address	Input the destination IP address you want to configure in the rule.
Destination Subnet Mask	Input the mask of destination IP address. Only need to configure when using single IP address.
Source Port	Input the source port you want to configure in the rule.
Destination Port	Input the destination port you want to configure in the rule.

3.5 Application

3.5.1 Multicast Setting

This page allows you to configure multicast-related parameter.

Interface	Multicast Vlan
1_TR069_R_VID_46	

Figure 3-5-1: Multicast Setting

3.5.1.1 IGMP Snooping Configuration

This page allows you to enable or disable the IGMP Snooping function.

Figure 3-5-2: IGMP Snooping

3.5.1.2 IGMP Proxy

This page allows you to enable IGMP proxy for a specified WAN connection. IGMP proxy takes effect for route mode WAN.

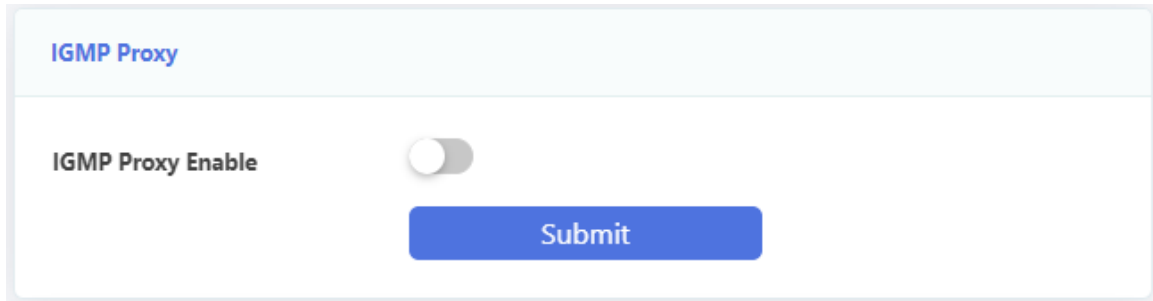


Figure 3-5-3: IGMP Proxy

3.5.1.3 MLD Snooping

This page allows you to enable or disable the MLD snooping function for IPv6, just like the IGMP snooping for IPv4.

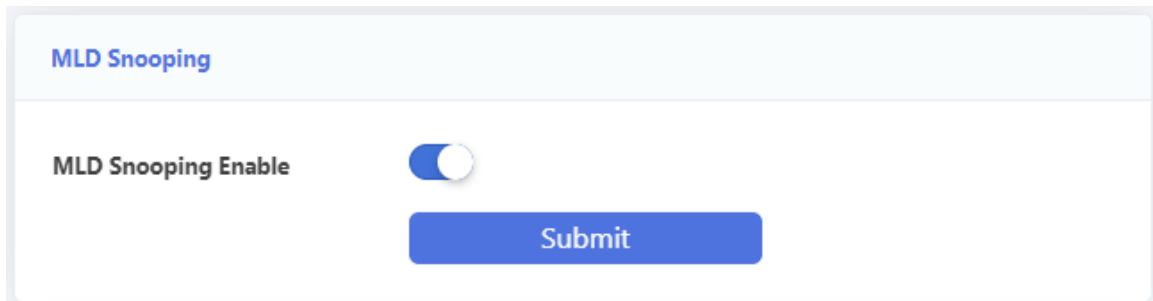


Figure 3-5-4: MLD Snooping

3.5.1.4 MLD Proxy

This page allows you to enable MLD proxy for IPv6, just like enable IGMP proxy for IPv4.

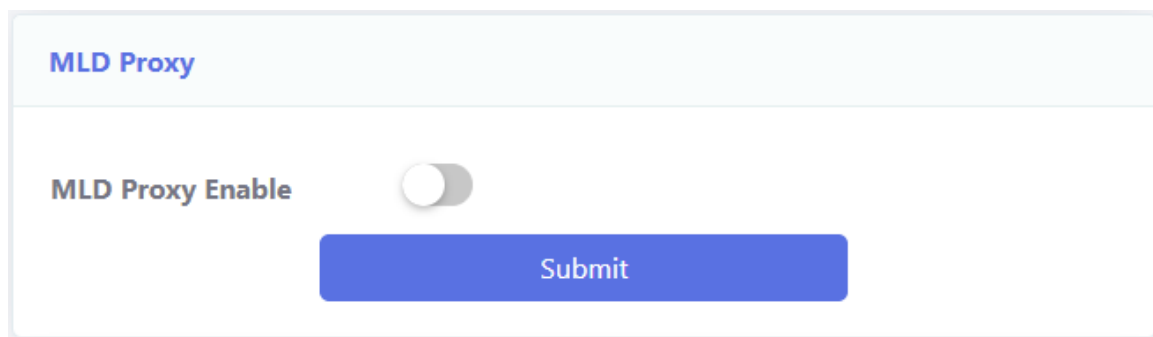


Figure 3-5-5: MLD Proxy

3.5.1.5 IPTV

This page allows you to configure multicast VLAN for WAN connections. Click the corresponding WAN name to add VLAN.

IPTV	
Interface	Multicast Vlan
1_TR069_R_VID_46	

Figure 3-5-6: IPTV

Multicast VLAN (blank indicates no setting)

1_TR069_R_VID_46

Submit

Figure 3-5-7: Multicast VLAN

3.5.2 Advance NAT

This page allows you to configure some advanced NAT settings such as Application Firewall, DMZ host, virtual server.

- Status
- Network
- ADVANCE SETTINGS
 - Security
 - Application
 - APPLICATION CONFIG
 - Multicast Setting
 - Advance NAT
 - Others
 - Management
 - Diagnostics

ALG

ftp

tftp

h323

rtsp

l2tp

ipsec

sip

pptp

Submit

DMZ Hosts

DMZ Host

Submit

Figure 3-5-8: Advance NAT

3.5.2.1 ALG

This page shows about ALG settings, such as h.323, SIP, RTSP, IPSEC, FTP, L2TP and so on.

The ALG configuration interface displays a list of protocols with their corresponding toggle switches. All switches are currently turned on. A blue 'Submit' button is located at the bottom of the list.

Protocol	Status
ftp	On
tftp	On
h323	On
rtsp	On
l2tp	On
ipsec	On
sip	On
pptp	On

Submit

Figure 3-5-9: ALG configuration

3.5.2.2 DMZ Hosts

This page allows you to configure DMZ server.

The DMZ Hosts configuration interface features a single 'DMZ Host' toggle switch, which is currently turned off. A blue 'Submit' button is positioned below the toggle.

DMZ Host	Status
DMZ Host	Off

Submit

Figure 3-5-10: DMZ configuration

3.5.2.3 Virtual Server Configuration

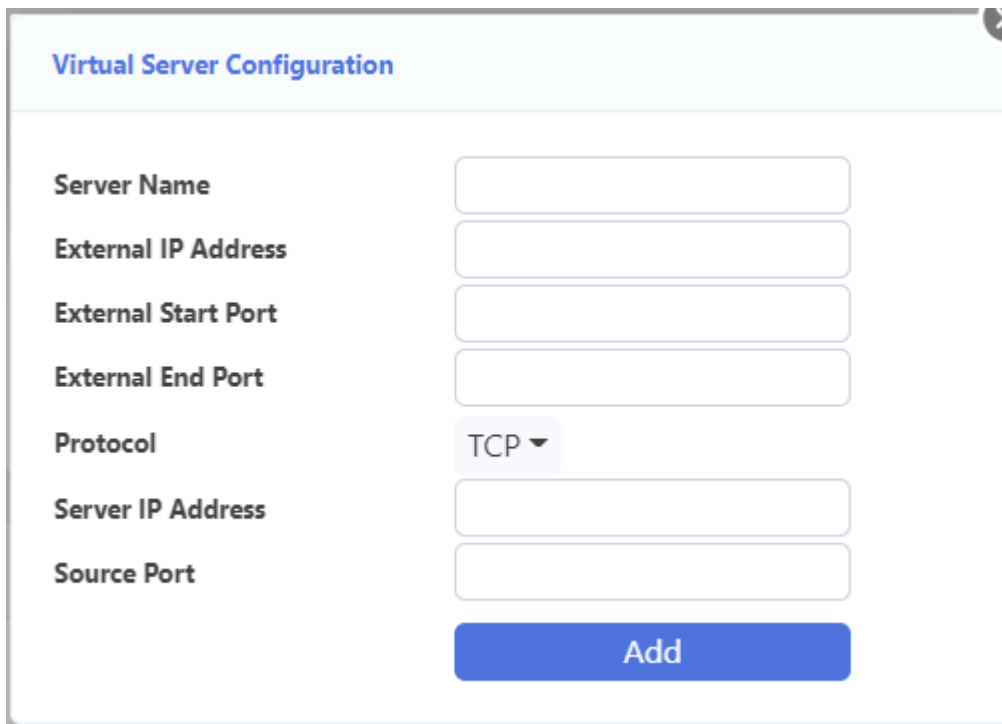
This page allows you to configure virtual server. After you click the “Add” button, you will see the configuration page.

The Virtual Server Configuration interface displays a table with the following columns: Server Name, External IP Address, External Start Port, External End Port, Protocol, Server IP Address, and Source Port. Below the table are two buttons: 'Add' (blue) and 'Delete Selected' (red).

Server Name	External IP Address	External Start Port	External End Port	Protocol	Server IP Address	Source Port

Add Delete Selected

Figure 3-5-11: Add Virtual Server



The screenshot shows a dialog box titled "Virtual Server Configuration". It contains several input fields and a dropdown menu. The fields are: "Server Name", "External IP Address", "External Start Port", "External End Port", "Server IP Address", and "Source Port". The "Protocol" field is a dropdown menu currently set to "TCP". A blue "Add" button is located at the bottom right of the dialog box.

Figure 3-5-12: Virtual Server configuration

You can select the “delete” checkbox and then click the “Delete Selected” button to remove service items from the service table.

3.5.3 Others

This page allows you to configure some other settings, including Dynamic DNS, UPnP, USB settings

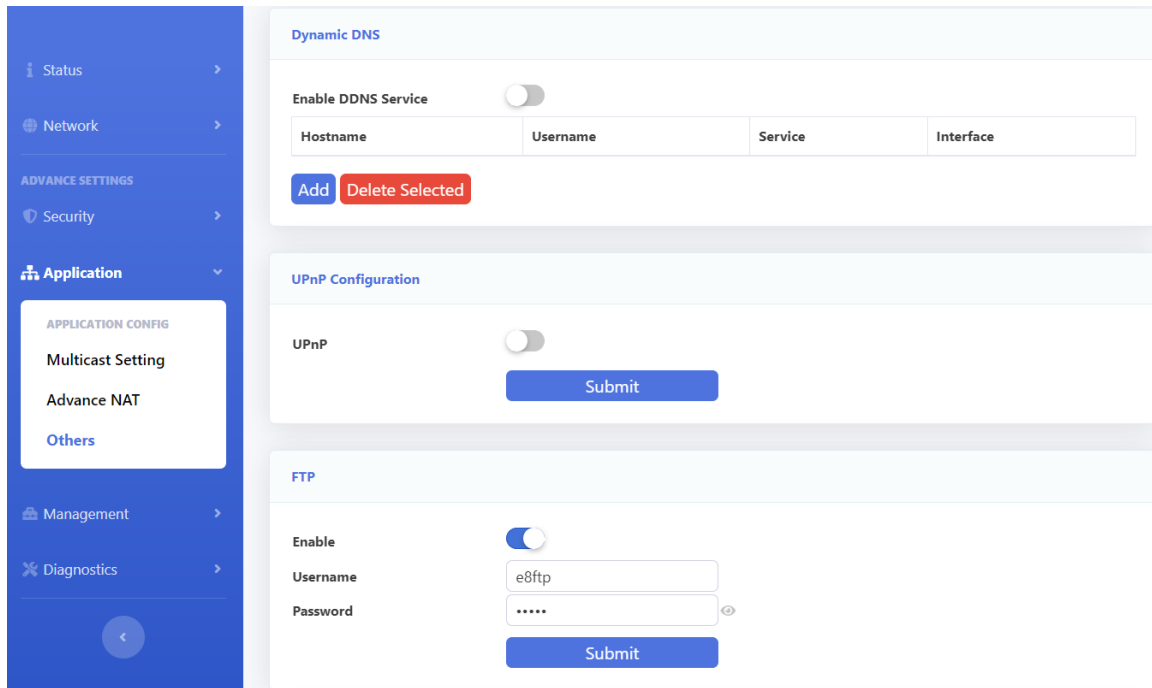


Figure 3-5-13: Other

3.5.3.1 Dynamic DNS

Dynamic DNS services allow you to change a dynamic IP address to a static host name in any multiple domains, allowing your router to be more easily accessed from different locations on the Internet.

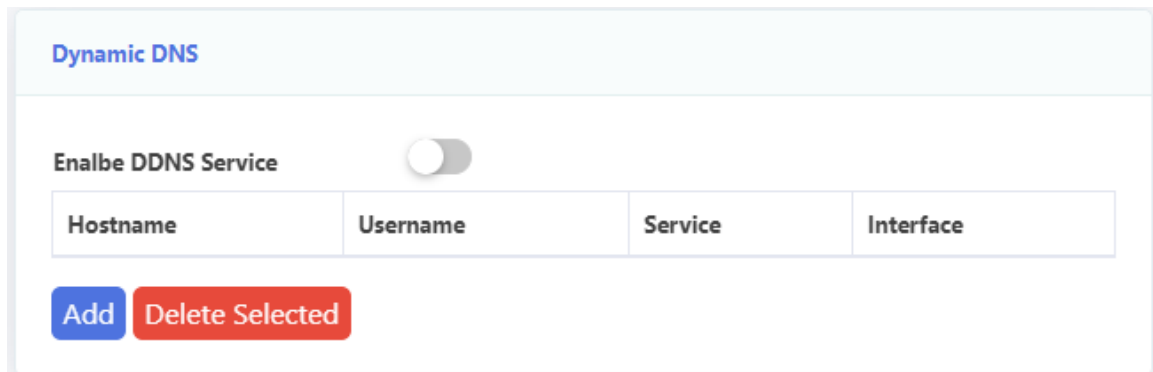


Figure 3-5-14: Add DDNS

Figure 3-5-15: DDNS configuration

Parameter	Illustration
DDNS Provider	Choose DDNS service provider.
Hostname	Set host name of the device.
Interface	The interface of accessing by DDNS.
Username	The username which is used to access DDNS server.
Password	The password which is used to access DDNS server.

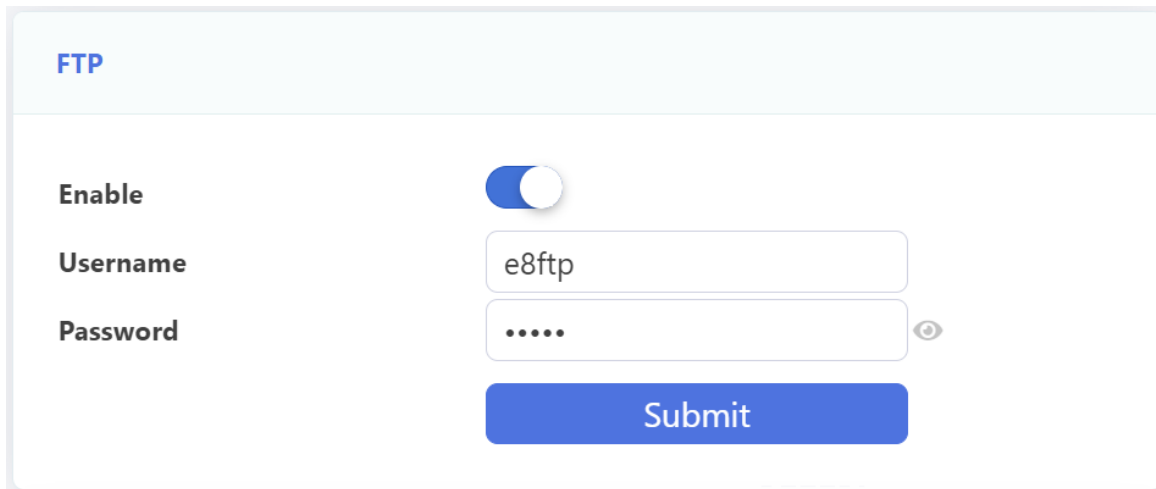
3.5.3.2 UPNP Configuration

This page is used to configure UPNP.

Figure 3-5-16: UPNP configuration

3.5.3.3 FTP


This page is used to configure FTP.



FTP

Enable

Username

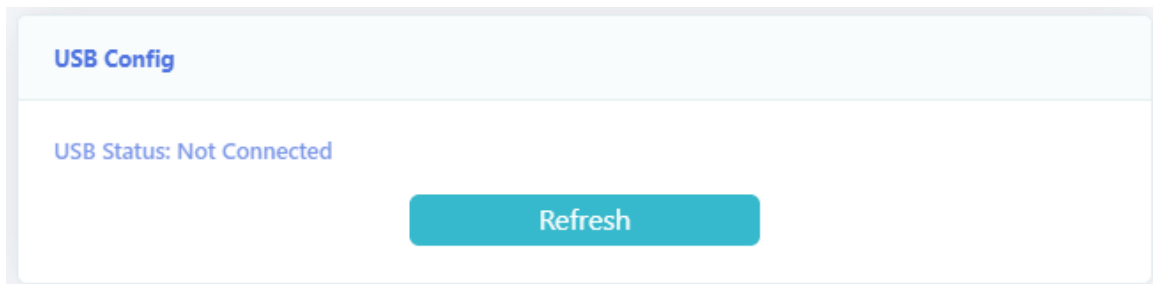
Password 

Submit

Figure 3-5-17: FTP configuration

3.5.3.4 USB Config

This page is used to configure USB.



USB Config

USB Status: Not Connected

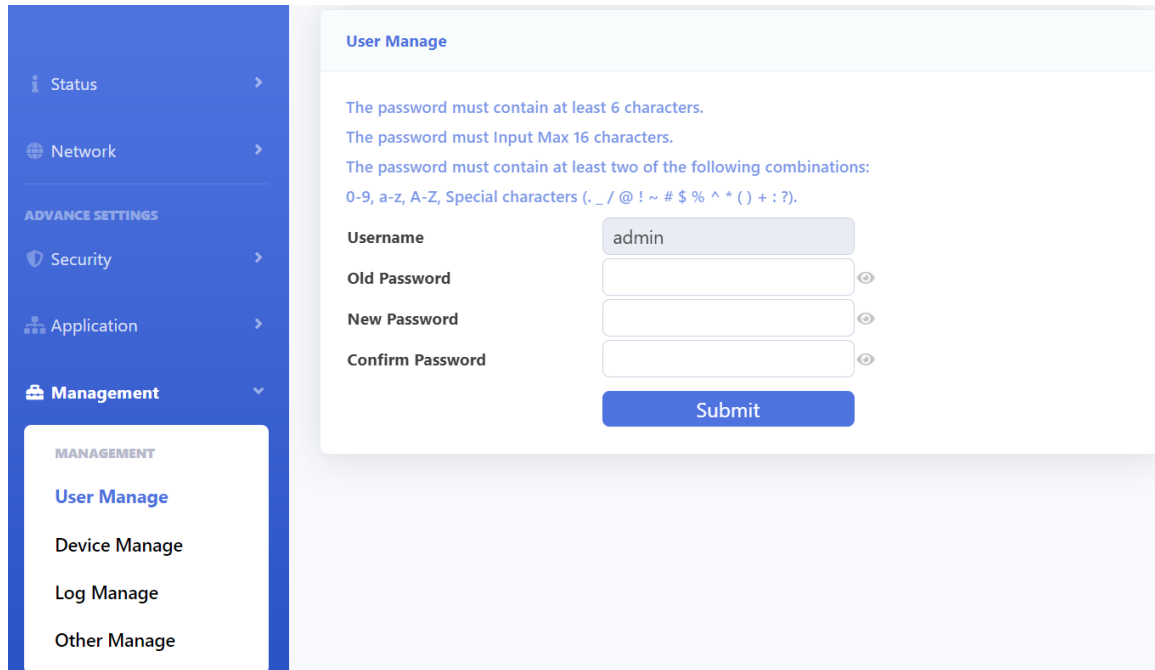
Refresh

Figure 3-5-18: USB configuration

3.6 Management

3.6.1 User Manage

This page allows you to change login password of current user.



The screenshot displays the 'User Manage' interface. On the left is a blue sidebar with navigation options: Status, Network, ADVANCE SETTINGS, Security, Application, and Management. Under 'Management', 'User Manage' is selected. The main content area shows the 'User Manage' title and three password requirements: 'The password must contain at least 6 characters.', 'The password must Input Max 16 characters.', and 'The password must contain at least two of the following combinations: 0-9, a-z, A-Z, Special characters (. _ / @ ! ~ # \$ % ^ * () + : ?)'. Below these are input fields for 'Username' (containing 'admin'), 'Old Password', 'New Password', and 'Confirm Password', each with a toggle icon. A blue 'Submit' button is at the bottom.

Figure 3-6-1: User management

3.6.2 Device Manage

This page allows you to manage devices, including upgrade, restart, restore factory default configuration, etc

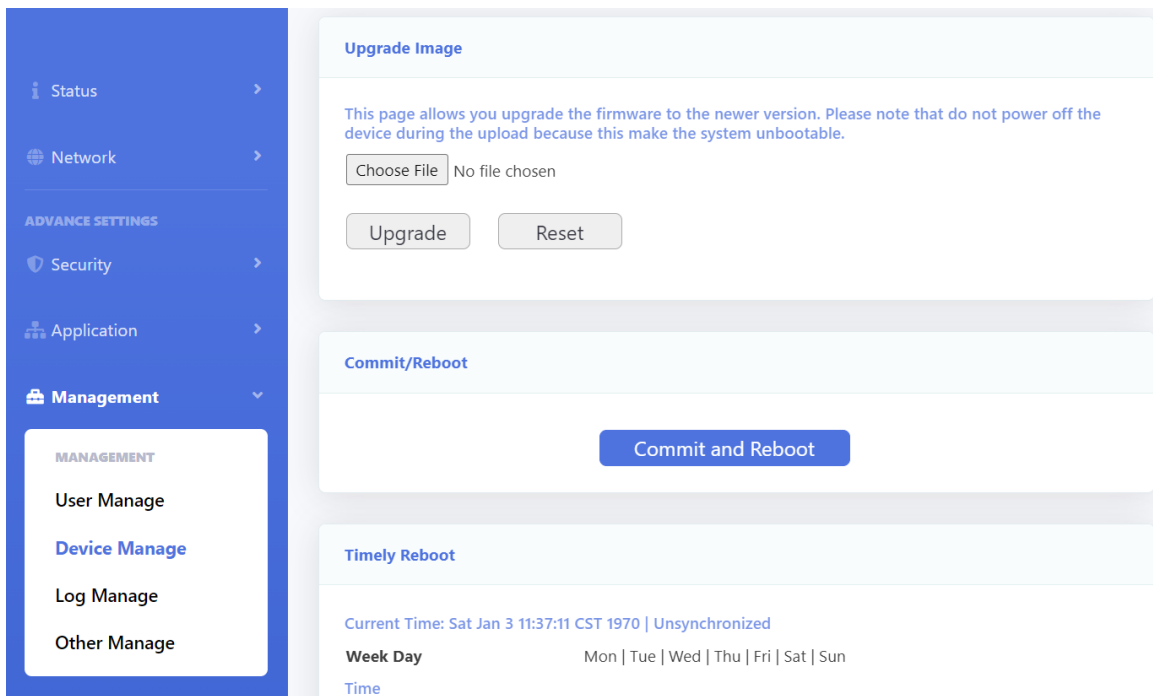


Figure 3-6-2: Device Manage

3.6.2.1 Upgrade Image

This page allows you to upgrade the device. You can select the upgrade firmware and click "Upgrade" to upgrade device. Please keep the power on, otherwise this device will be damaged. It will reboot automatically when finish upgrade.

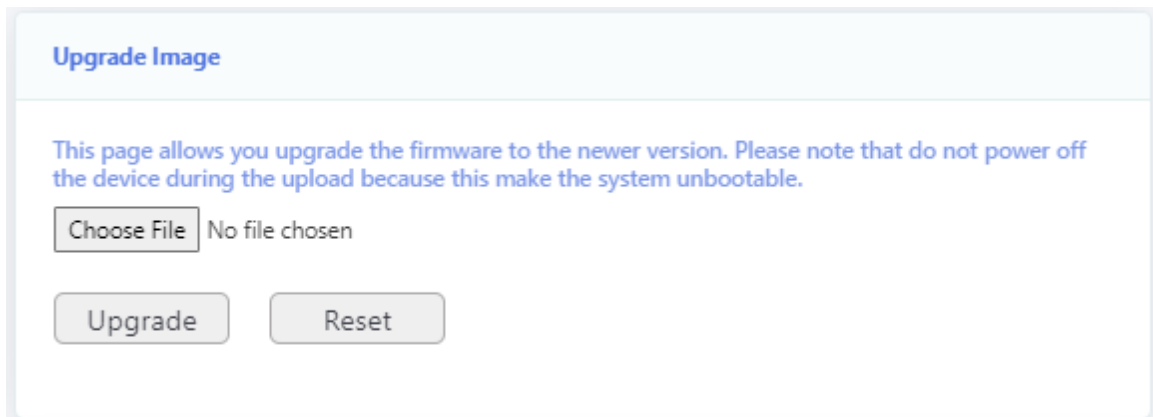


Figure 3-6-3: Device upgrade

3.6.2.2 Commit/Reboot

This page allows you to reboot the device. The process of reboot will take several minutes.

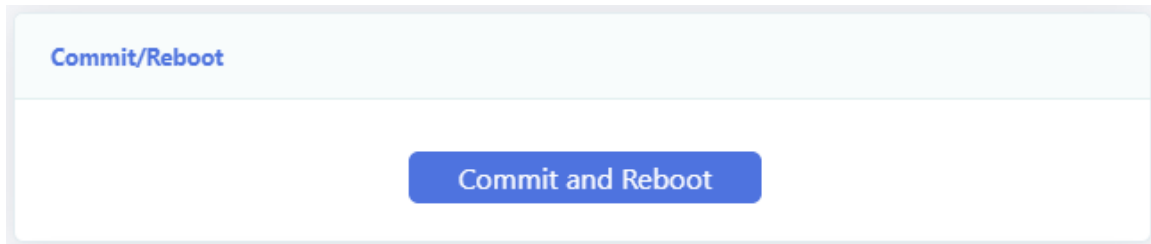


Figure 3-6-4: Device reboot

3.6.2.3 Timely Reboot

This page is used to configure timely reboot. The device will reboot at the set time, but the function will take effect only after the synchronization time.

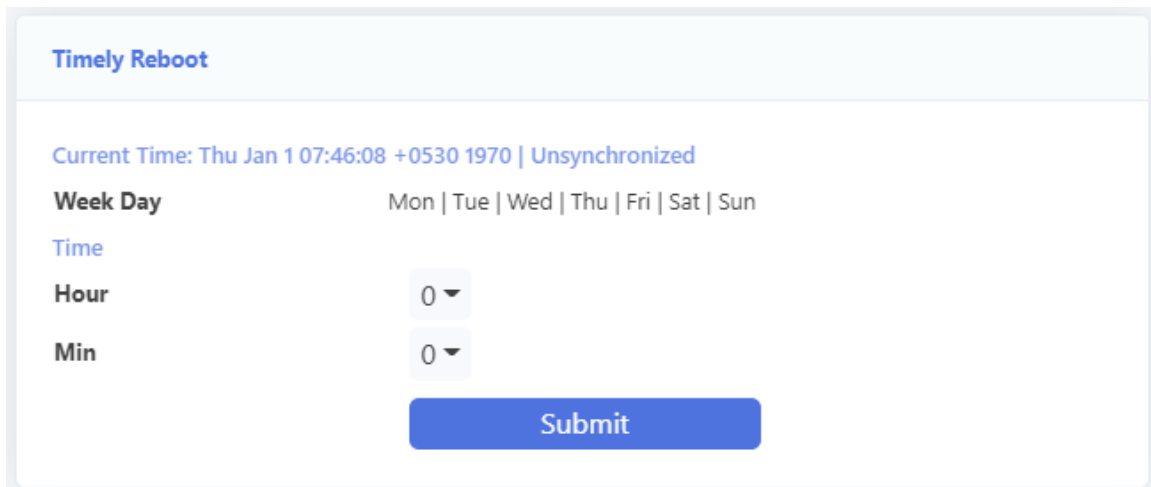


Figure 3-6-4: Timely reboot

3.6.2.4 Load Default

This page allows you to restore the device to default settings. You can click "Restore Default" or "Restore factory configuration" button to restore settings of the device. "Restore Default" button restore the LAN parameter, "Restore Factory configuration" button restore all the ONU configurations. After restored, it will restart automatically.

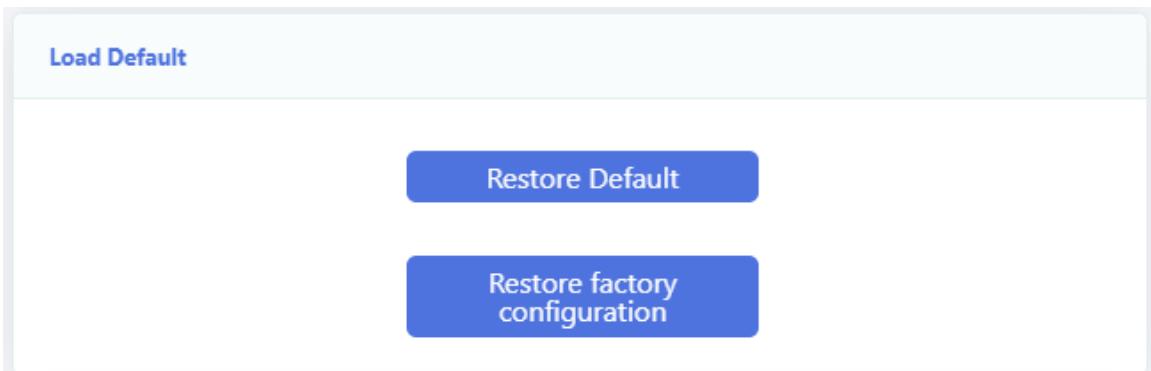


Figure 3-6-6: Load default

3.6.2.5 Current Configuration Management

This page allows you to backup the configurations of ONU. "Download" button can download the current configuration file to your PC. "Cancel self custom default" button can remove your previous default configuration which uploaded before.

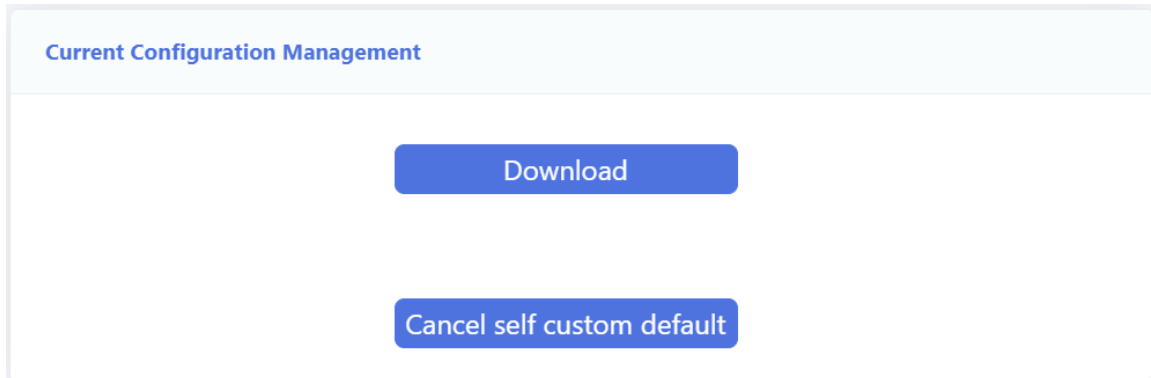


Figure 3-6-7: Download configuration Management

3.6.2.6 Upload Configuration Management

This page allows you to restore the configurations of ONU. "Upload" button can upload the configuration file to device. "Upload As Default" button can upload your configuration file as default configuration.

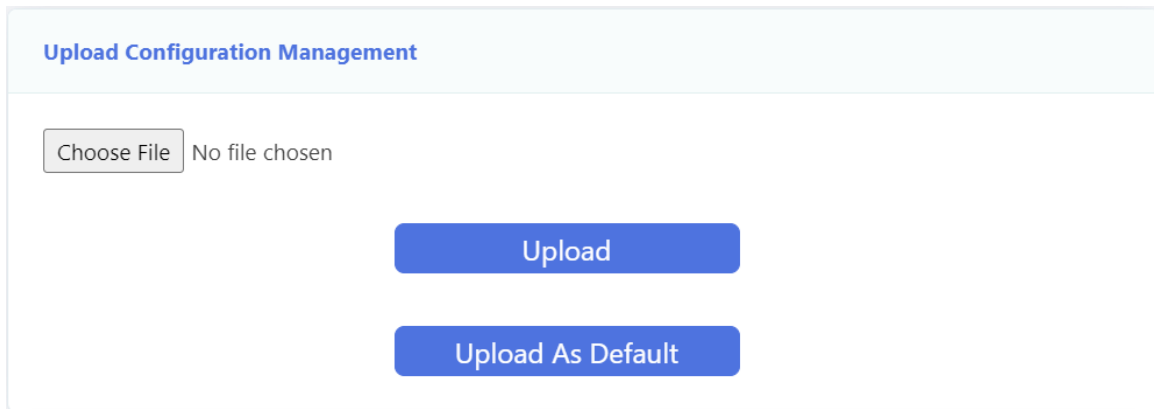


Figure 3-6-8: Upload configuration Management

3.6.2.7 Upload when End Maintain

This page allows you to upload new data to TR069 server, when the device is connected to the TR069 server and click "End Maintain" button.

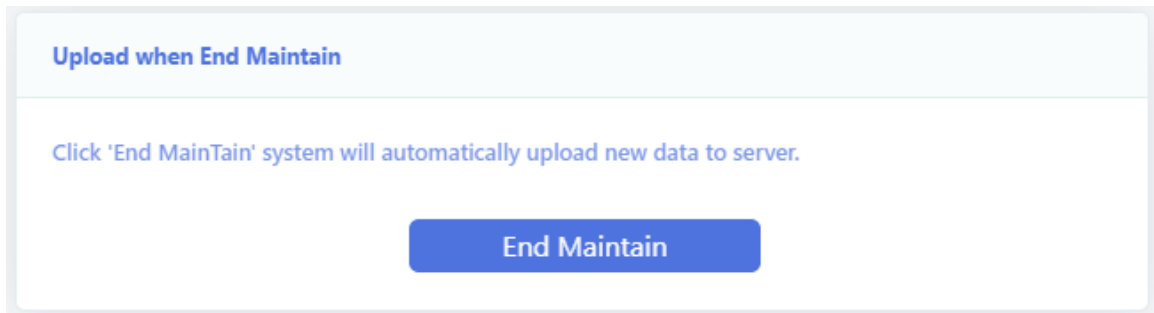


Figure 3-6-9: Upload when End Maintain

3.6.3 Log Manage

This page allows you to make some settings on the system log including record, view, download logs

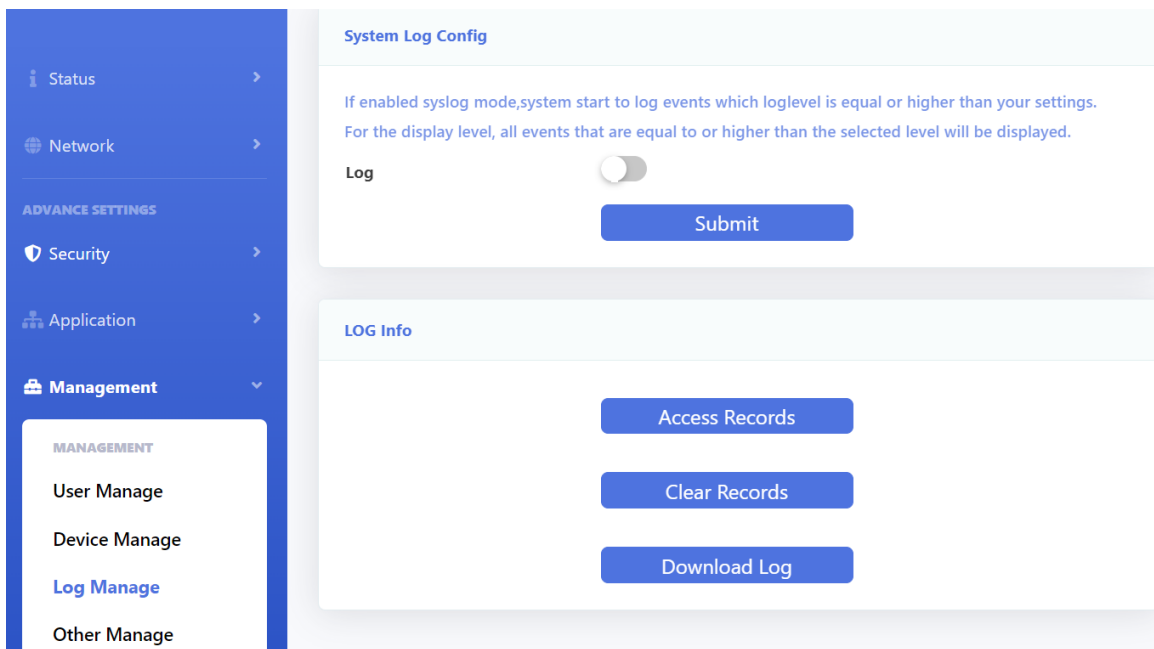


Figure 3-6-10: Log Manage

3.6.3.1 System Log

This page allows you to set up log level and display level, and log server as well.

System Log Config

If enabled syslog mode, system start to log events which loglevel is equal or higher than your settings.
For the display level, all events that are equal to or higher than the selected level will be displayed.

Log

Log Level Emergency ▾

Display Level Emergency ▾

Storage Mode none ▾

[Submit](#)

Figure 3-6-11: Log settings

Parameters	Illustration
Log Level	Log record level, include Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debugging.
Display Level	Log display level, include Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debugging.
Storage Mode	Can select to store the log in local or remote server.

3.6.3.2 LOG Info

This page allows you to view and clear the log information.

LOG Info

[Access Records](#)

[Clear Records](#)

[Download Log](#)

Figure 3-6-12: Log Info

3.6.4 Other Manage

This page allows you to configure the ONU's Type to HGU or SFU. In SFU mode, you should configure LAN VLAN through OLT, no need to set WAN or other configuration on the web page.

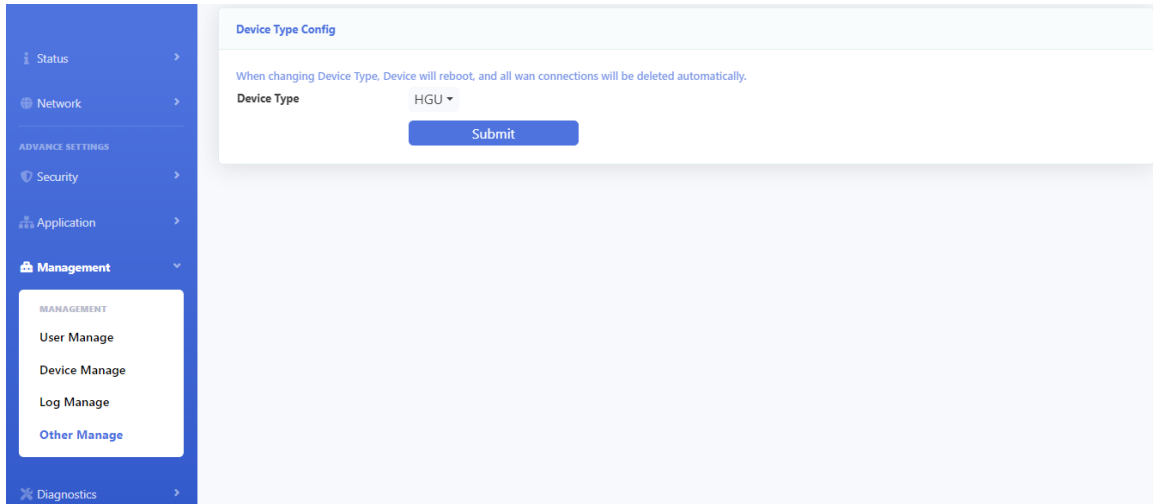


Figure 3-6-13: Device Type Config

3.7 Diagnostics

3.7.1 Network diagnostics

3.7.1.1 Network diagnostics

This page is used for ping test and traceroute test. You can diagnose connection status between ONU and other devices. Please note that when the traceroute is running, do not perform the traceroute test again.

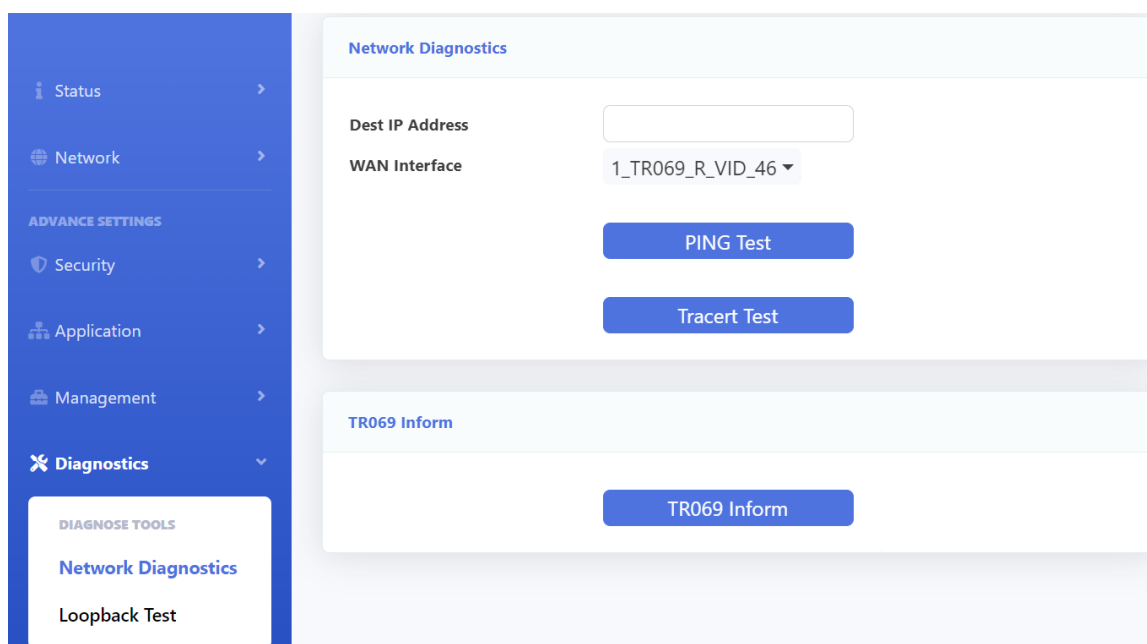


Figure 3-7-1: Network diagnostics

Parameters	Illustration
Dest IP Address	Input the destination IP you want to ping or tracert.
WAN Interface	Select the interface that needs to diagnose.

3.7.1.2 TR069 Inform

This page is used to manual send TR069 inform to ACS.

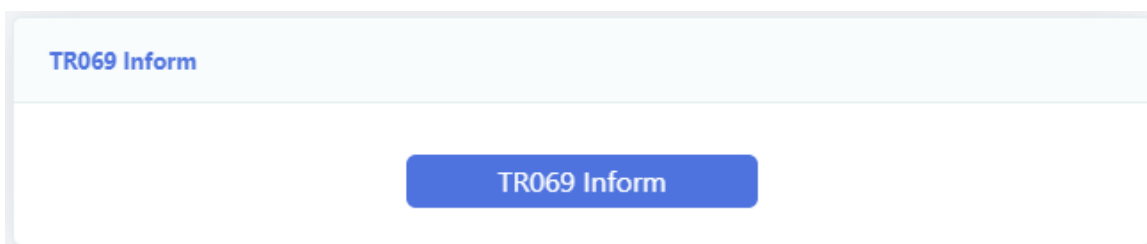


Figure :3-7-2 TR069 Inform

3.7.2 Loopback Test

3.7.2.1 Loopback Test

This page is used to configure loopback detect function. By default, loop detection is turned on.

Loopback Test

Enable Loopback Detection

Detection Frame Interval

Recover Frame Interval

EtherType

VLAN ID

Submit

Port Loopback Detect State

Port	Status
LAN1	No Loopback
LAN2	No Loopback
LAN3	No Loopback
LAN4	No Loopback
LAN5	No Loopback

Figure 3-7-3: Loopback detect settings

3.7.2.2 Port Loopback Detect State

This page is used to show the loop status of each port.

Port Loopback Detect State

Port	Status
LAN1	No Loopback
LAN2	No Loopback
LAN3	No Loopback
LAN4	No Loopback
LAN5	No Loopback

Figure 3-7-4: Loopback state

Chapter 4 Examples

4.1 Internet service

There are two configuration methods for Internet service. One works on bridge mode and another works on route mode.

4.1.1 Requirement

- 1) ONU works on bridge mode, service VLAN is 9. User surf the Internet via LAN port 1.
- 2) ONU works on route mode, service VLAN is 10. ONU gets IP address via DHCP.

4.1.2 Steps

Before configuring, make sure ONU has registered and been authorized successfully. Connect PC to one LAN port of ONU directly with twisted cable.

4.1.2.1 Bridge mode for Internet service

- 1) Add a WAN connection

Choose “Network > WAN > WAN Config” in navigation menu. Add a bridge mode WAN connection as the following parameters.

- ✧ Mode is bridge.
- ✧ Enable VLAN and VLAN ID is 9.
- ✧ Service mode is OTHER.
- ✧ Bind port 1.
- ✧ Other parameters keep default.

The screenshot shows the 'WAN Config' page with the following settings:

- Connectin Name:** Add New Wan
- Mode:** Bridge
- IP Version:** IPv4
- Enabled Vlan:**
- Vlan ID:** 9
- 802.1p:** NONE
- MTU:** 1500
- ServiceMode:** Other
- Disable LAN DHCP:**

Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
LAN_5	

Submit

Figure 4-1-1: Add a bridge WAN connection

2) Surf the Internet

Connect PC to LAN 1 port. After get IP address from DHCP server in the network, the PC can surf the Internet.

4.1.2.2 Route mode for Internet service

1) Add a WAN connection

Choose “Network > WAN > WAN Config” in navigation menu. Add a route mode WAN connection as the following parameters.

- ✧ Protocol mode is IPv4.
- ✧ Choose DHCP.
- ✧ NAT function is checked.
- ✧ Enable VLAN and VLAN ID is 10.
- ✧ Service mode is INTERNET.
- ✧ Bind port 1.
- ✧ Other parameters keep default.

The screenshot shows the 'WAN Config' interface with the following settings:

- Connectin Name:** Add New Wan
- Mode:** Route
- IP Version:** IPv4
- Connection Mode:** DHCP (selected), Static, PPPoE
- Enabled NAT:**
- Enabled Vlan:**
- Vlan ID:** 10
- 802.1p:** NONE
- MTU:** 1500
- Request DNS:**
- ServiceMode:** INTERNET
- Disable LAN DHCP:**

Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
LAN_5	

Submit

Figure 4-1-2: Add a route WAN connection

2) Surf the Internet

Connect PC to LAN port 1. The PC gets IP address from ONU and ONU gets IP address from DHCP server in the network, and then you can surf the Internet.

4.2 IPTV service

There are two methods for IPTV service, IGMP snooping and IGMP proxy. You must enable IGMP proxy when ONU works on route mode.

4.2.1 Requirement

- 1) ONU works on bridge mode for IPTV service, VLAN is 20.
- 2) ONU works on route mode for IPTV service, VLAN is 30.

4.2.2 Steps

Before configuring, make sure ONU has registered and been authorized successfully.

Connect PC to one LAN port of ONU directly with twisted cable.

4.2.2.1 Bridge mode for IGMP

1) Add a WAN connection

Choose “Network > WAN > WAN Config” in navigation menu. Add a bridge mode WAN connection as the following parameters.

- ✧ Protocol mode is IPv4.
- ✧ Enable VLAN and VLAN ID is 20.
- ✧ Service mode is OTHER.
- ✧ Bind port 2.
- ✧ Other parameters keep default.

The screenshot shows the 'WAN Config' interface with the following settings:

- Connectin Name:** Add New Wan
- Mode:** Bridge
- IP Version:** IPv4
- Enabled Vlan:**
- Vlan ID:** 20
- 802.1p:** NONE
- MTU:** 1500
- ServiceMode:** Other
- Disable LAN DHCP:**
- Bind Port :**
 - LAN_1
 - LAN_3
 - LAN_5
 - LAN_2
 - LAN_4

A blue 'Submit' button is located at the bottom of the form.

Figure 4-2-1: Add a bridge WAN connection

2) Enable IGMP snooping

Choose “Application > Multicast Setting > IGMP Snooping Configuration” in navigation menu. Check down IGMP snooping. IGMP snooping is checked by default. It will not be mentioned in the rear examples.

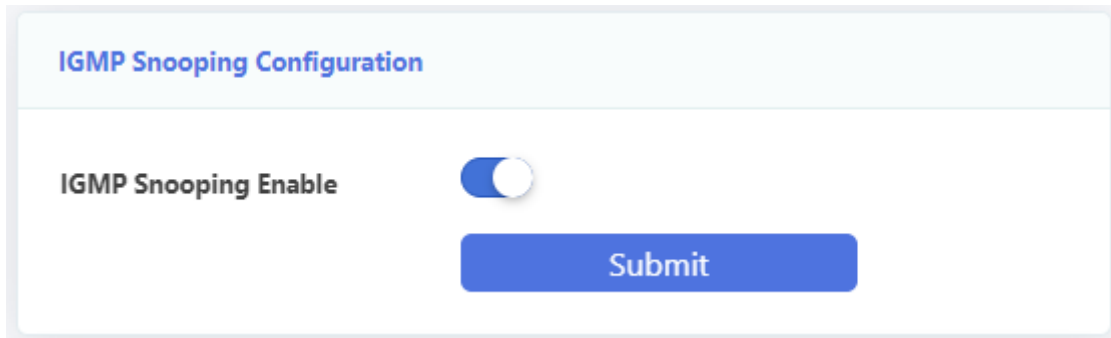


Figure 4-2-2: Enable IGMP snooping

3) Add multicast snooping VLAN

Choose “Application > Multicast Setting > IPTV” in navigation menu. Click on choose the relevant WAN connection and add multicast VLAN, the result is as shown in the figure.

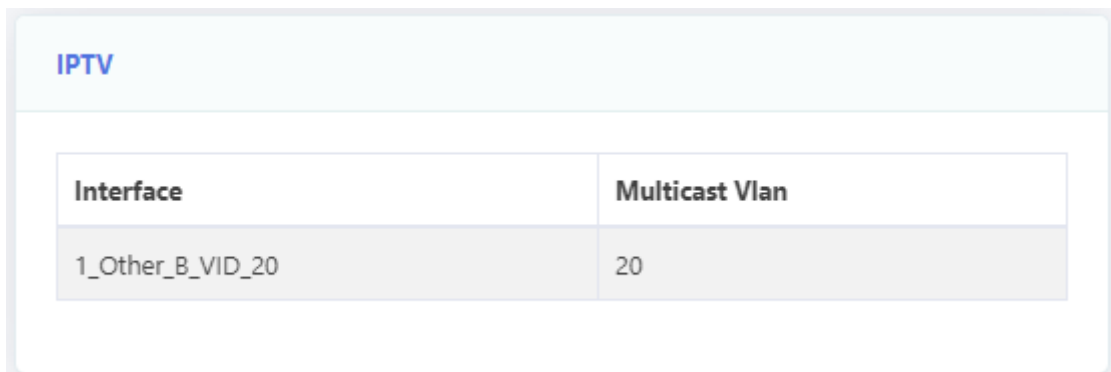


Figure 4-2-3: Add multicast Snooping VLAN

4) Join multicast group

User sends an IGMP report message through LAN port 2. Report message doesn't take any VLAN tag.

4.2.2.2 Route mode for IGMP

1) Add a WAN connection

Choose “Network > WAN > WAN Config” in navigation menu. Add a route mode WAN connection as the following parameters.

- ✧ Mode is Route.
- ✧ Protocol mode is IPv4.
- ✧ Choose DHCP. (Provided by ISP)
- ✧ NAT function is checked.
- ✧ Enable VLAN and VLAN ID is 30.
- ✧ Service mode is INTERNET.
- ✧ Bind port 2.

✧ Other parameters keep default.

The screenshot shows the 'WAN Config' interface with the following settings:

- Connectin Name:** Add New Wan
- Mode:** Route
- IP Version:** IPv4
- Connection Mode:** DHCP (selected), Static, PPPoE
- Enabled NAT:**
- Enabled Vlan:**
- Vlan ID:** 30
- 802.1p:** NONE
- MTU:** 1500
- Request DNS:**
- ServiceMode:** INTERNET
- Disable LAN DHCP:**

Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
LAN_5	

Submit

Figure 4-2-4: Add a route WAN connection

2) Enable IGMP proxy

Choose “Application > Multicast Setting > IGMP Proxy” in navigation menu. Enable IGMP proxy and choose the relevant WAN connection.

The screenshot shows the 'IGMP Proxy' configuration interface with the following settings:

- IGMP Proxy Enable:**
- Interface:** 1_INTERNET_R_VID_30

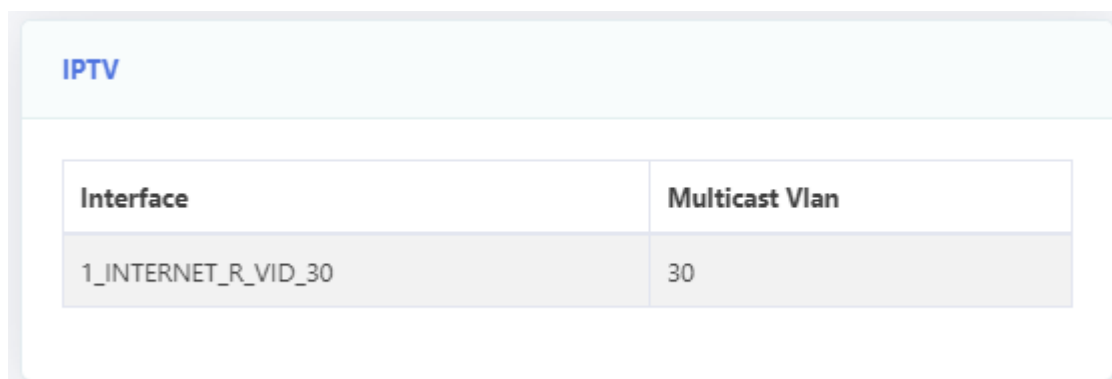
Submit

Figure 4-2-5: Enable IGMP proxy

3) Add multicast proxy VLAN

Choose “Application > Multicast Setting > IPTV” in navigation menu. Click on

choose the relevant WAN connection and add multicast VLAN, the result is as shown in the figure.



Interface	Multicast Vlan
1_INTERNET_R_VID_30	30

Figure 4-2-6: Add multicast proxy VLAN

4) Join multicast group

User sends an IGMP report message through LAN port 2 after got an IP address from ONU.

4.3 Internet and IPTV service mixed

This example introduces how to achieve Internet service and IPTV service at the same time.

4.3.1 Requirement

1) ONU uses route mode for Internet service and bridge mode for IPTV service.

LAN 1 is used for Internet service, VLAN is 10; LAN 2 is used for IPTV service, VLAN is 20.

2) ONU uses route mode for Internet service and IPTV service.

LAN 1 is used for Internet service, VLAN is 11; LAN 2 is used for IPTV service, VLAN is 11.

4.3.2 Steps

Before configuring, make sure ONU has registered and been authorized successfully. Connect PC to one LAN port of ONU directly with twisted cable.

4.3.2.1 Route and bridge mode for mixed service

1) Add WAN connections

Choose “Network > WAN > WAN Config” in navigation menu. Add a route mode WAN connection as the following parameters.

- ✧ Protocol mode is IPv4.

- ✧ Choose DHCP. (Provided by ISP)
- ✧ Enable VLAN and VLAN ID is 10.
- ✧ Service mode is INTERNET.
- ✧ Bind port 1.
- ✧ Other parameters keep default.

WAN Config

Connectin Name: Add New Wan ▾

Mode: Route ▾

IP Version: IPv4 ▾

Connection Mode: **DHCP** Static PPPoE

Enabled NAT:

Enabled Vlan:

Vlan ID:

802.1p: NONE ▾

MTU:

Request DNS:

ServiceMode: INTERNET ▾

Disable LAN DHCP:

Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
LAN_5	

Figure 4-3-1: Add a route mode WAN

Add a bridge mode WAN connection, enable VLAN and VLAN ID is 20, service mode is OTHER and bind port 2.

The screenshot shows the WAN Config page with the following settings:

- Connectin Name: Add New Wan
- Mode: Bridge
- IP Version: IPv4
- Enabled Vlan:
- Vlan ID: 20
- 802.1p: NONE
- MTU: 1500
- ServiceMode: Other
- Disable LAN DHCP:

Under Bind Port, LAN_1 and LAN_2 are selected. LAN_3 and LAN_4 are also visible. A Submit button is at the bottom.

Figure 4-3-2: Add a bridge mode WAN

2) Add IGMP snooping VLAN

Choose “Application > Multicast Setting > IPTV ” in navigation menu. Click the relevant WAN connection and add multicast VLAN.

The screenshot shows the IPTV configuration page with a table of Multicast VLANs:

Interface	Multicast Vlan
1_INTERNET_R_VID_10	
2_Other_B_VID_20	20

Figure 4-3-3: Add multicast VLAN

3) Surf the Internet

Connect PC to LAN port 1. The PC gets an IP address from ONU and ONU gets an IP address from DHCP server in the network, and then you can surf the Internet.

4) Watch IPTV

Connect STB to LAN port 2. After STB gets an IP address from ISP via DHCP, you can

watch IPTV.

4.3.2.2 Route mode for mixed service

1) Add WAN connection

Choose “Network > WAN > WAN Config” in navigation menu. Add a route mode WAN connection as the following parameters.

- ✧ Protocol mode is IPv4.
- ✧ Choose DHCP. (Provided by ISP).
- ✧ Enable VLAN and VLAN ID is 11.
- ✧ Service mode is INTERNET.
- ✧ Bind port 1 and port 2 .
- ✧ Other parameters keep default.

The screenshot displays the 'WAN Config' interface with the following settings:

- Connectin Name:** Add New Wan
- Mode:** Route
- IP Version:** IPv4
- Connection Mode:** DHCP (selected), Static, PPPoE
- Enabled NAT:**
- Enabled Vlan:**
- Vlan ID:** 11
- 802.1p:** NONE
- MTU:** 1500
- Request DNS:**
- ServiceMode:** INTERNET
- Disable LAN DHCP:**
- Bind Port :** LAN_1, LAN_2, LAN_3, LAN_4, LAN_5

A blue 'Submit' button is located at the bottom of the configuration panel.

Figure 4-3-4: Add a route mode WAN connection

2) Enable IGMP proxy

Choose “Application > Multicast > IGMP Proxy” in navigation menu. Enable IGMP proxy and choose the relevant WAN connection .

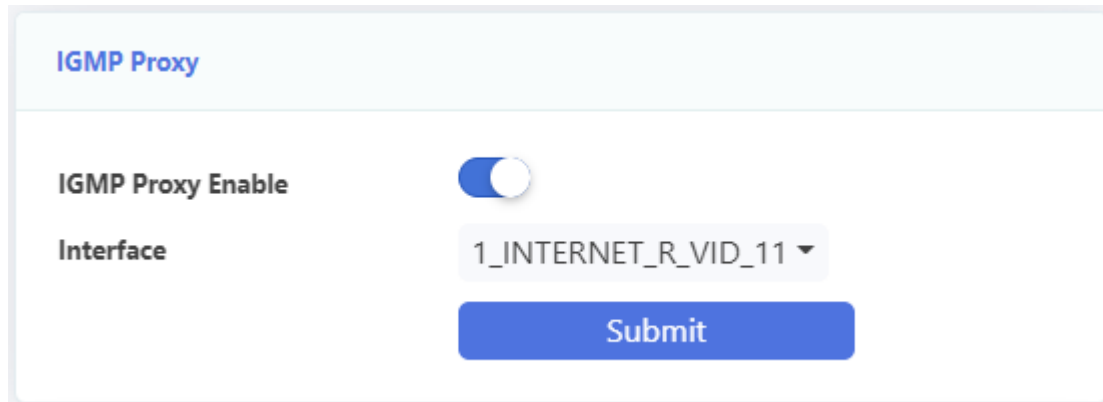


Figure 4-3-5: Enable IGMP proxy

3) Add Multicast VLAN

Choose “Application > Multicast Setting > IPTV ” in navigation menu. Click the relevant WAN connection and add multicast VLAN.



Interface	Multicast Vlan
1_INTERNET_R_VID_11	11

Figure 4-3-6:Add multicast VLAN.

4) Surf the Internet

Connect PC to LAN port 1. The PC gets an IP address from ONU and ONU gets an IP address from DHCP server in the network, and then you can surf the Internet.

5) Watch IPTV

Connect STB to LAN port 2. After STB gets an IP address from ISP via DHCP, you can watch IPTV.

4.4 Update image

You can update software image on webpage.

Choose “Management > Device Manage > Update Image” in navigation menu. Select the software image file with .tar as suffix, click “Upgrade” button. ONU will restart automatically after updated. The whole process needs about 2 minutes.

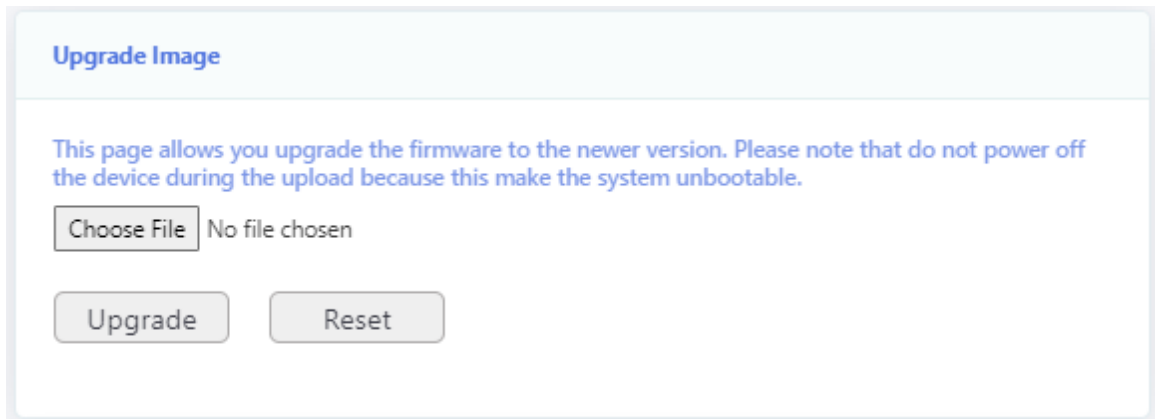


Figure 4-4-1: Update software

Chapter 5 FAQ

1. **Q:** All indicators are not lit?

A: (1) The indicator LED hasn't come up yet, you need to wait about two minutes.

(2) Power is off or power adapter is bad.

2. **Q:** Why PON/LOS indicator flashing red?

A: (1) There is no optical signal. Maybe the fiber is broken down or connection loosened.

(2) Optical power is too low.

(3) The fiber is dusty.

3. **Q:** LAN indicators are not lit?

A: (1) Indicator LED switch is turned off.

(2) The cable breaks down or connection loosened.

(3) The cable type incorrect or too long.

4. **Q:** PC can't visit web UI?

A: (1) PC and ONU are not in the same network fragment. By default, LAN IP is 192.168.1.1/24.

(2) The cable breaks down.

(3) IP conflict or have loopback.

5. **Q:** User can't surf the Internet normally.

A: (1) PC has set a wrong IP and gateway or network is bad.

(2) There is loopback or attack in network.

(3) Route mode WAN connection doesn't get an IP or DNS is disabled.

6. **Q:** ONU stops to work after working for some time.

A: (1) Power supply is not working properly.

(2) The device overheats.