AirLive

ONU-10XG(S)-AX304P-2.5G

USER MANUAL

Contents

Chapter 1 Product Introduction

1.1 Product Description

The 10G PON ONU-10XG(S)-AX304P-2.5G developed by AirLive comes in two models a XG-PON and XGS-PON, providing multiple rate Ethernet ports of 2.5GE/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.

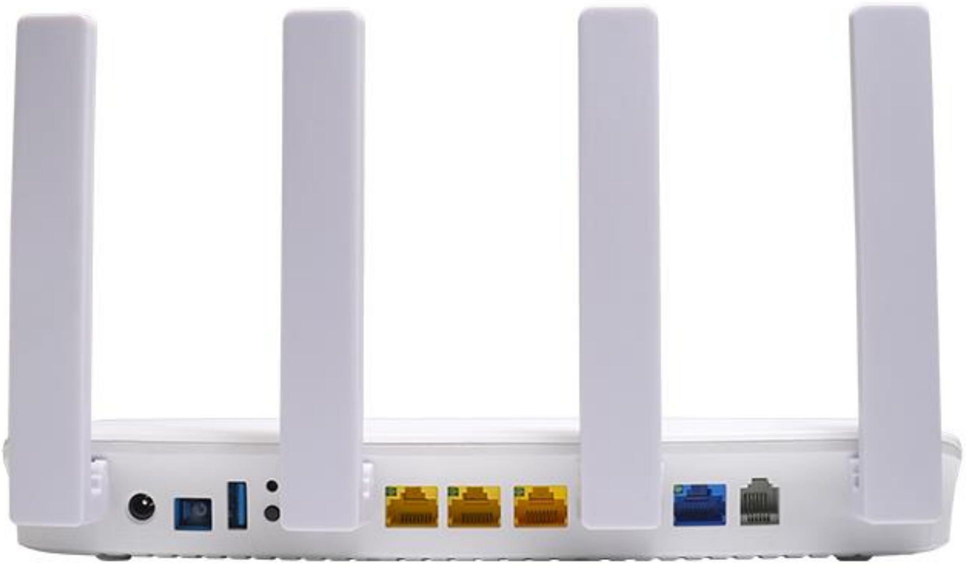


Figure 1-1-1: ONU-10XG(S)-AX304P-2.5G

There are two specifications available for this ONU, XG or XGS-PON.

Product	Specification
XG/XGS-PON ONU	2.5GE+3GE+1POTS+1USB3.0+WiFi 6 XG-PON ONU
	2.5GE+3GE+1POTS+1USB3.0+WiFi 6 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 PON port: Class B+ TX optical power: 6dBm(XGS-PON), 5dBm(XG-PON), RX sensitivity: -28dBm, Overload optical power: -7dBm Transmission distance: 20km
Wavelength	XG(S)-PON:DS 1577nm/US 1270nm
Optical interface	SC single mode, SC/UPC connector
Interface	1*2.5GE, Auto-negotiation,RJ45 ports 3*GE, Auto-negotiation,RJ45 ports 1*POTS, RJ11 Connector 1*USB3.0
Wireless	Compliant with IEEE802.11b/g/n/ac/ax,speed up to 3 Gbps, 4T4R(four external antennas).
LED	PON/LOS, WAN, WiFi, USB,PHONE
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, 2A
Power consumption	24W
Dimension	244mm*131mm*36mm (L*W*H)
Net weight	0.425Kg

1.4 Application chart

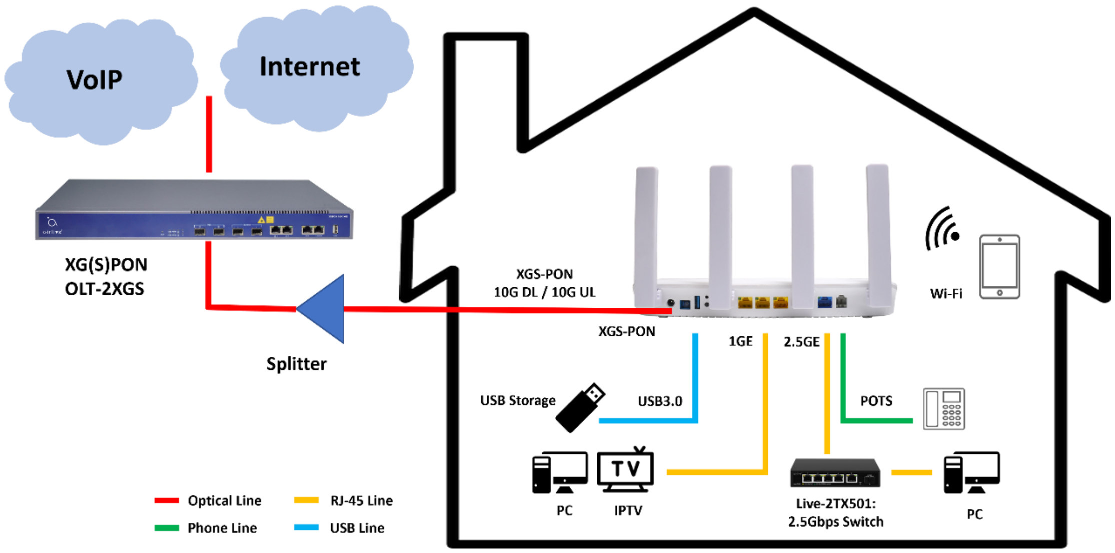


Figure 1-4-1: Application chart, when using XG-Pon it will be 10G DL/2.5GUL

1.5 Panel description

Interface panel

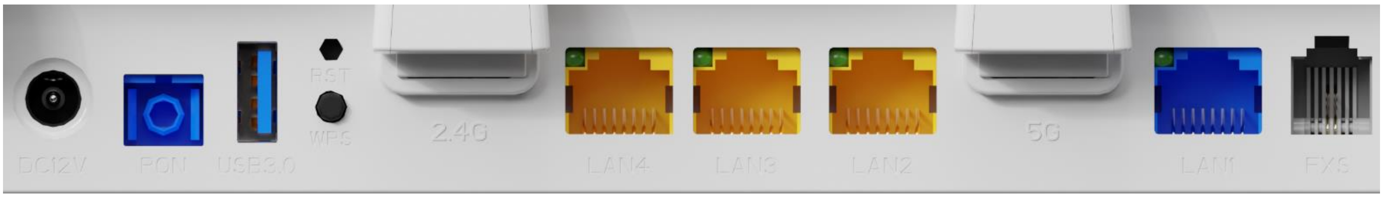


Figure 1-5-1: Interface panel

Name	Function
DC 12V	Connect with power adapter. DC 12V, 2A.
PON	Connect to OLT by SC type fiber connector, single mode optical fiber cable.
USB 3.0	External USB port, connect to USB storage device.
WPS	Press WPS button for 1 ~ 4 seconds, starts to pair 2.4G; Press WPS button for 4 ~ 7 seconds, starts to pair 5G.

RST	Press RST 6 seconds for reboot, greater than 6 seconds for restoring user default configuration, greater than 12 seconds for restoring factory configuration as default.
LAN1-4	The blue LAN1 is a 2.5GE port and the yellow LAN2-4 are 1GE ports. Connect PC or other devices to GE port by Cat5 cable, RJ-45 connector and connect to 2.5GE port by Cat5e/Cat6/Cat7 cable, RJ-45 connector.
FXS	Connect to the telephone with FXS port by telephone wire.

Indication Panel

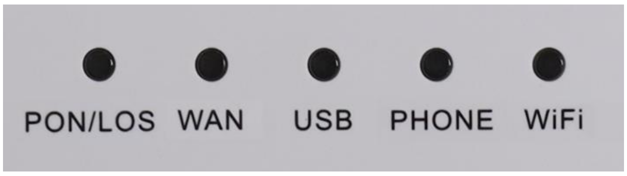


Figure 1-5-2: Indication panel

Name	Status	Function
PON/LOS	OFF	Device not started/Received incorrect optical power
	Green always on	Device has been registered to OLT.
	Flash green	Device registering.
	Flash red	Received optical power is lower or stronger than the sensitivity of the optical receiver.
	Red always on	Device starting up
WAN	On	WAN connection is up.
	Off	WAN connection is down.
	Blink	Data passing WAN connection.

PHONE	OFF	Device is power off or not registered to the soft-switch.
	ON	Device has registered to the soft-switch.
	Flash	The port is working.
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.
WiFi	OFF	Device is power off or WiFi is turned off.
	ON	WiFi is turned on.
	Flash	WiFi is turned on and 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. If something is wrong after shipping, please contact carrier; other damage or lack of some parts, please contact with your 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 powered ON, the indicators should light up as for normal operation. Check whether the PON interface status LED (PON/LOS) is continuously on green. 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/CAT5e/CAT6/CAT7 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 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”.

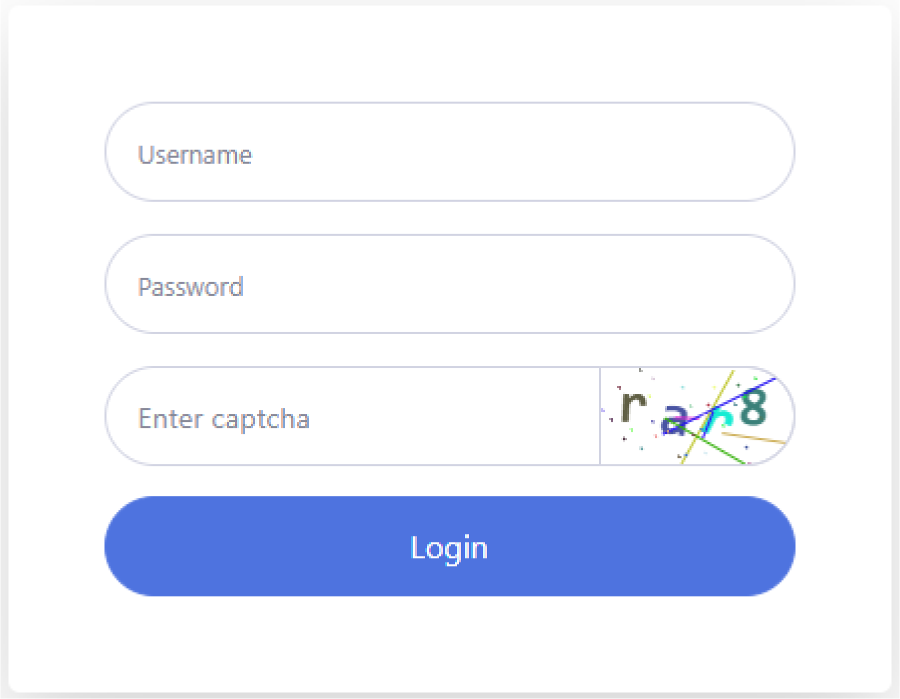


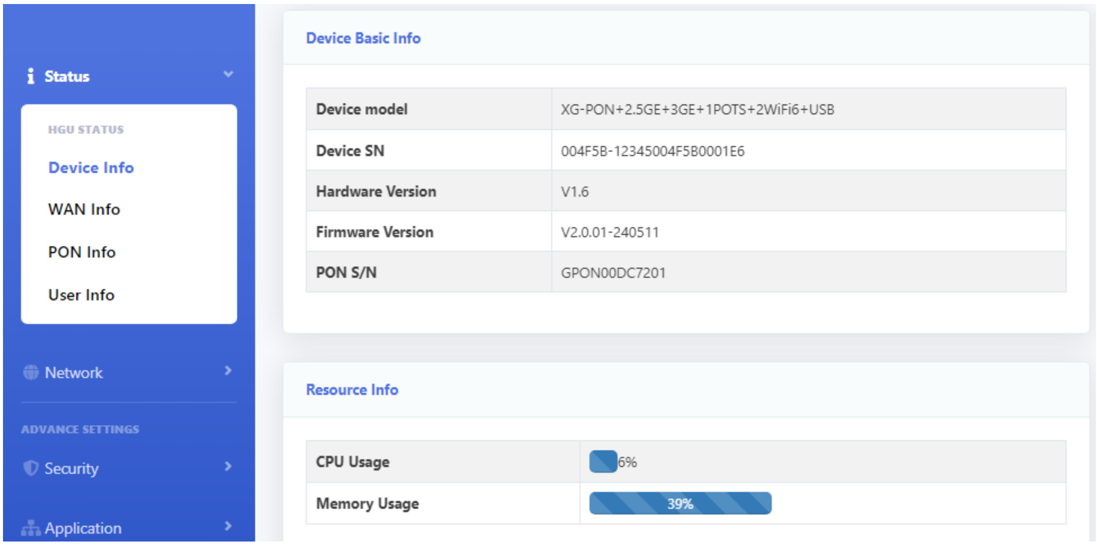
Figure 3-1-1: Login

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.



Device Basic Info

Device model	XG-PON+2.5GE+3GE+1POTS+2WiFi6+USB
Device SN	004F5B-12345004F5B0001E6
Hardware Version	V1.6
Firmware Version	V2.0.01-240511
PON S/N	GPON00DC7201

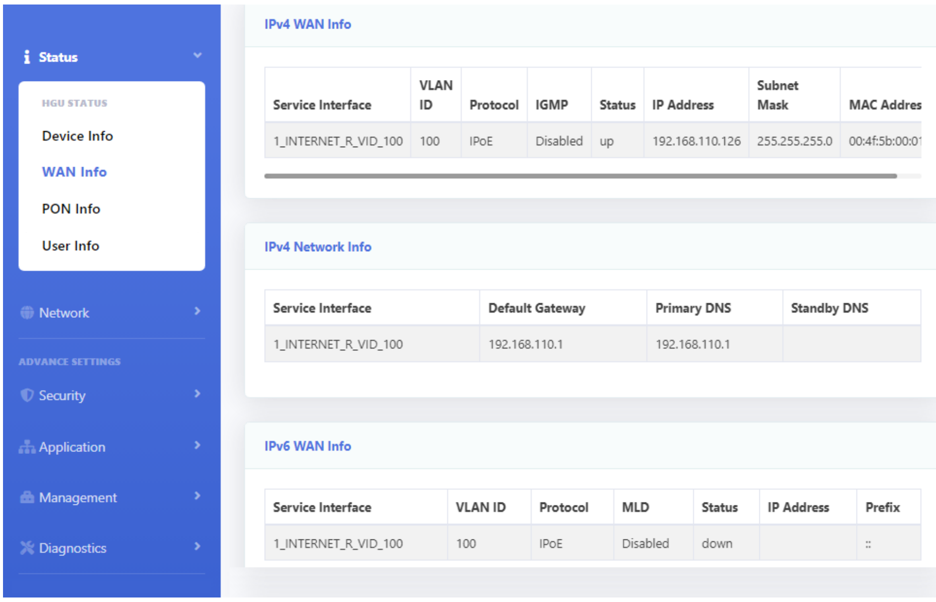
Resource Info

CPU Usage	6%
Memory Usage	39%

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.



IPv4 WAN Info

Service Interface	VLAN ID	Protocol	IGMP	Status	IP Address	Subnet Mask	MAC Addres
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	

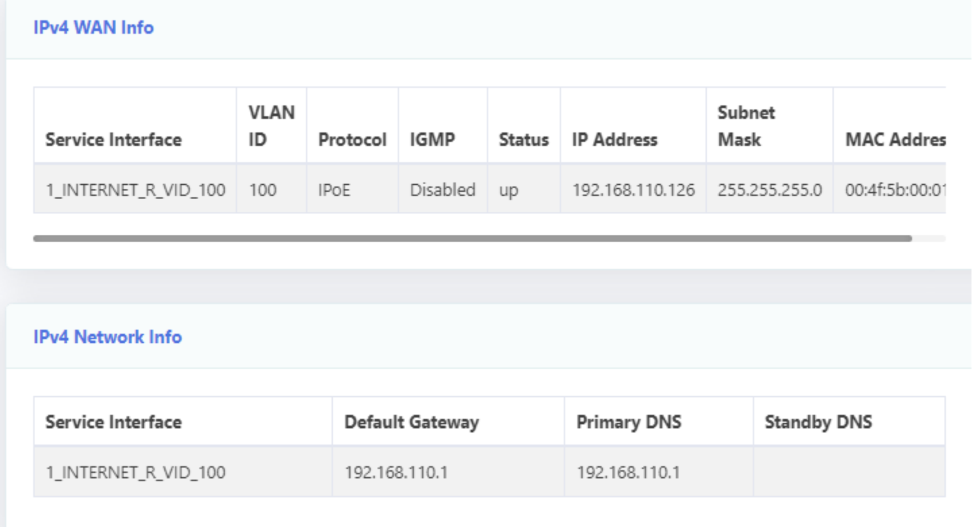
IPv6 WAN Info

Service Interface	VLAN ID	Protocol	MLD	Status	IP Address	Prefix
1_INTERNET_R_VID_100	100	IPoE	Disabled	down		::

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 Addres
1_INTERNET_R_VID_100	100	IPoE	Disabled	up	192.168.110.126	255.255.255.0	00:4f:5b:00:0

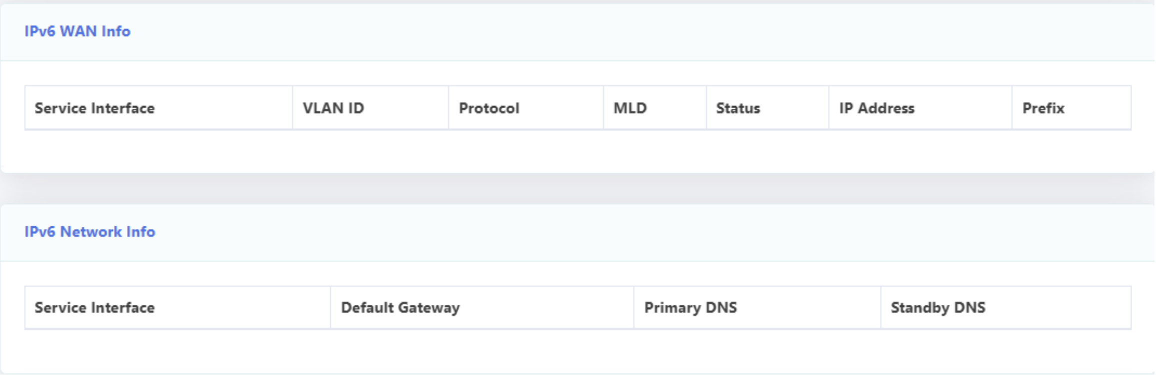
IPv4 Network Info

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

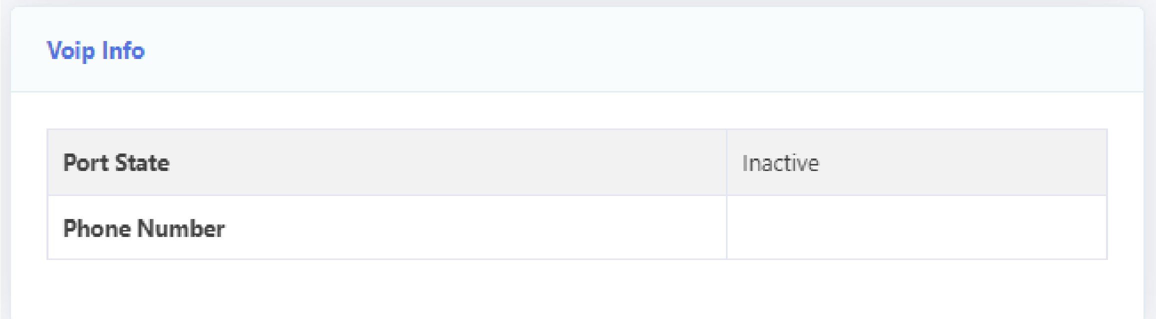
IPv6 Network Info

Service Interface	Default Gateway	Primary DNS	Standby DNS

Figure 3-2-4: IPv6 WAN Information

3.2.2.3 VoIP Information

This page shows VoIP information which includes registration status and phone number.



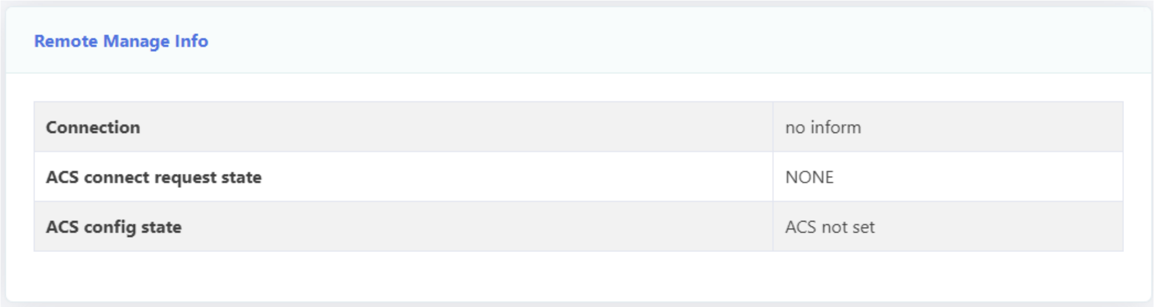
Voip Info

Port State	Inactive
Phone Number	

Figure 3-2-5: VoIP Info

3.2.2.4 TR069 Status

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



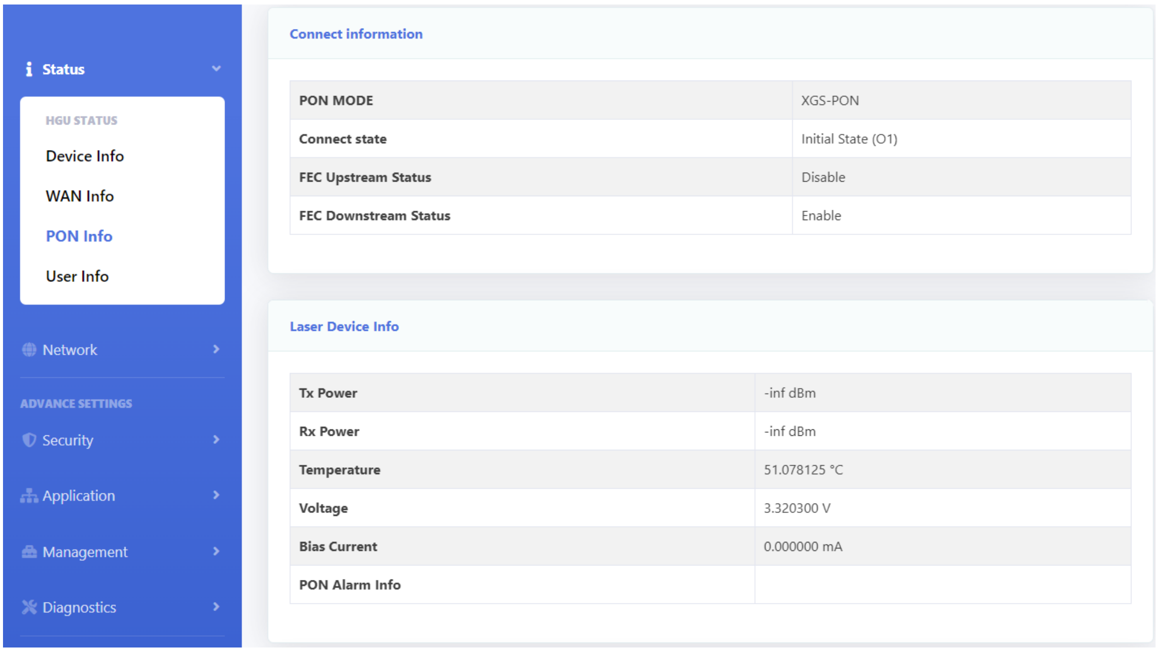
Remote Manage Info

Connection	no inform
ACS connect request state	NONE
ACS config state	ACS not set

Figure 3-2-6: 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.



Connect information

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

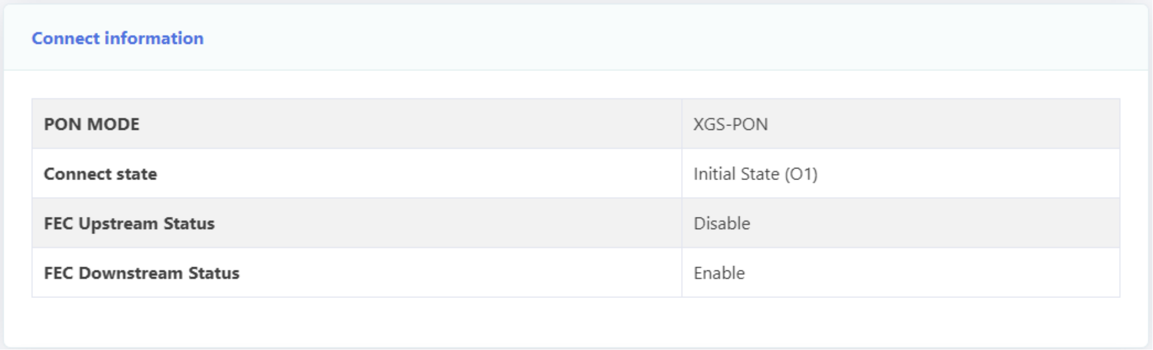
Laser Device Info

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 3-2-7: PON Info

3.2.3.1 Connect information

This page shows the PON connection information and FEC information.



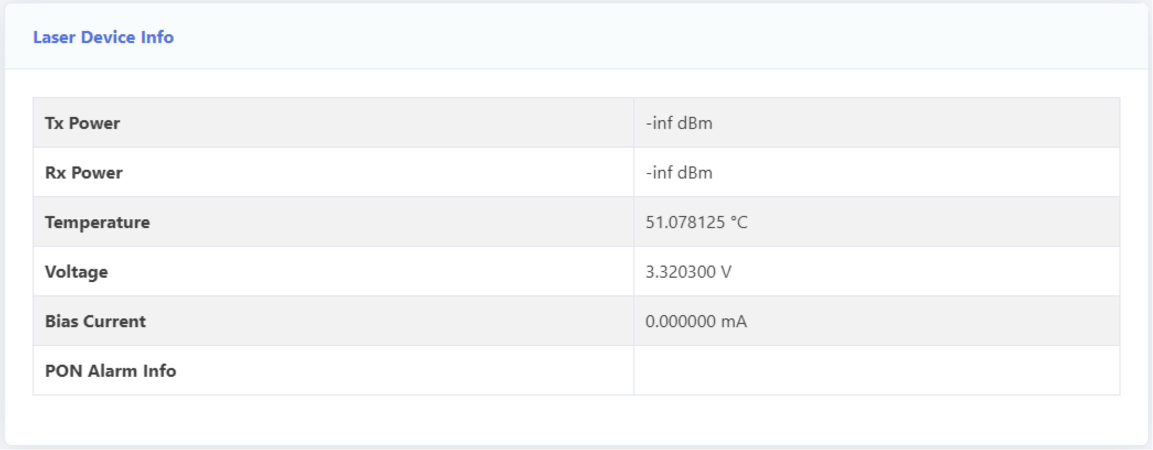
Connect information

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

Figure 3-2-8: Connection Info

3.2.3.2 Laser Device Info

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



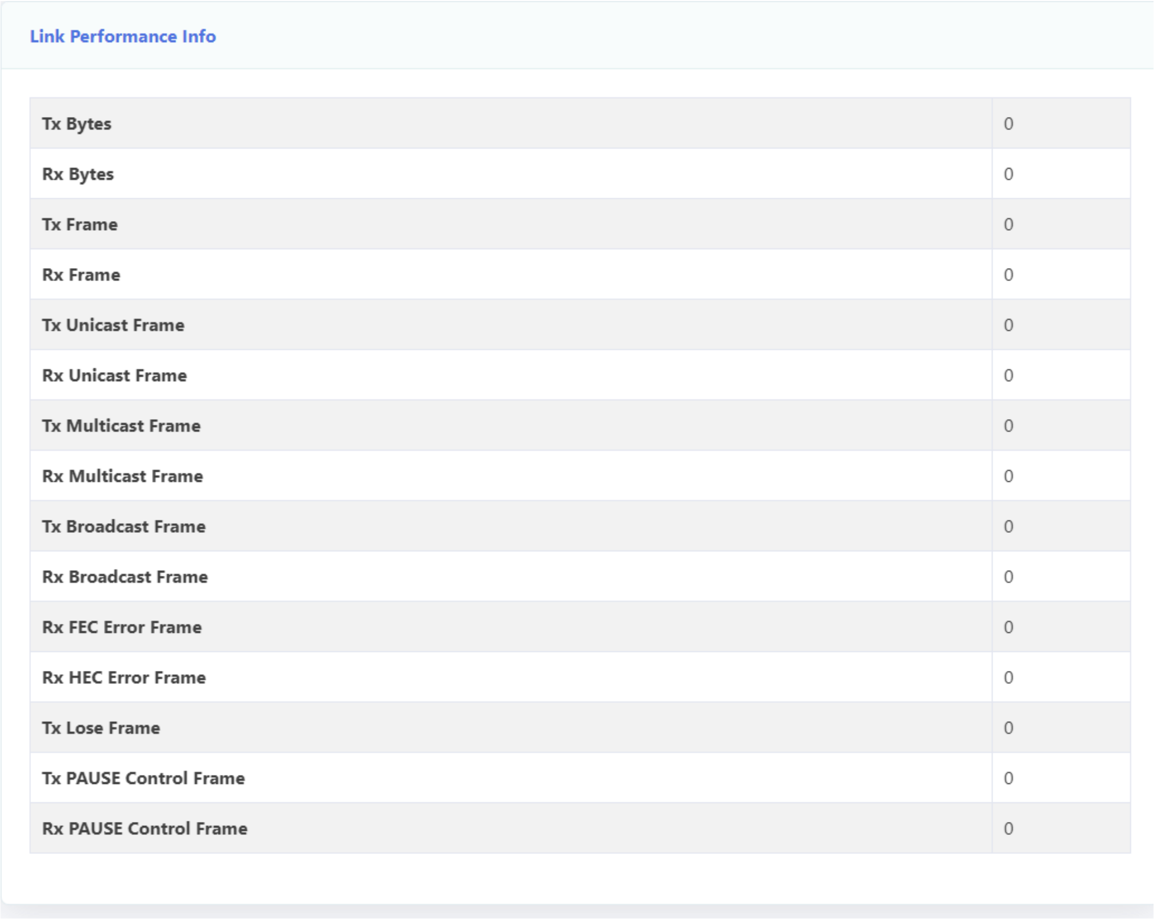
Laser Device Info

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 3-2-9: Laser Device Info

3.2.3.3 Link Performance Info

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



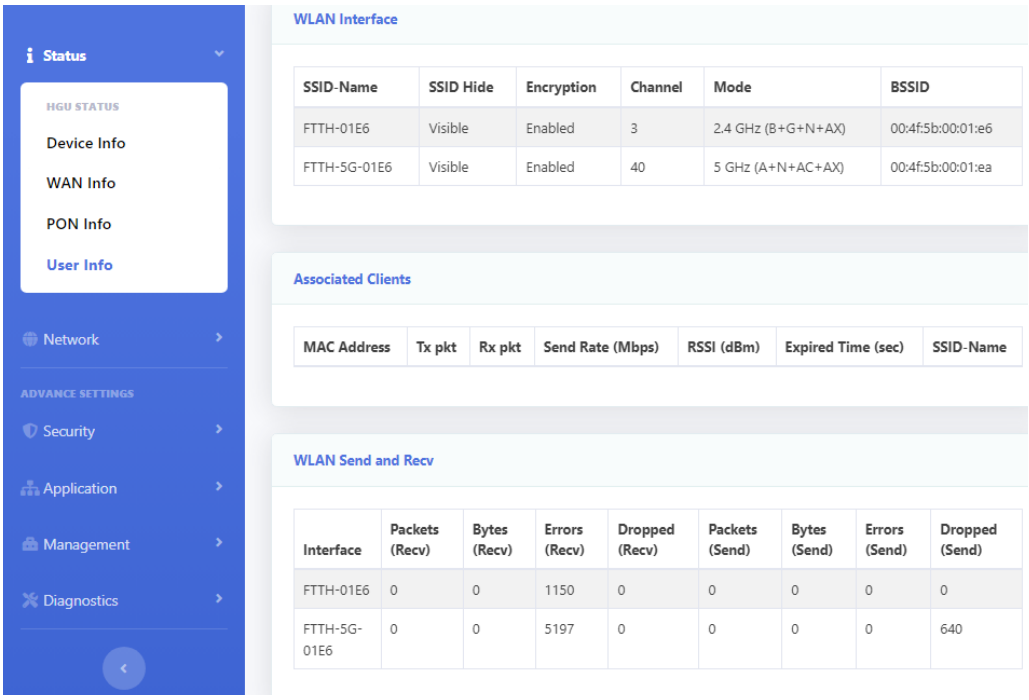
Link Performance Info

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 3-2-10: Link Performance Info

3.2.4 User Info

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



WLAN Interface

SSID-Name	SSID Hide	Encryption	Channel	Mode	BSSID
FTTH-01E6	Visible	Enabled	3	2.4 GHz (B+G+N+AX)	00:4f:5b:00:01:e6
FTTH-5G-01E6	Visible	Enabled	40	5 GHz (A+N+AC+AX)	00:4f:5b:00:01:ea

Associated Clients

MAC Address	Tx pkt	Rx pkt	Send Rate (Mbps)	RSSI (dBm)	Expired Time (sec)	SSID-Name

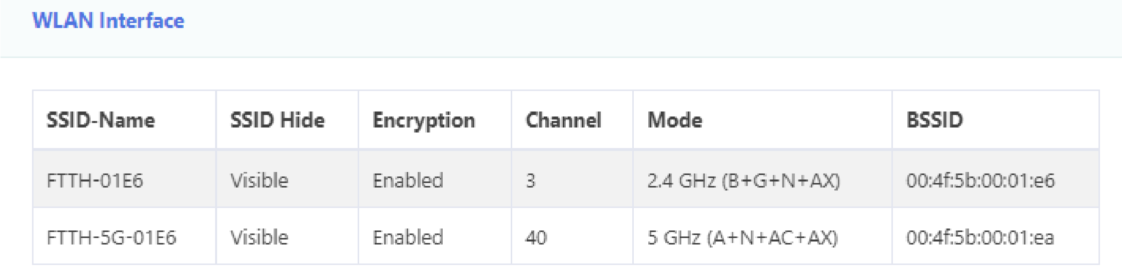
WLAN Send and Recv

Interface	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dropped (Send)
FTTH-01E6	0	0	1150	0	0	0	0	0
FTTH-5G-01E6	0	0	5197	0	0	0	0	640

Figure 3-2-11: User info

3.2.4.1 WLAN Interface

This page shows WLAN information, including SSID name, channel, whether enable security or not.



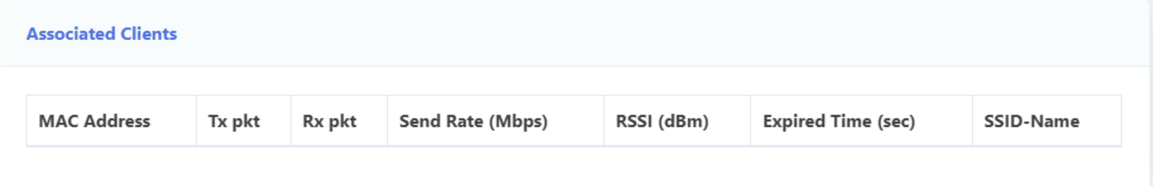
WLAN Interface

SSID-Name	SSID Hide	Encryption	Channel	Mode	BSSID
FTTH-01E6	Visible	Enabled	3	2.4 GHz (B+G+N+AX)	00:4f:5b:00:01:e6
FTTH-5G-01E6	Visible	Enabled	40	5 GHz (A+N+AC+AX)	00:4f:5b:00:01:ea

Figure 3-2-12: WLAN Interface

3.2.4.2 Associated Clients

The page shows the clients information associated with the WLAN, including the packet on send or receive direction, Send Rate, RSSI, Expired Time and SSID-Name.



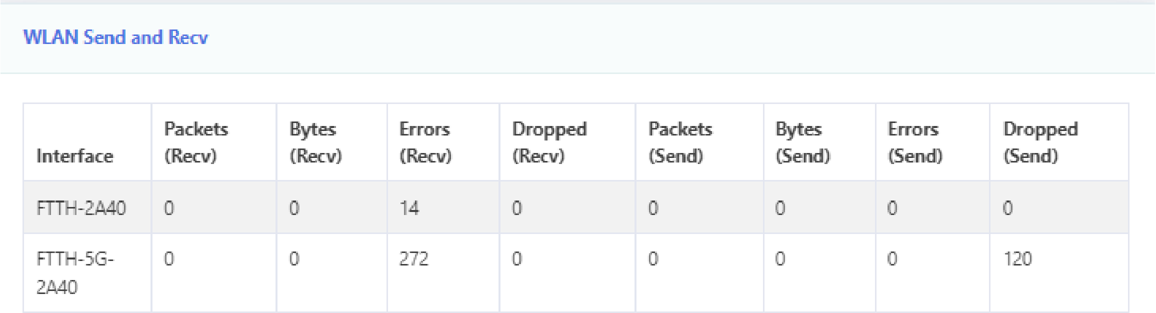
Associated Clients

MAC Address	Tx pkt	Rx pkt	Send Rate (Mbps)	RSSI (dBm)	Expired Time (sec)	SSID-Name

Figure 3-2-13:Associated Clients

3.2.4.3 WLAN Interface Statistics

The page shows the statistics of the WLAN in the sending and receiving directions.



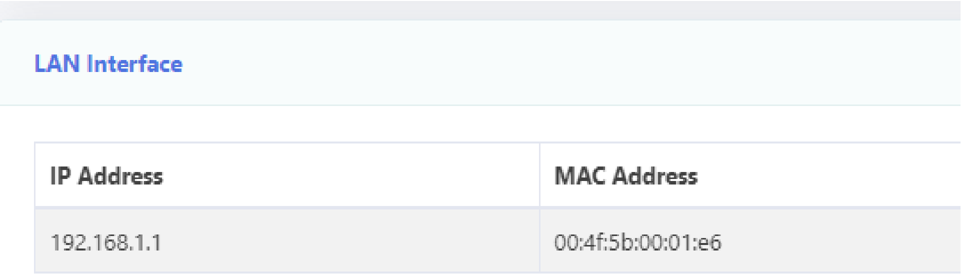
WLAN Send and Recv

Interface	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dropped (Send)
FTTH-2A40	0	0	14	0	0	0	0	0
FTTH-5G-2A40	0	0	272	0	0	0	0	120

Figure 3-2-14: WLAN Interface Statistics

3.2.4.4 LAN Interface

This page shows LAN address and LAN gateway.



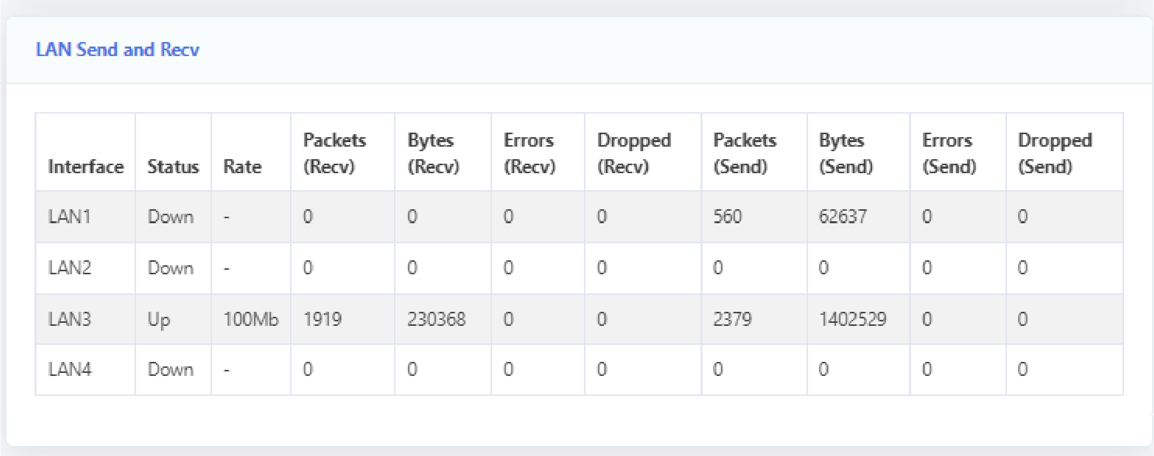
LAN Interface

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

Figure 3-2-15: LAN Interface

3.2.4.5 LAN Interface Statistics

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



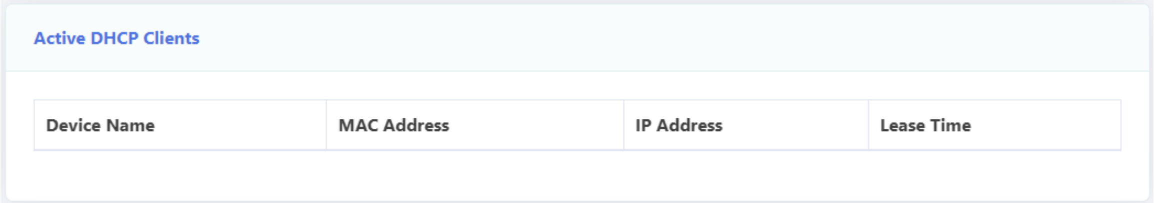
LAN Send and Recv

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	560	62637	0	0
LAN2	Down	-	0	0	0	0	0	0	0	0
LAN3	Up	100Mb	1919	230368	0	0	2379	1402529	0	0
LAN4	Down	-	0	0	0	0	0	0	0	0

Figure 3-2-16: LAN Interface Statistics

3.2.4.6 Active DHCP Clients

This page shows the lease information of the DHCP server.

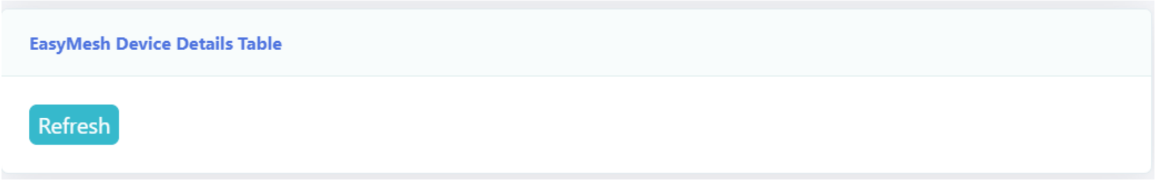


Active DHCP Clients

Device Name	MAC Address	IP Address	Lease Time

Figure 3-2-17:Active DHCP Clients

3.2.4.7 EasyMesh Device Details Table



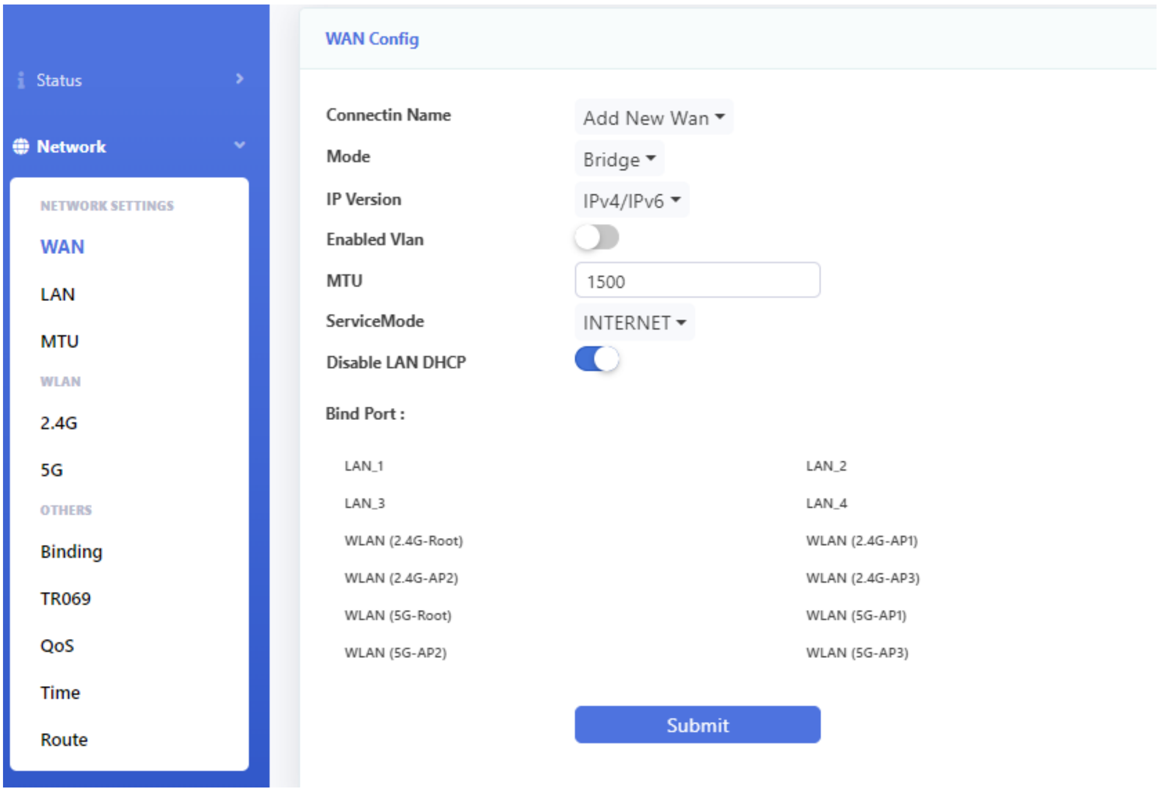
EasyMesh Device Details Table

Figure 3-2-18: EasyMesh Device Details Table

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.



Connectin Name: Add New Wan

Mode: Bridge

IP Version: IPv4/IPv6

Enabled Vlan: ○

MTU: 1500

ServiceMode: INTERNET

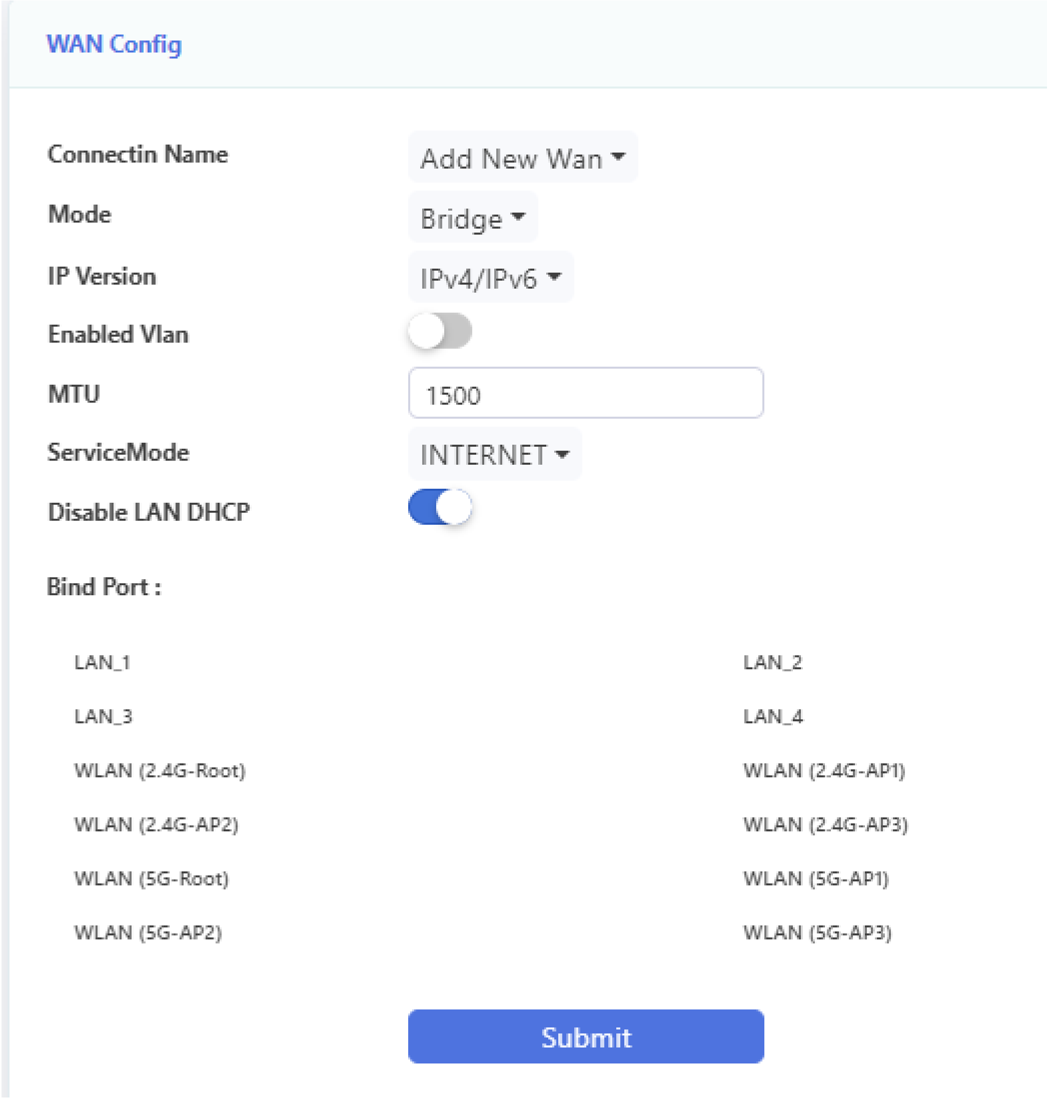
Disable LAN DHCP: ●

Bind Port :

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.



WAN Config

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
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

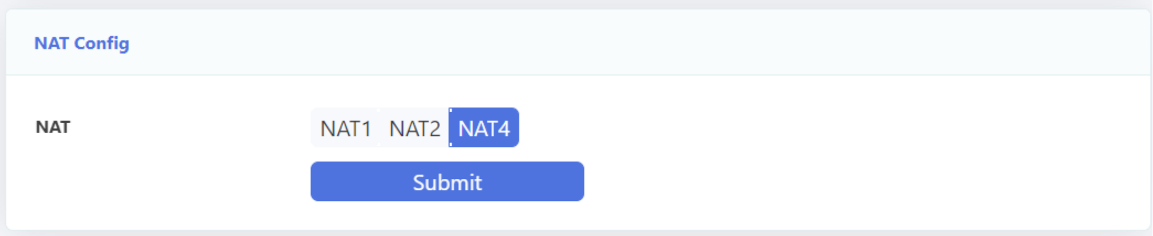
Figure 3-3-2:WAN config

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. E. g.: If this wan connection is used for VoIP, you should select the service mode which contains VOIP, such as TR069_VOIP_INTERNET, TR069_VOIP, VOIP or VOIP_INTERNET.
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 or SSID the wan connection has included.

3.3.1.2 NAT Config

This page allows you to set NAT type.



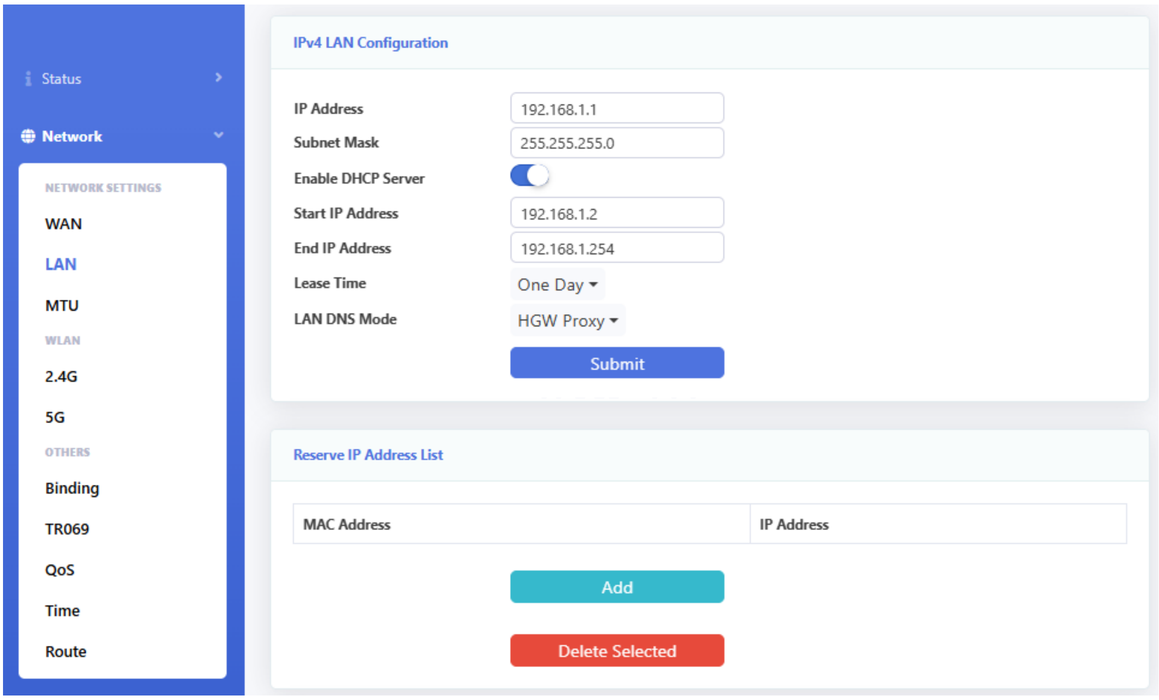
NAT Config

NAT: NAT1 NAT2 NAT4

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.



IPv4 LAN Configuration

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Enable DHCP Server: ●
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Lease Time: One Day
LAN DNS Mode: HGW Proxy

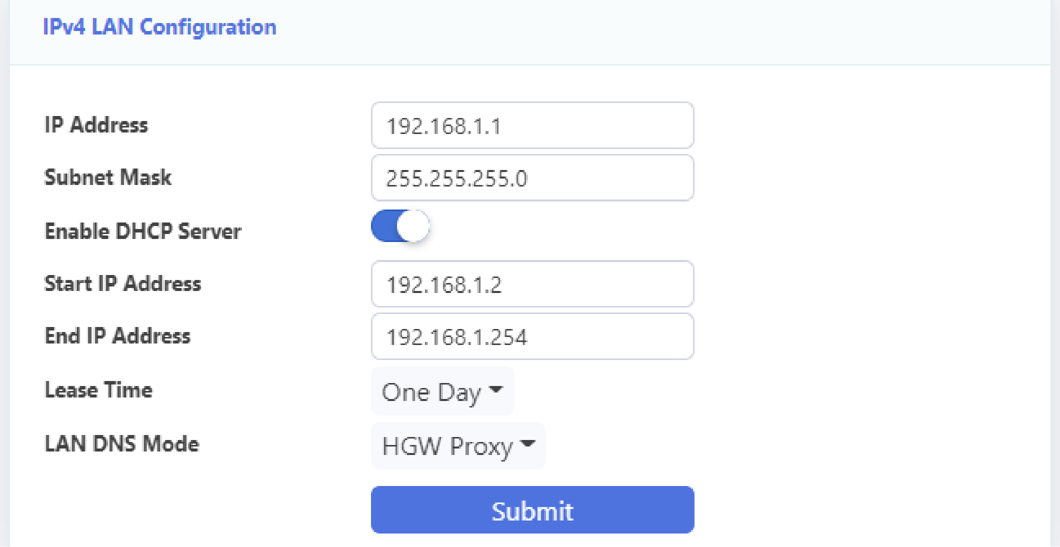
Reserve IP Address List

MAC Address	IP Address

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.



IPv4 LAN Configuration

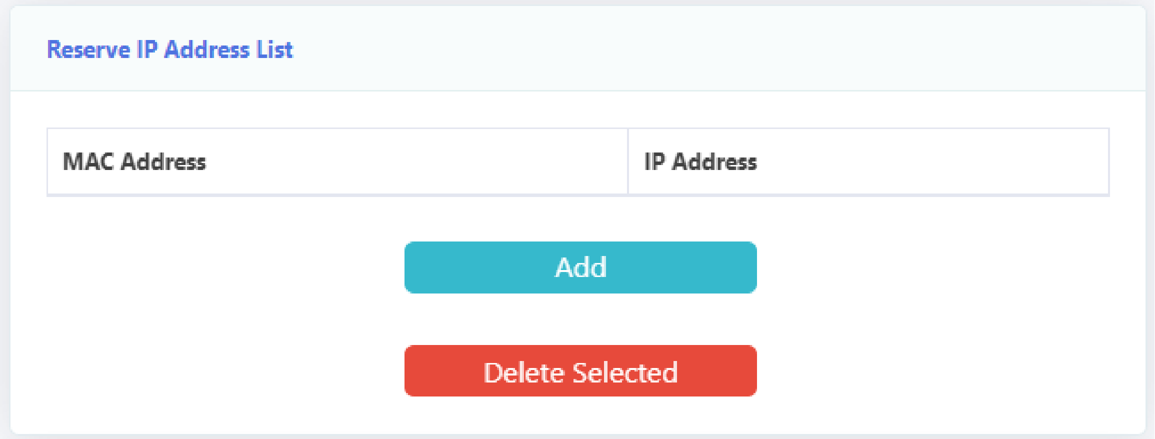
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Enable DHCP Server: ●
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Lease Time: One Day
LAN DNS Mode: HGW Proxy

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.



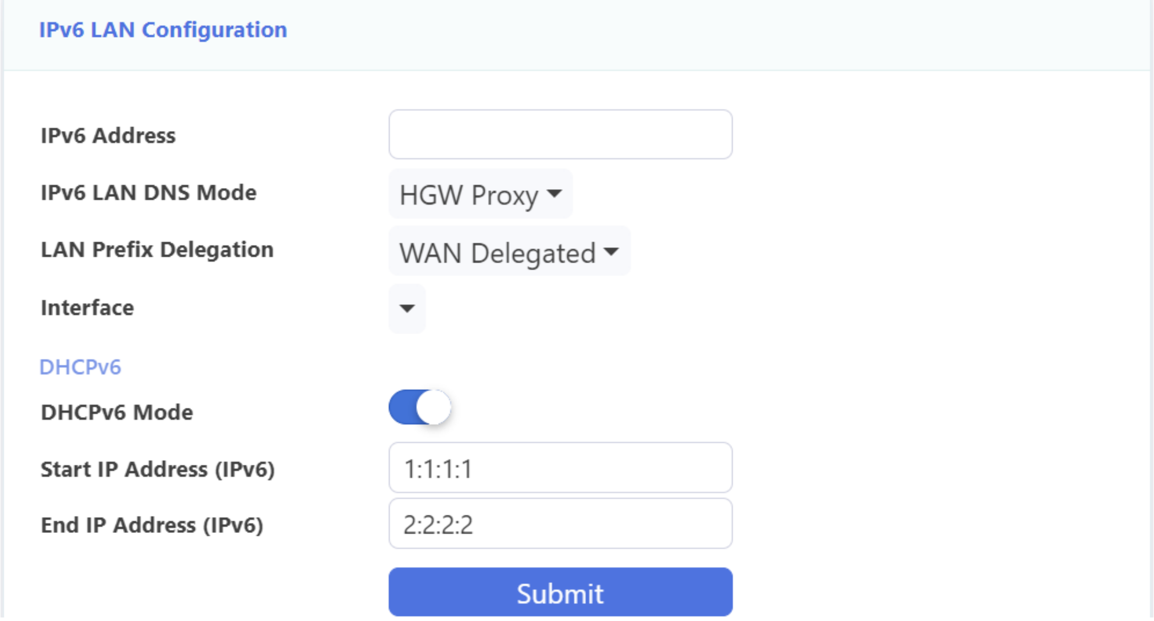
Reserve IP Address List

MAC Address	IP Address

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.



IPv6 LAN Configuration

IPv6 Address

IPv6 LAN DNS Mode: HGW Proxy

LAN Prefix Delegation: WAN Delegated

Interface

DHCPv6

DHCPv6 Mode

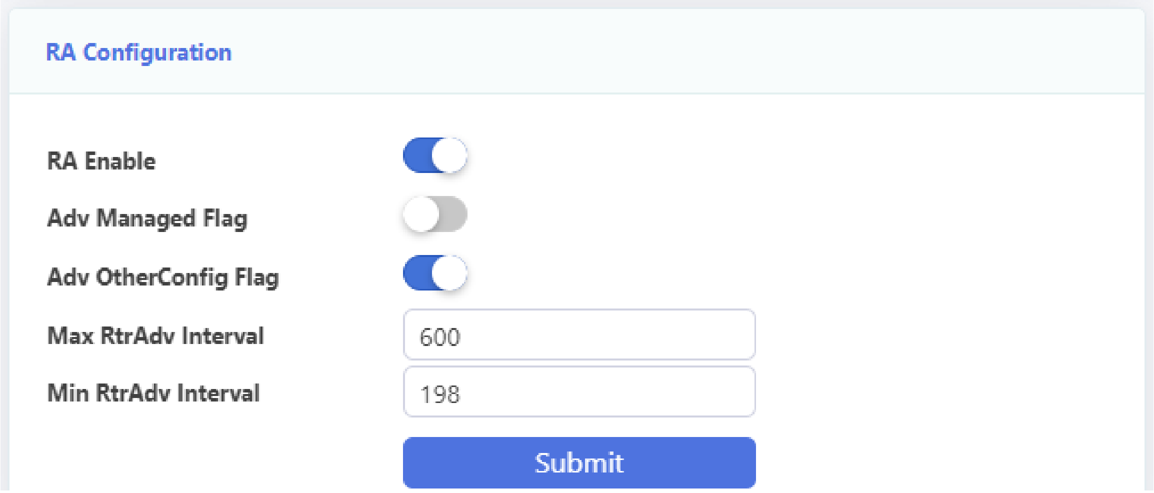
Start IP Address (IPv6): 1:1:1:1

End IP Address (IPv6): 2:2:2:2

Figure 3-3-7: IPv6 configuration

3.3.2.4 RA Configuration

This page allows you to do RA configuration.



RA Configuration

RA Enable

Adv Managed Flag

Adv OtherConfig Flag

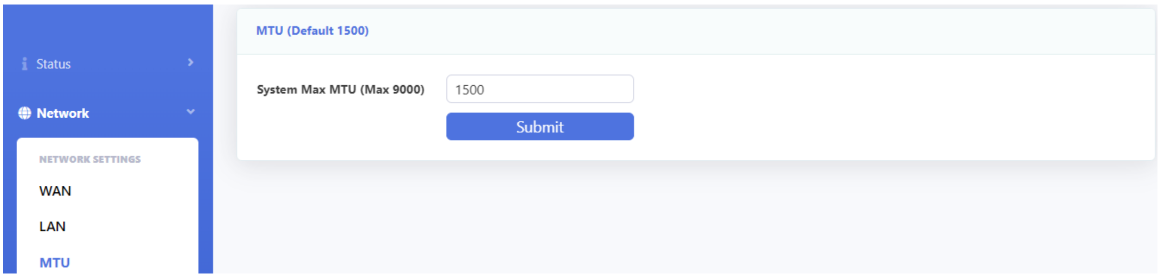
Max RtrAdv Interval: 600

Min RtrAdv Interval: 198

Figure 3-3-8: RA configuration

3.3.3 MTU

This page allows you to set system MTU.



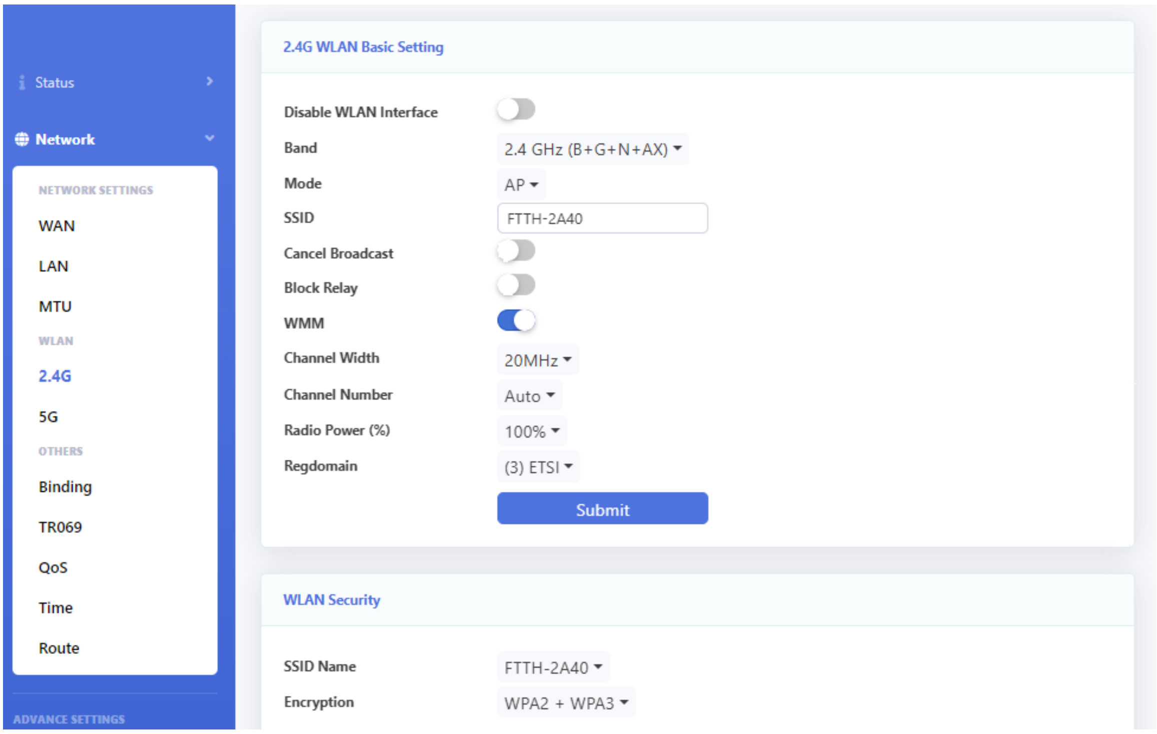
MTU (Default 1500)

System Max MTU (Max 9000): 1500

Figure 3-3-9: MTU

3.3.4 WLAN (2.4G)

This page is used to configure WIFI (2.4G) parameters. On each page, after configured you should click “Submit” button to save it. it is recommended to configure the Band to 2.4GHz (B+G+N+AX).



2.4G WLAN Basic Setting

Disable WLAN Interface
Band: 2.4 GHz (B+G+N+AX)
Mode: AP
SSID: FTTH-2A40
Cancel Broadcast
Block Relay
WMM
Channel Width: 20MHz
Channel Number: Auto
Radio Power (%): 100%
Regdomain: (3) ETSI

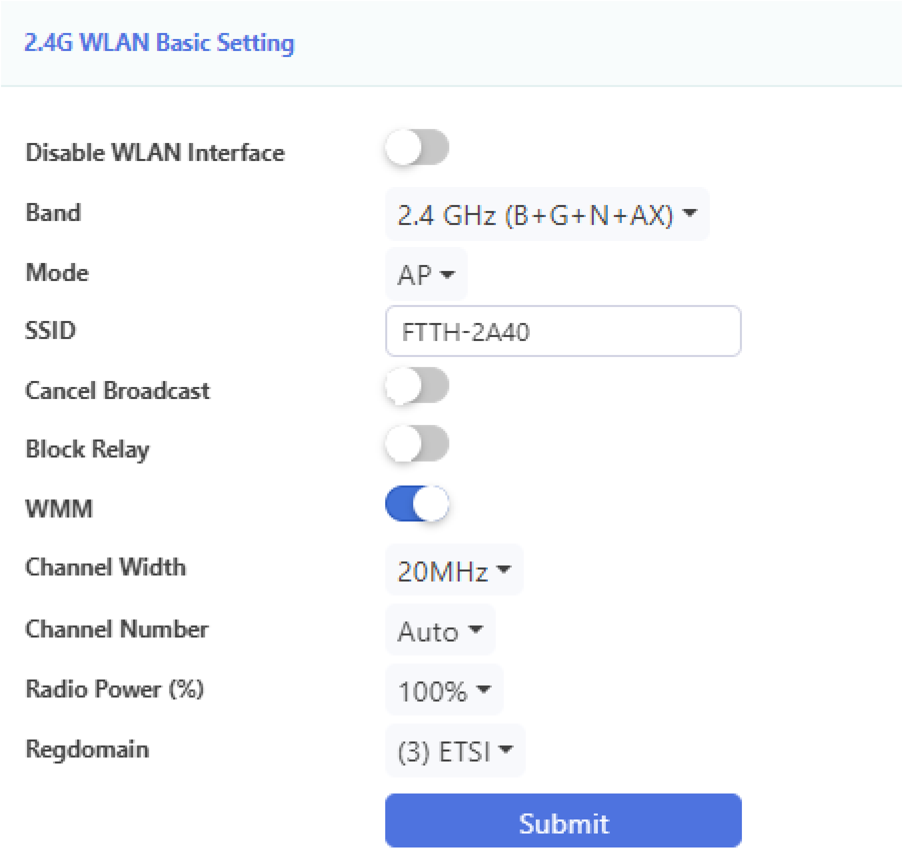
WLAN Security

SSID Name: FTTH-2A40
Encryption: WPA2 + WPA3

Figure 3-3-10: 2.4G

3.3.4.1 2.4G WLAN Basic Setting

This page allows you to configure wireless basic settings. Basic settings include wireless switch, 2.4G WiFi band, SSID name, channel and so on.



2.4G WLAN Basic Setting

Disable WLAN Interface

Band: 2.4 GHz (B+G+N+AX)

Mode: AP

SSID: FTTH-2A40

Cancel Broadcast

Block Relay

WMM

Channel Width: 20MHz

Channel Number: Auto

Radio Power (%): 100%

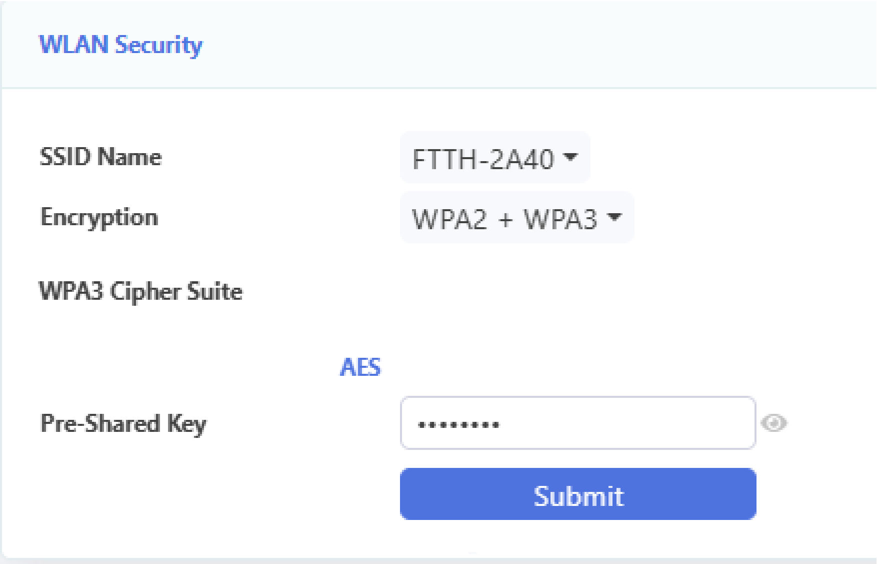
Regdomain: (3) ETSI

Figure 3-3-11: 2.4 G WLAN Basic Setting

Parameter	Illustration
Disable WLAN Interface	Enable or Disable WLAN.
Band	Choose 2.4G WiFi band. This device supports 802.11ax.
SSID	SSID Name. It is used to distinguish from other WLAN.
Cancel Broadcast	Disable or Enable transmit broadcast in WLAN.
Block Relay	Disable or Enable isolate WLAN clients.
WMM	WiFi MultiMedia. Video and audio traffic will have higher priority when WMM is enabled.
Channel width	WLAN channel width.
Channel Number	WLAN channel, default value is auto.
Radio power	Configure wifi transmit power.
Regdomain	Configure country or region.

3.3.4.2 WLAN security

This page is used to set the WLAN security, Encryption mode and the pre-share key.



WLAN Security

SSID Name: FTTH-2A40

Encryption: WPA2 + WPA3

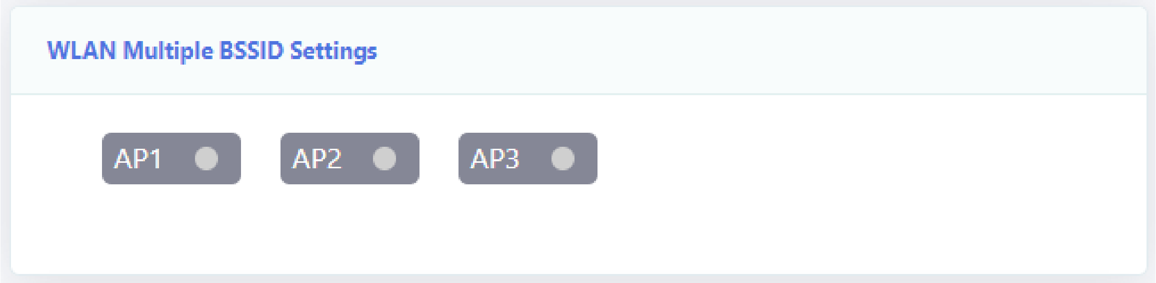
WPA3 Cipher Suite: AES

Pre-Shared Key: ••••••••

Figure 3-3-12: WLAN Security

3.3.4.3 Multiple AP

This page allows you to configure multiple AP parameters. They are turned off by default.

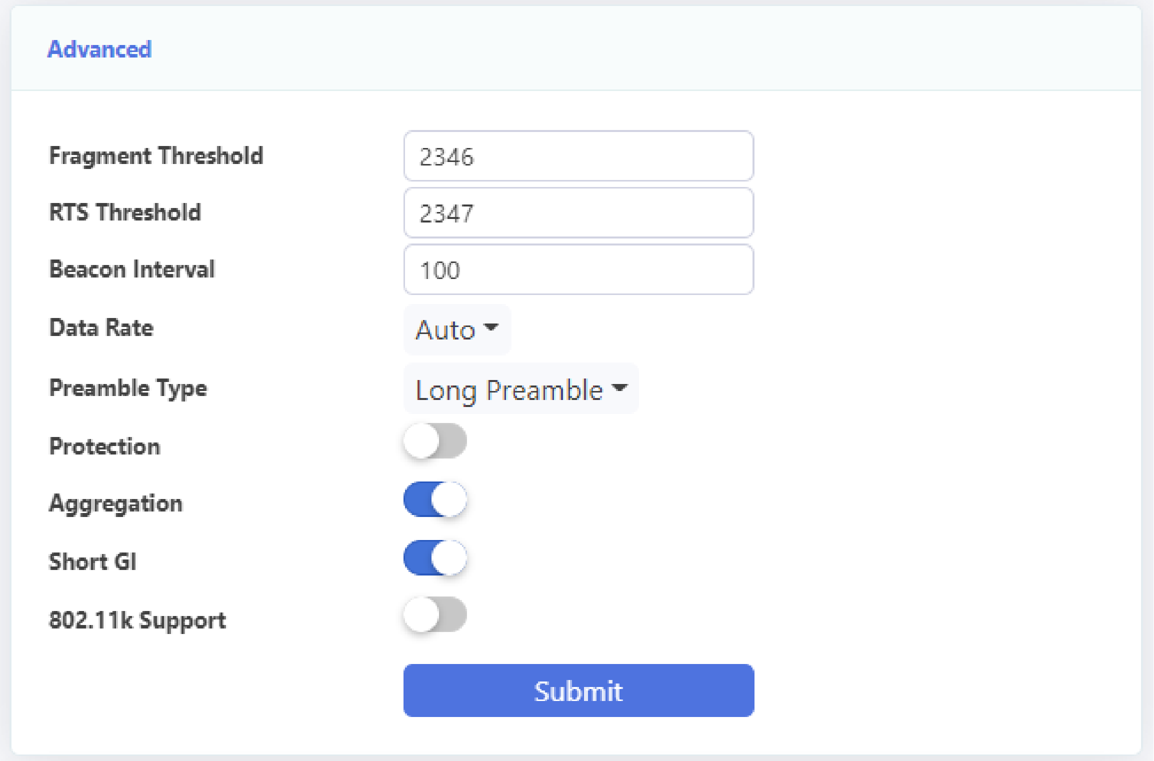


WLAN Multiple BSSID Settings

Figure 3-3-13:Multiple AP

3.3.4.4 WLAN advanced

These settings are only for more technically advanced users who have sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



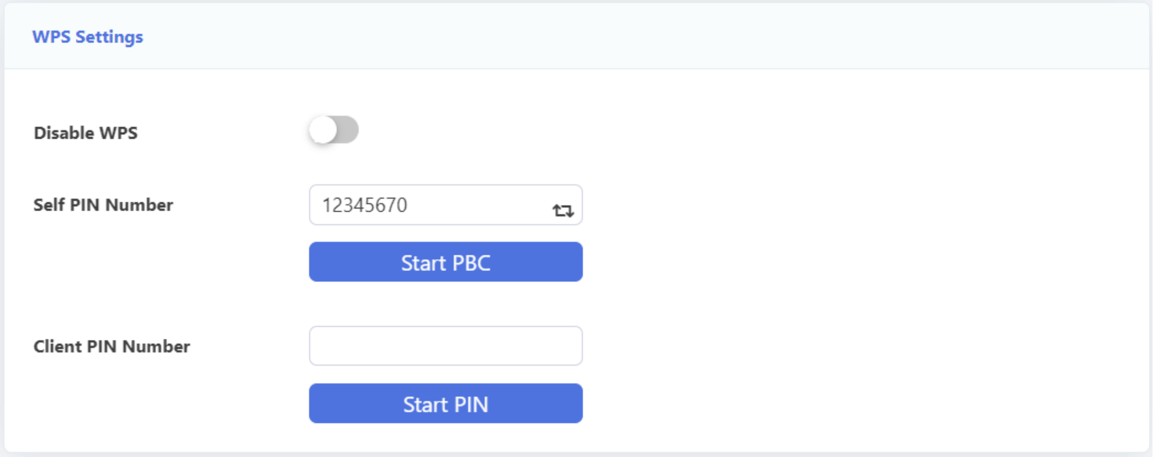
Advanced

Fragment Threshold	2346
RTS Threshold	2347
Beacon Interval	100
Data Rate	Auto
Preamble Type	Long Preamble
Protection	Off
Aggregation	On
Short GI	On
802.11k Support	Off

Figure 3-3-14: WLAN Advanced

3.3.4.5 WPS

These settings allows you to configure WPS setting.



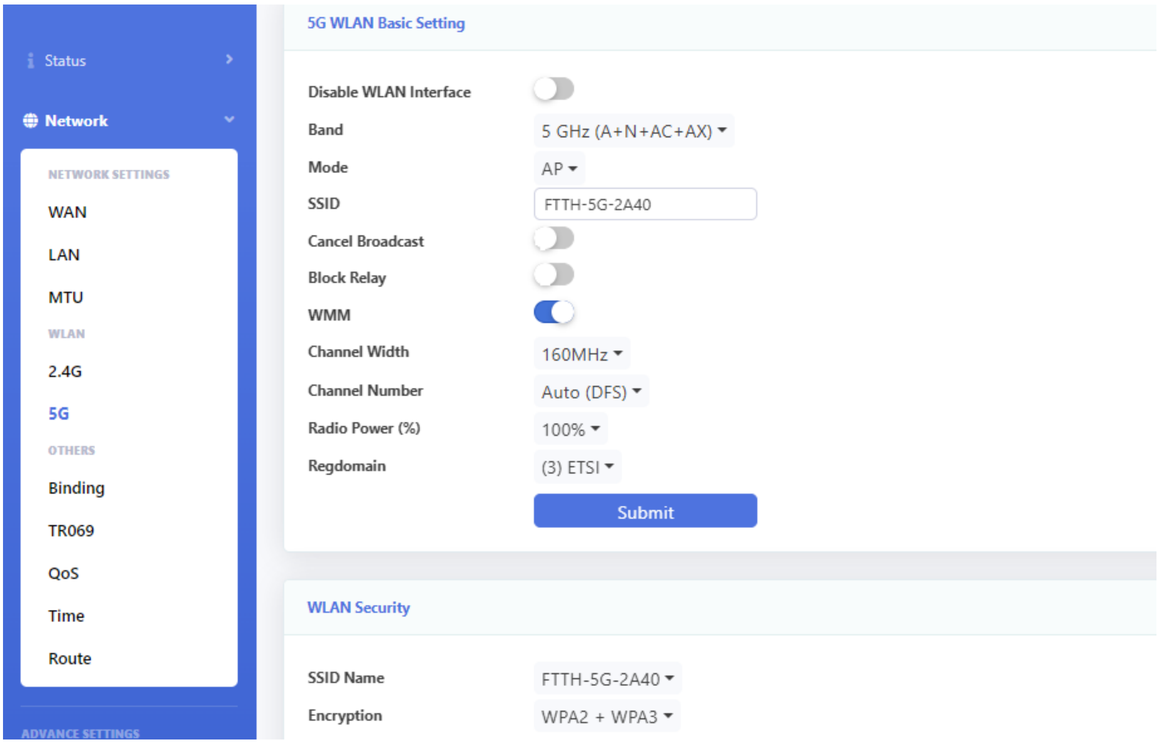
WPS Settings

Disable WPS	Off
Self PIN Number	12345670
Client PIN Number	

Figure 3-3-15: WPS Settings

3.3.5 WLAN (5G)

This page is used to configure WIFI (5G) parameters. On each page, after configured you should click “Submit” button to save it. And this device supports WiFi6, if the terminal device also supports WiFi6, it is recommended to configure the Band to 5GHz (A+N+AC+AX).



5G WLAN Basic Setting

Disable WLAN Interface ○
Band: 5 GHz (A+N+AC+AX)
Mode: AP
SSID: FTTH-5G-2A40
Cancel Broadcast ○
Block Relay ○
WMM ●
Channel Width: 160MHz
Channel Number: Auto (DFS)
Radio Power (%): 100%
Regdomain: (3) ETSI

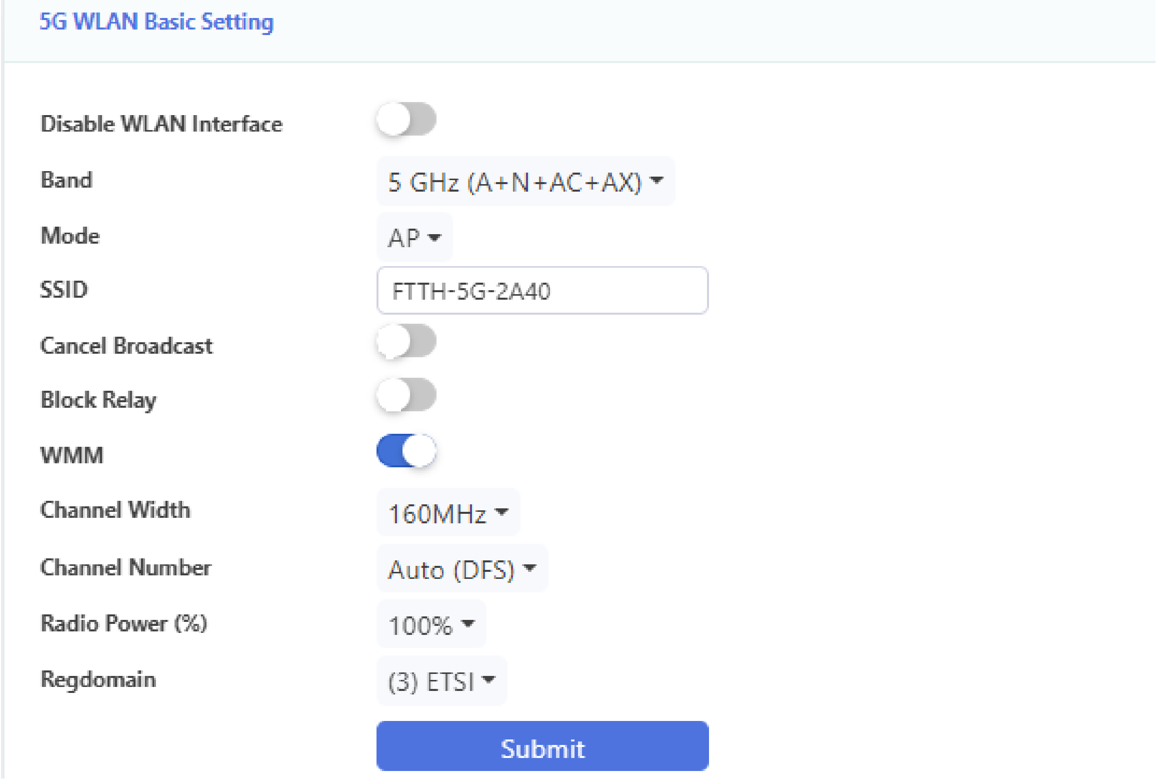
WLAN Security

SSID Name: FTTH-5G-2A40
Encryption: WPA2 + WPA3

Figure 3-3-16: 5G

3.3.5.1 5G WLAN Basic Setting

This page allows you to configure wireless basic settings. Basic settings include wireless switch, SSID name, channel width, channel number, radio power and so on.



5G WLAN Basic Setting

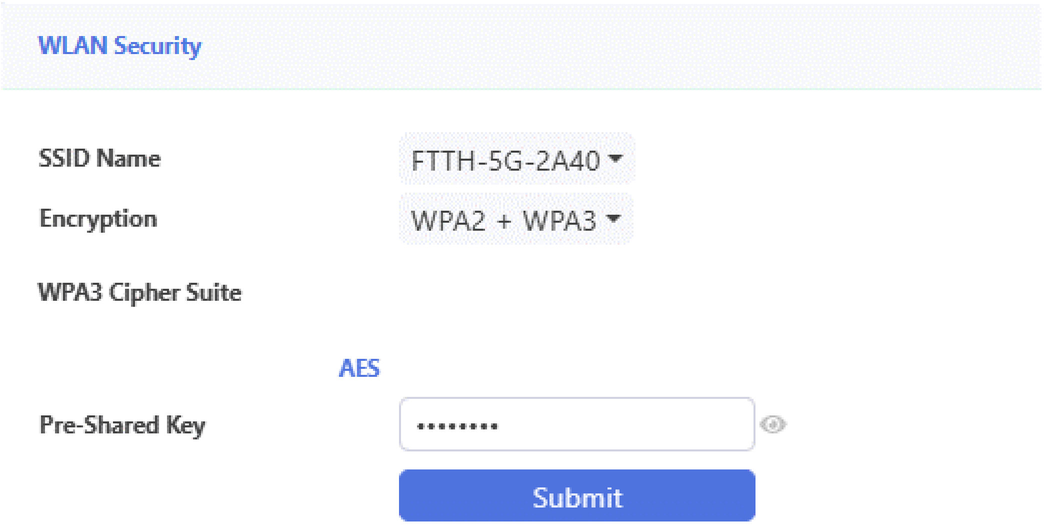
Disable WLAN Interface ○
Band: 5 GHz (A+N+AC+AX)
Mode: AP
SSID: FTTH-5G-2A40
Cancel Broadcast ○
Block Relay ○
WMM ●
Channel Width: 160MHz
Channel Number: Auto (DFS)
Radio Power (%): 100%
Regdomain: (3) ETSI

Figure 3-3-17: 5G WLAN Basic Setting

Parameter	Illustration
Disable WLAN Interface	Enable or Disable WLAN.
Band	Choose 5G WiFi band. This device supports 802.11ax.
SSID	SSID Name. It is used to distinguish from other WLAN.
Cancel Broadcast	Disable or Enable transmit broadcast in WLAN.
Block Relay	Disable or Enable isolate WLAN clients.
WMM	WiFi MultiMedia. Video and audio traffic will have higher priority when WMM is enabled.
Channel width	WLAN channel width.
Channel Number	WLAN channel, default value is auto.
Radio power	Configure wifi transmit power.
Regdomain	Configure country or region.

3.3.5.2 WLAN security

This page is used to set the WLAN security, Encryption mode and the pre-share key.



WLAN Security

SSID Name: FTTH-5G-2A40

Encryption: WPA2 + WPA3

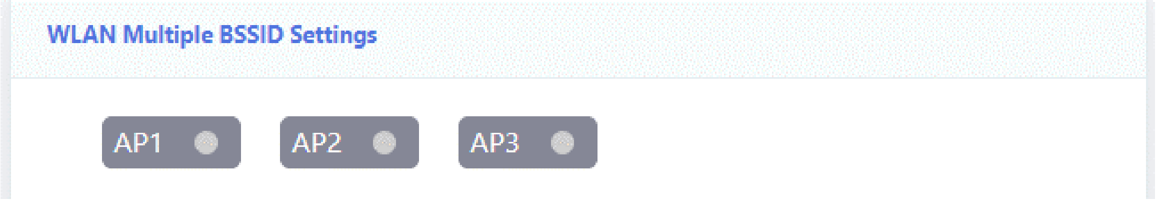
WPA3 Cipher Suite: AES

Pre-Shared Key: ••••••••

Figure 3-3-18:5G WLAN Security

3.3.5.3 Multiple AP

This page allows you to configure multiple AP parameters. They are turned off by default.

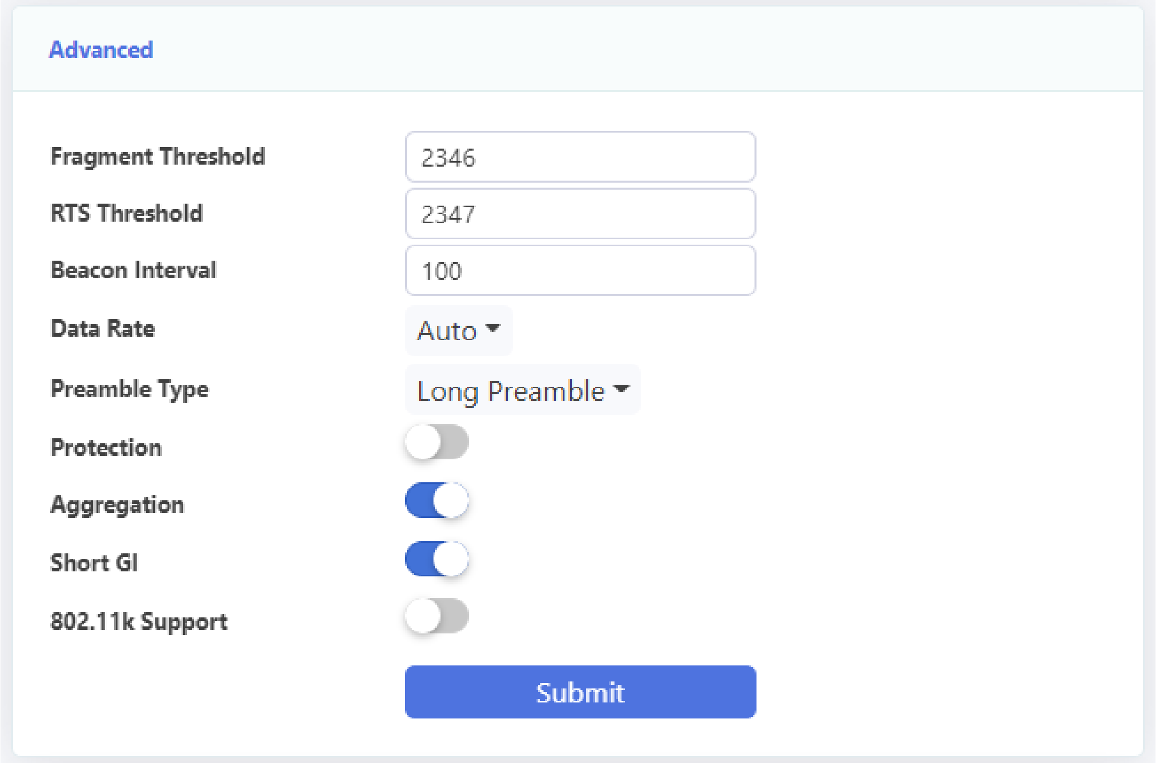


WLAN Multiple BSSID Settings

Figure 3-3-19:Multiple AP

3.3.5.4 WLAN advanced

These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



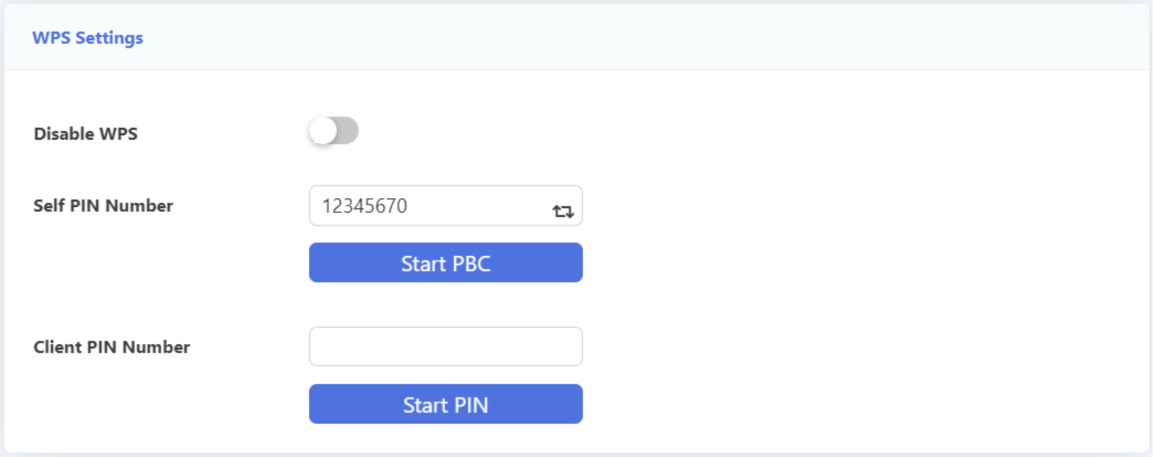
Advanced

Fragment Threshold	2346
RTS Threshold	2347
Beacon Interval	100
Data Rate	Auto
Preamble Type	Long Preamble
Protection	○
Aggregation	●
Short GI	●
802.11k Support	○

Figure 3-3-20: WLAN Advanced

3.3.5.5 WPS

These settings allow you to configure WPS setting.



WPS Settings

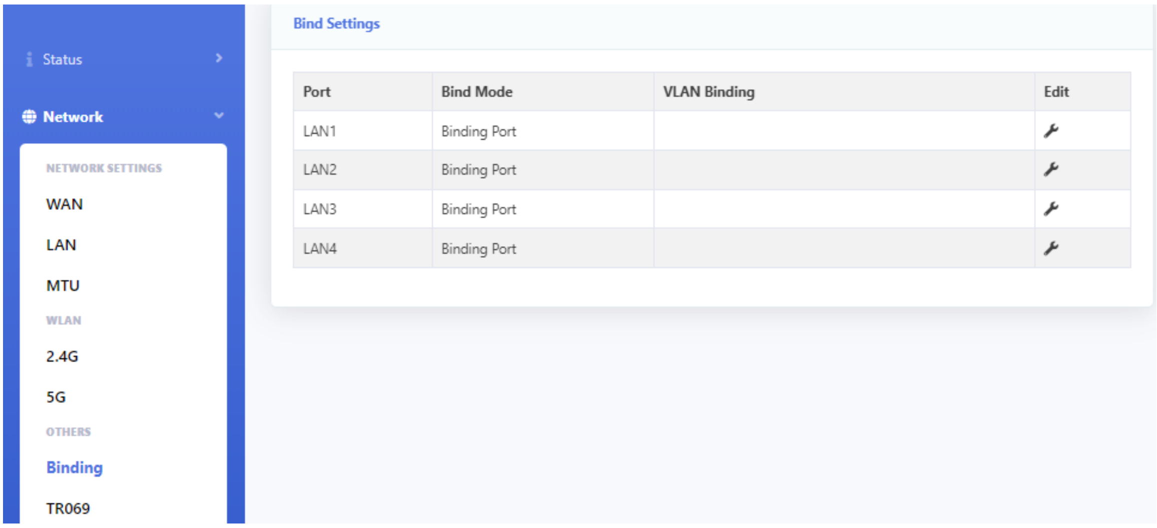
Disable WPS	○
Self PIN Number	12345670
Client PIN Number	

Figure 3-3-21: WPS Settings

3.3.6 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.



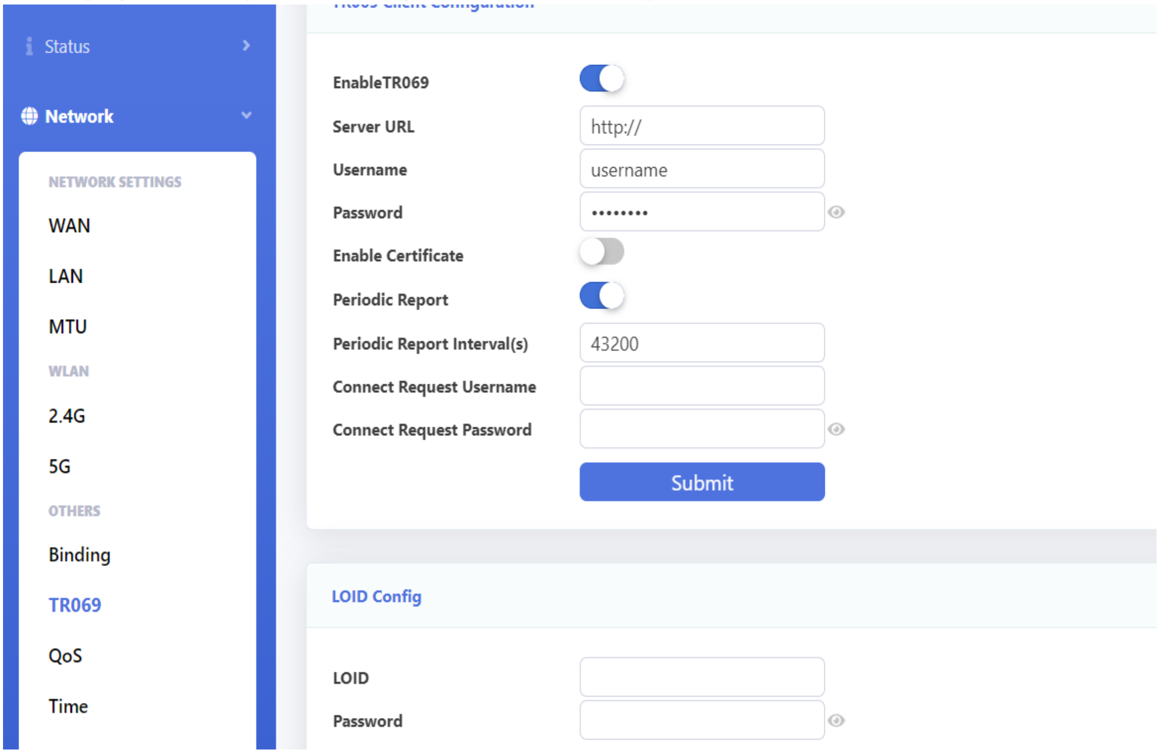
Bind Settings

Port	Bind Mode	VLAN Binding	Edit
LAN1	Binding Port		🔧
LAN2	Binding Port		🔧
LAN3	Binding Port		🔧
LAN4	Binding Port		🔧

Figure 3-3-22: Binding Settings

3.3.7 TR069

This page allows you to configure Tr069-related parameters.



EnableTR069	● On
Server URL	http://
Username	username
Password	••••••••
Enable Certificate	○ Off
Periodic Report	● On
Periodic Report Interval(s)	43200
Connect Request Username	
Connect Request Password	

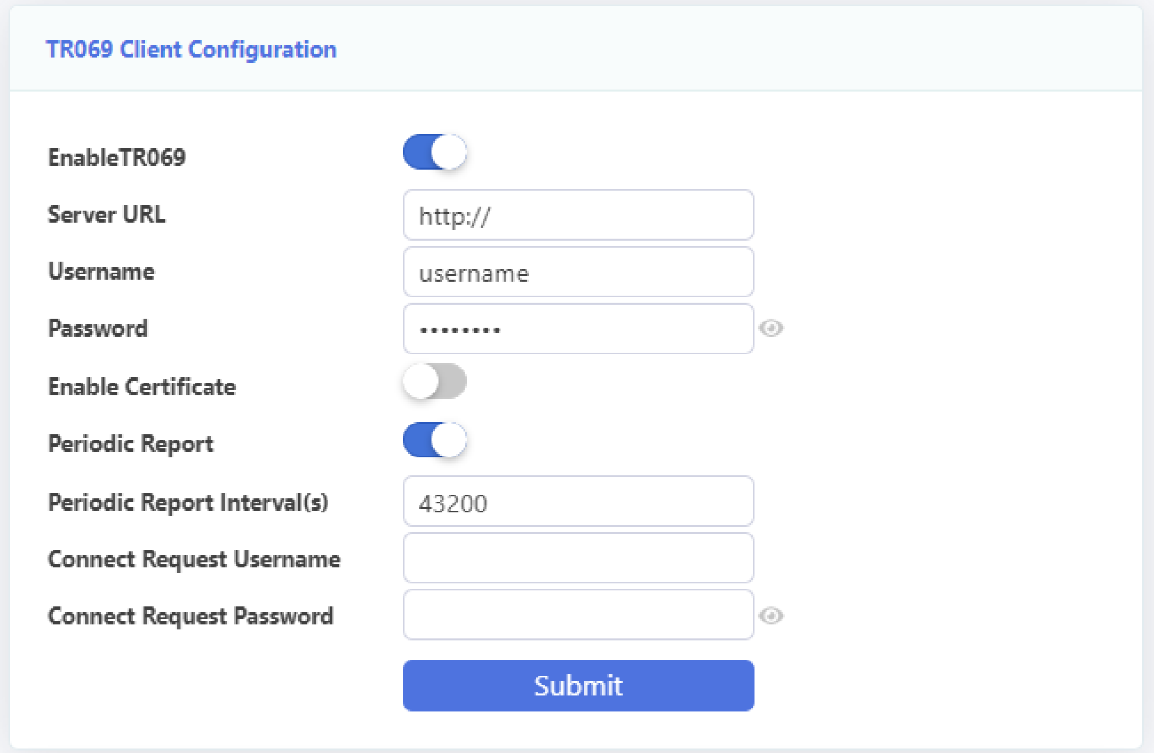
LOID Config

LOID	
Password	

Figure 3-3-23: TR069

3.3.7.1 ACS Client Configuration

This page allows you to configure ACS connection parameters.



TR069 Client Configuration

EnableTR069: on

Server URL: http://

Username: username

Password: ••••••••

Enable Certificate: off

Periodic Report: on

Periodic Report Interval(s): 43200

Connect Request Username:

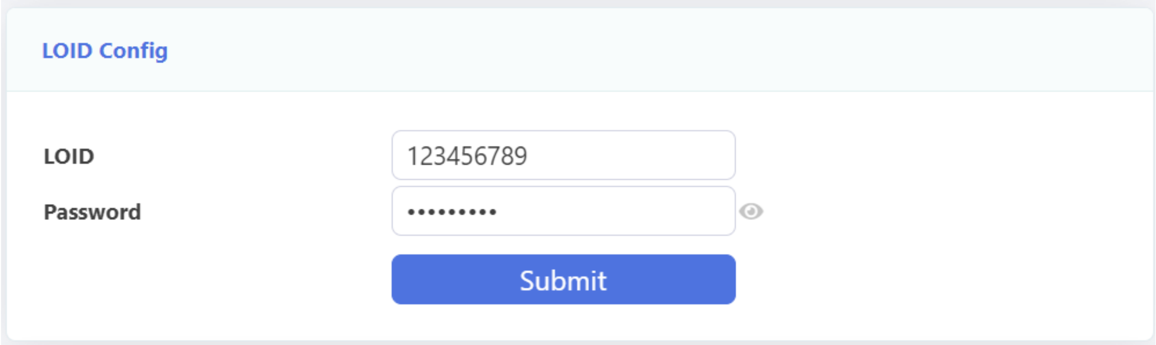
Connect Request Password:

Figure 3-3-24: 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.

3.3.7.2 LOID Config

LOID is used for PON authentication.



LOID Config

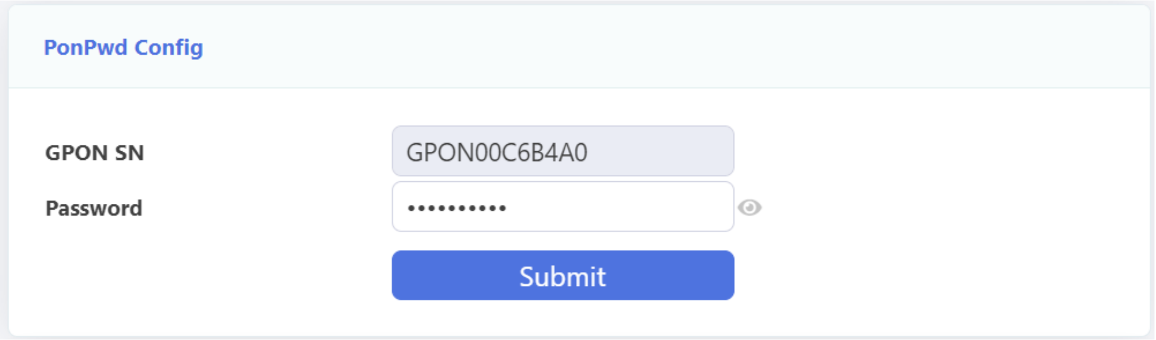
LOID 123456789

Password •••••••••

Figure 3-3-25: LOID configuration

3.3.7.3 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

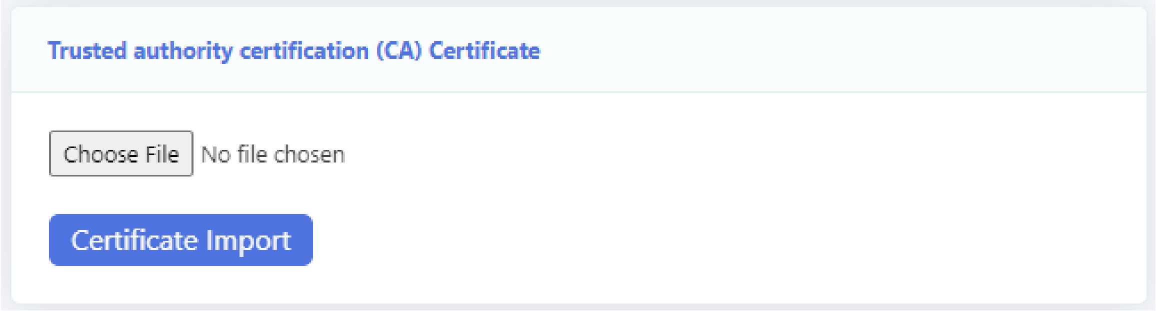
GPON SN GPON00C6B4A0

Password ••••••••••

Figure 3-3-26: Password configuration

3.3.7.4 CA Certificate

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



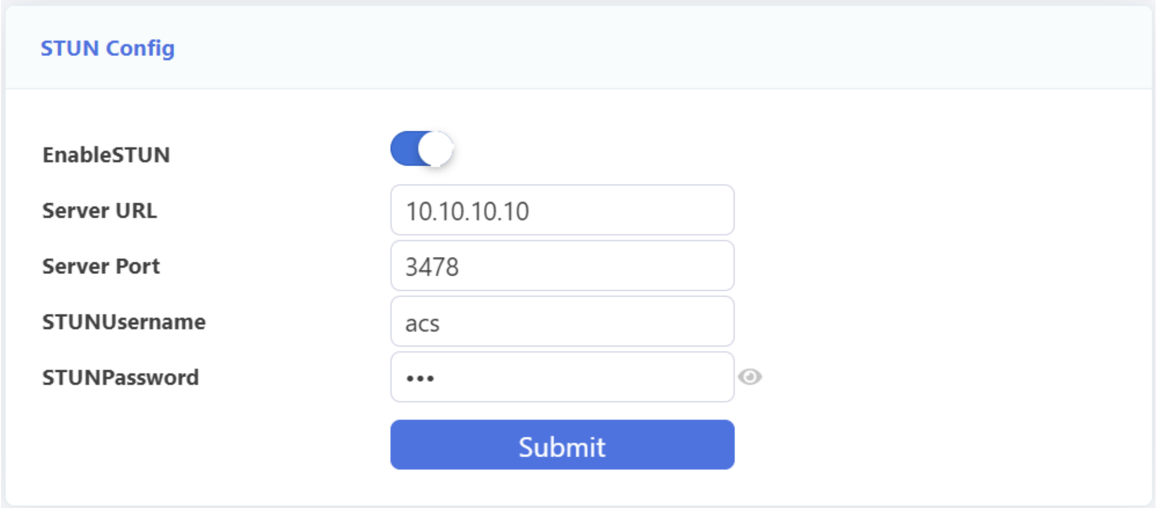
Trusted authority certification (CA) Certificate

Choose File No file chosen

Figure 3-3-27: Upload CA certificate

3.3.7.5 STUN

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



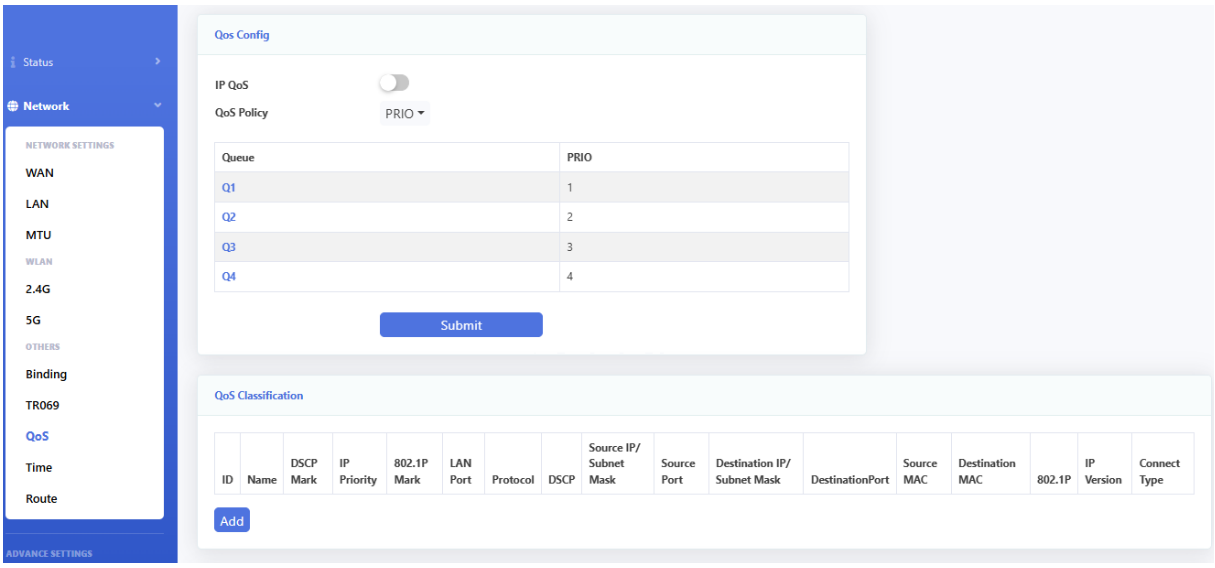
STUN Config

EnableSTUN	●
Server URL	10.10.10.10
Server Port	3478
STUNUsername	acs
STUNPassword	•••

Figure 3-3-28: STUN Config

3.3.8 Qos

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



Qos Config

IP QoS	○
QoS Policy	PRIO ▾

Queue	PRIO
Q1	1
Q2	2
Q3	3
Q4	4

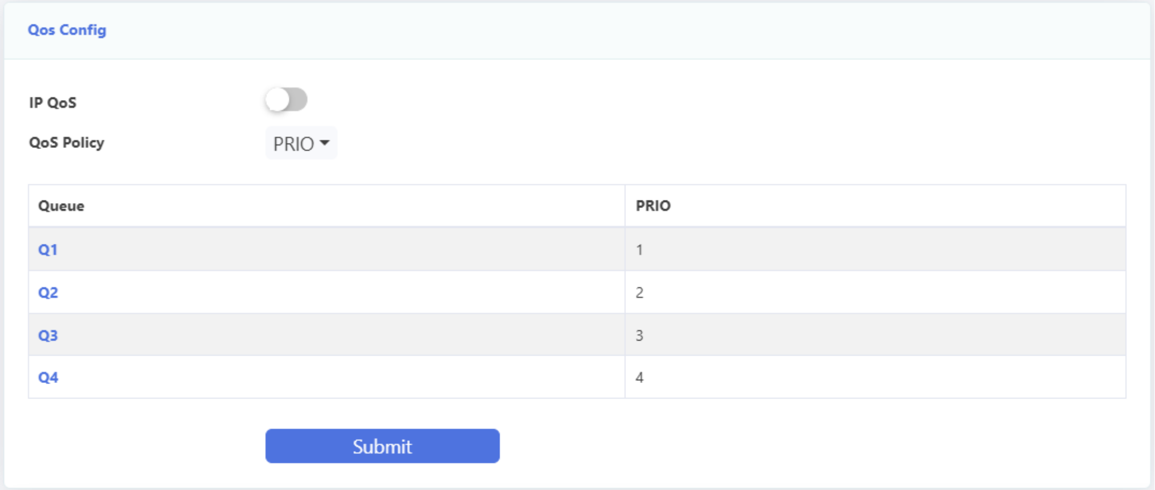
QoS Classification

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

Figure 3-3-29: Qos

3.3.8.1 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'.



Qos Config

IP QoS

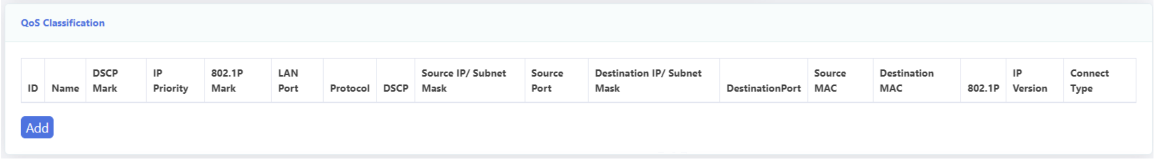
QoS Policy PRIO

Queue	PRIO
Q1	1
Q2	2
Q3	3
Q4	4

Figure 3-3-30: QoS Config

3.3.8.2 QoS Classification

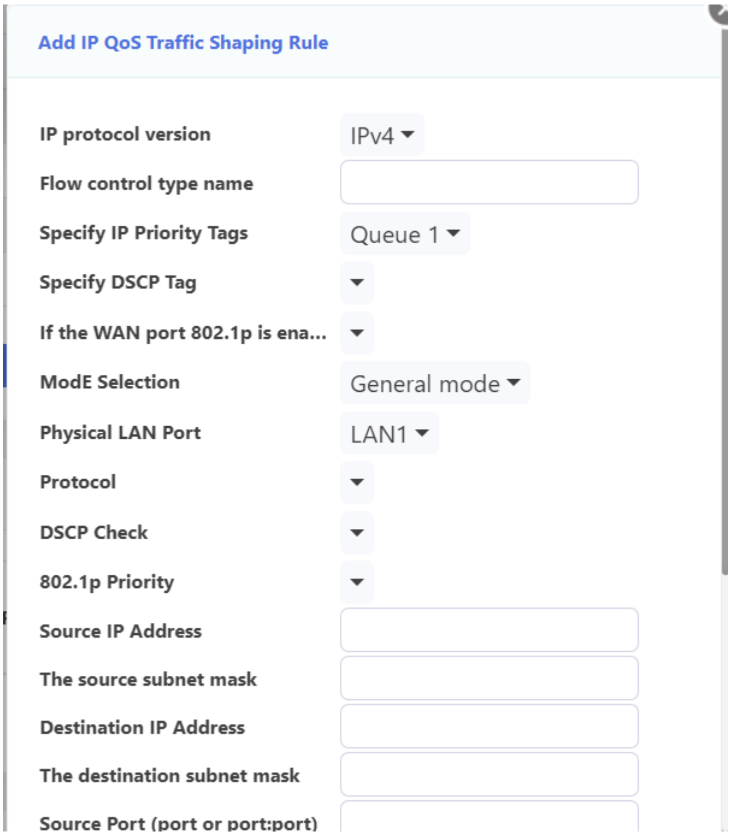
This page is used to configure the QoS classification. Click on the "Add" button to add the network traffic control type rules.



QoS Classification

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

Figure 3-3-31: 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

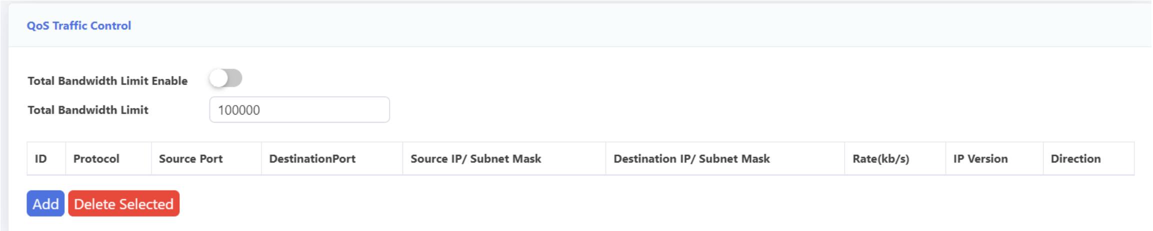
Source Port (port or port:port)

Figure 3-3-32: 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.

3.3.8.3 QoS Traffic Control

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



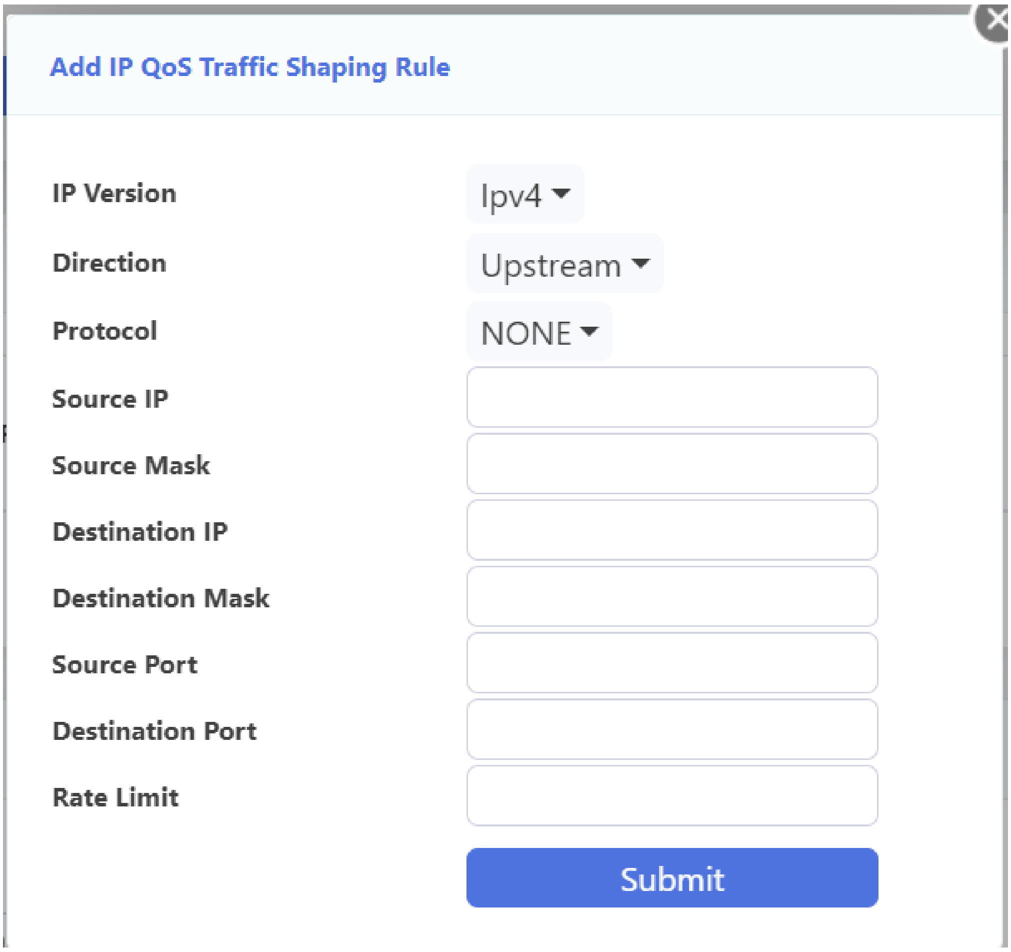
QoS Traffic Control

Total Bandwidth Limit Enable

Total Bandwidth Limit: 100000

ID	Protocol	Source Port	DestinationPort	Source IP/ Subnet Mask	Destination IP/ Subnet Mask	Rate(kb/s)	IP Version	Direction

Figure 3-3-33: QoS Traffic Control



Add IP QoS Traffic Shaping Rule

IP Version: Ipv4

Direction: Upstream

Protocol: NONE

Source IP

Source Mask

Destination IP

Destination Mask

Source Port

Destination Port

Rate Limit

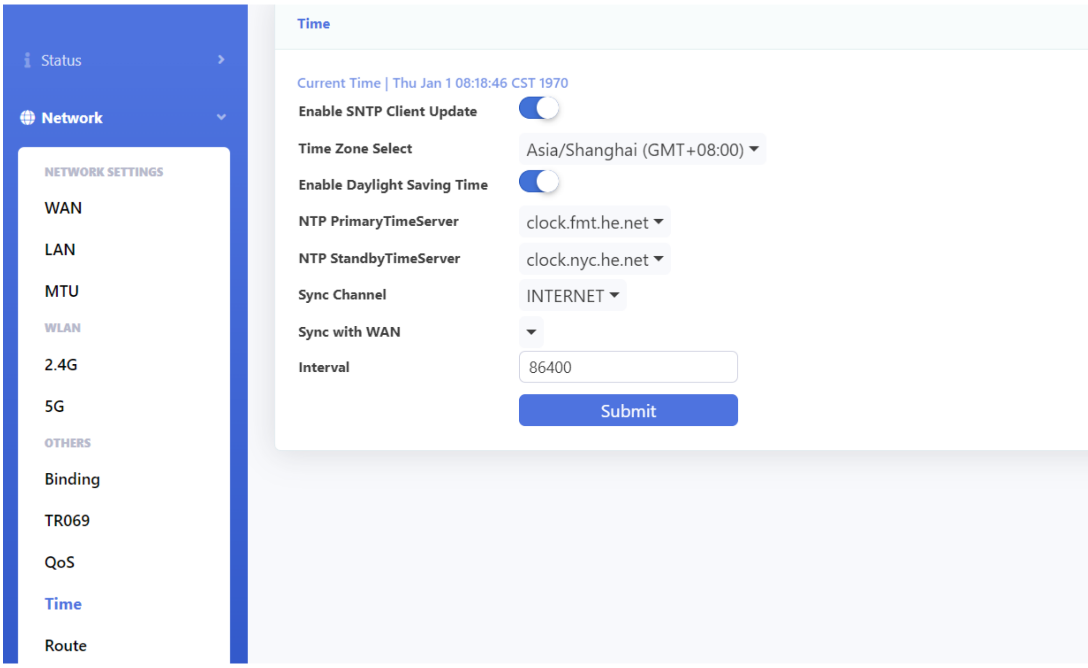
Figure 3-3-34: QoS Traffic Control Shaping Rule

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	Iput 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.

3.3.9 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.



Time

Current Time | Thu Jan 1 08:18:46 CST 1970

Enable SNTP Client Update: on

Time Zone Select: Asia/Shanghai (GMT+08:00)

Enable Daylight Saving Time: on

NTP PrimaryTimeServer: clock.fmt.he.net

NTP StandbyTimeServer: clock.nyc.he.net

Sync Channel: INTERNET

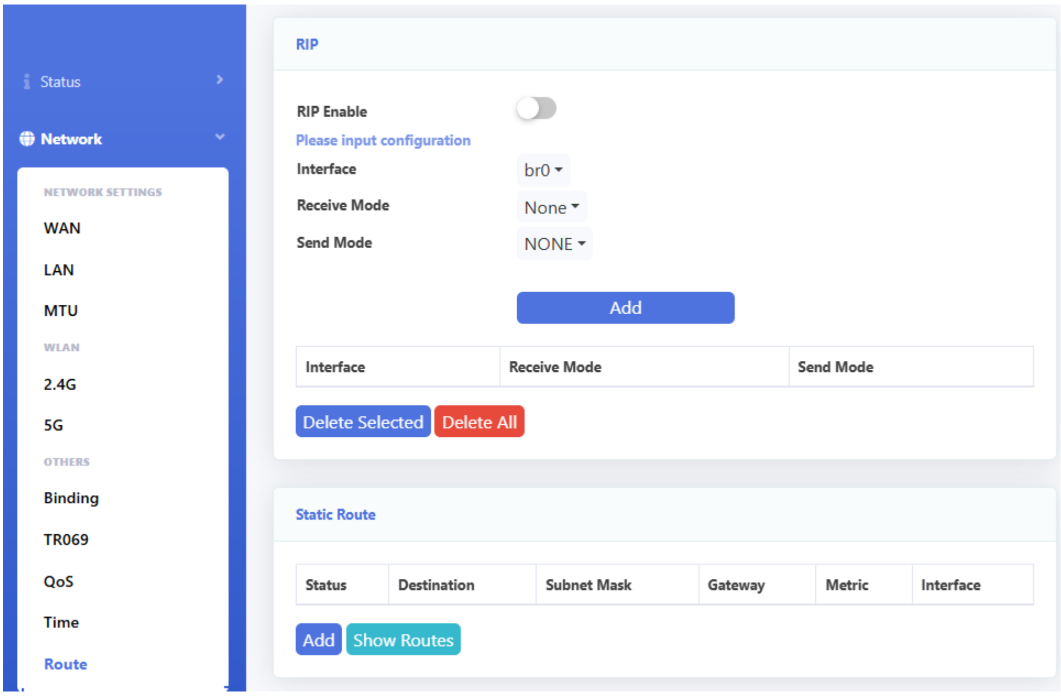
Sync with WAN:

Interval: 86400

Figure 3-3-35: Time server

3.3.10 Route

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



RIP

RIP Enable

Please input configuration

Interface br0

Receive Mode None

Send Mode NONE

Interface	Receive Mode	Send Mode

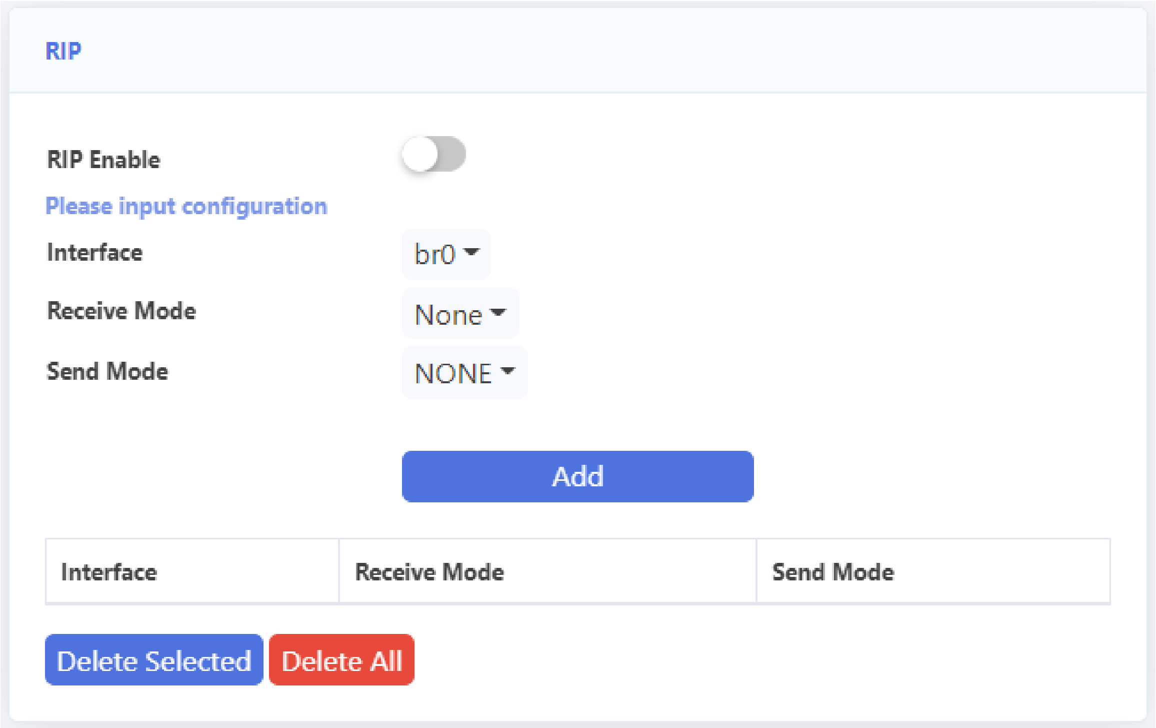
Static Route

Status	Destination	Subnet Mask	Gateway	Metric	Interface

Figure 3-3-36: Route

3.3.10.1 RIP Configuration

This page allows you to configure RIP function.



RIP

RIP Enable

Please input configuration

Interface br0

Receive Mode None

Send Mode NONE

Interface	Receive Mode	Send Mode

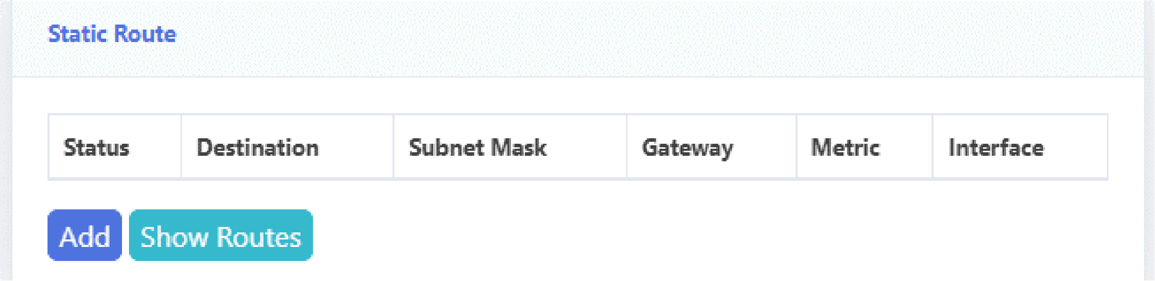
Figure 3-3-37: RIP configuration

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.

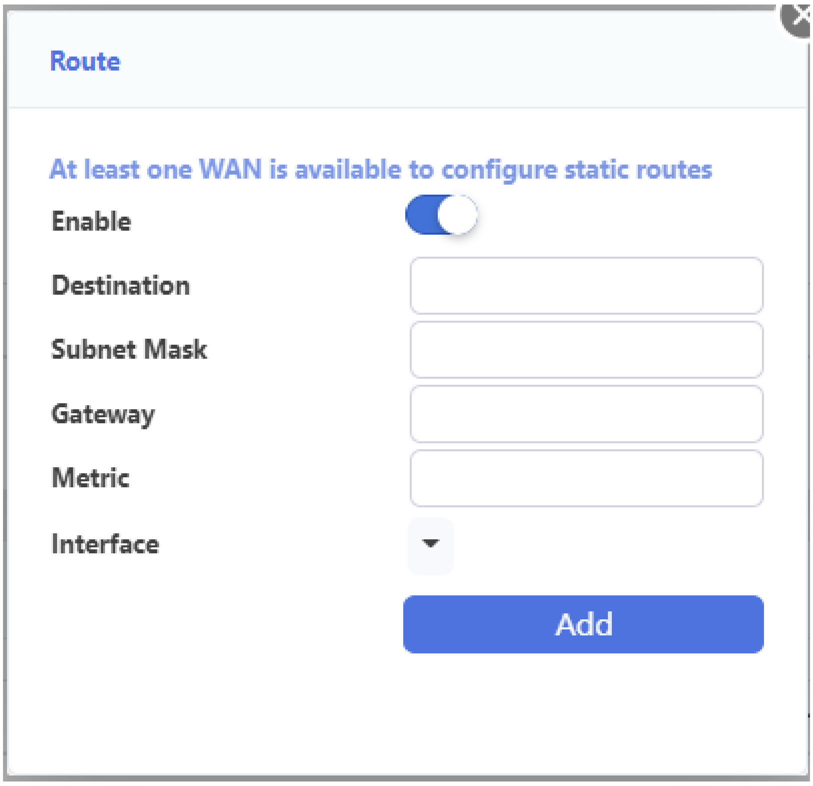
3.3.10.2 Static route

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


Static Route

Status	Destination	Subnet Mask	Gateway	Metric	Interface

Figure 3-3-38: Static route


Route

At least one WAN is available to configure static routes

Figure 3-3-39: 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.

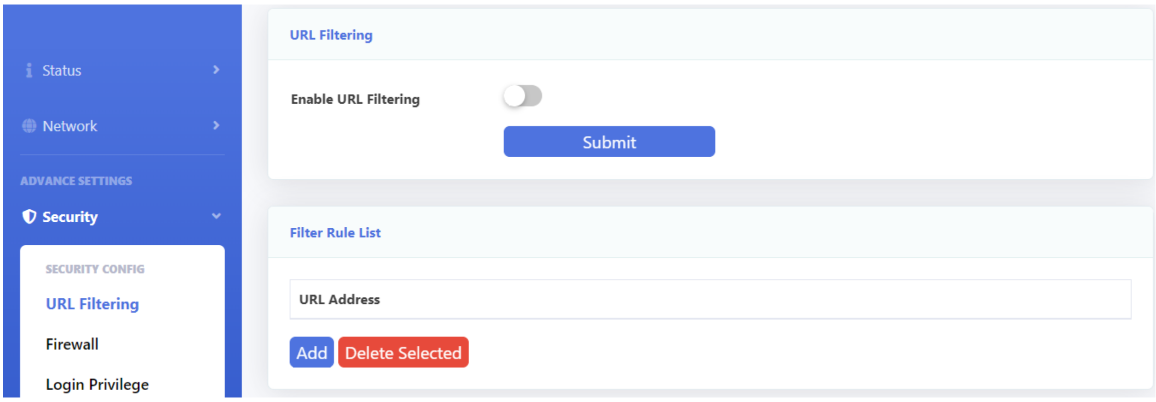
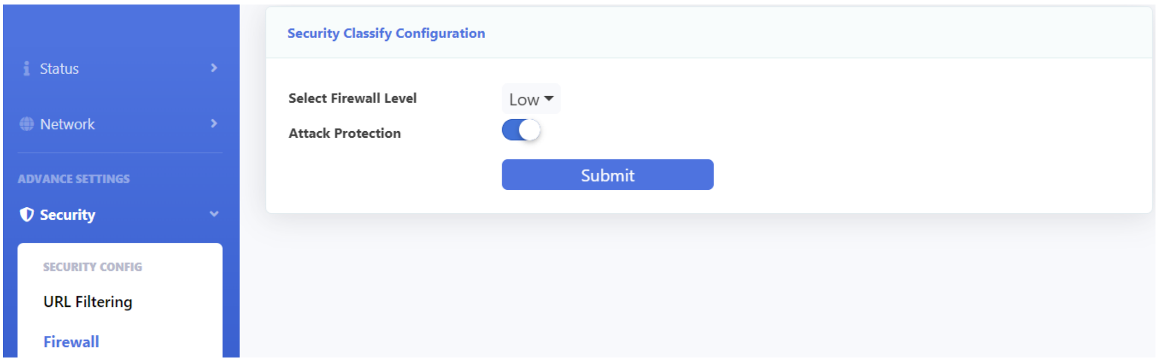


Figure 3-4-1: URL Filter

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.



Security Classify Configuration

Select Firewall Level: Low

Attack Protection: on

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.

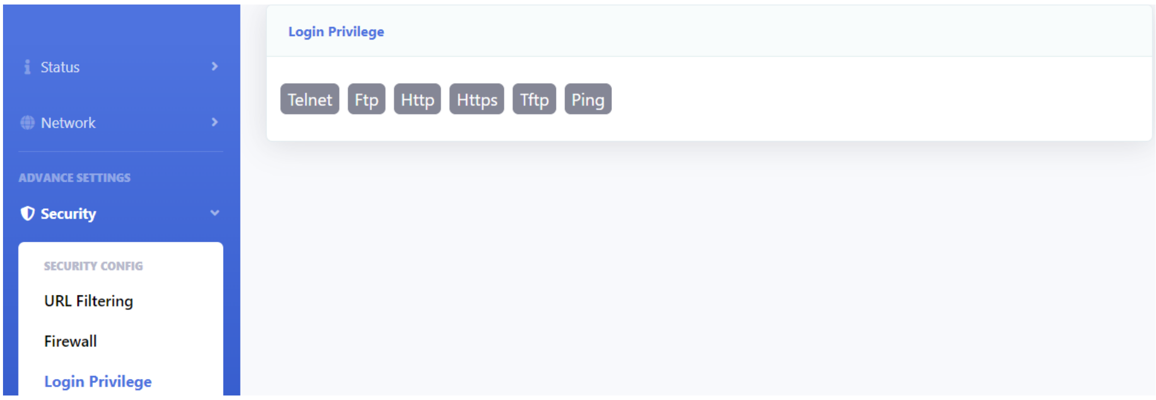
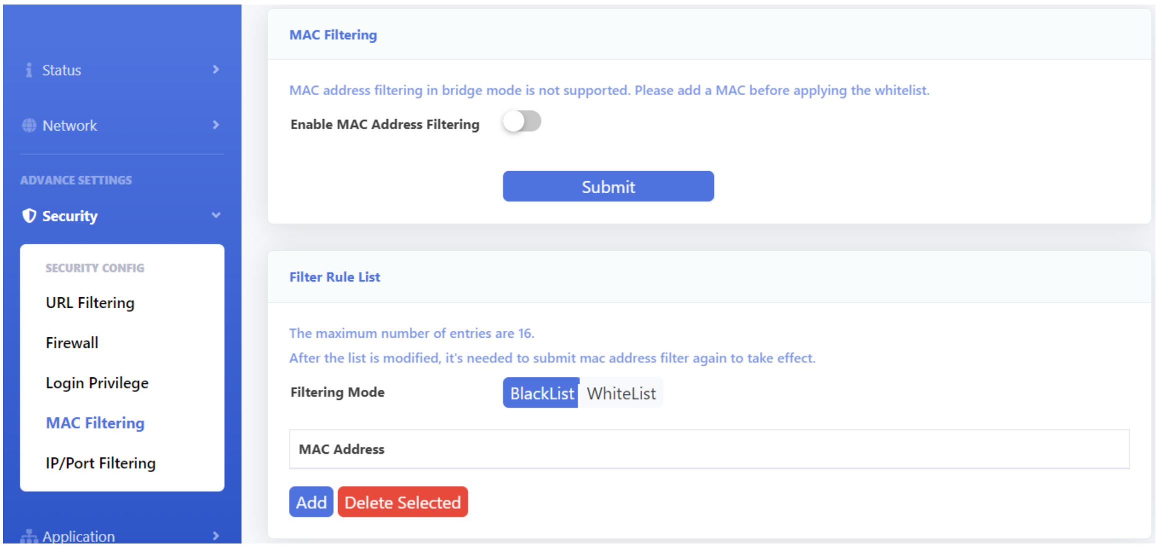


Figure 3-4-3: Login Privilege

3.4.4 MAC Filtering

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



MAC Filtering

MAC address filtering in bridge mode is not supported. Please add a MAC before applying the whitelist.

Enable MAC Address Filtering ○

Filter Rule List

The maximum number of entries are 16.

After the list is modified, it's needed to submit mac address filter again to take effect.

Filtering Mode: BlackList

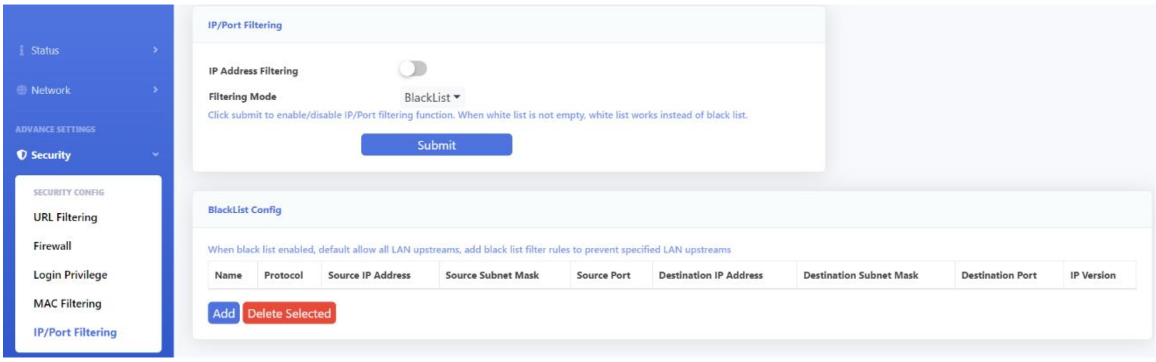
MAC Address

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.



IP/Port Filtering

IP Address Filtering ○

Filtering Mode: BlackList

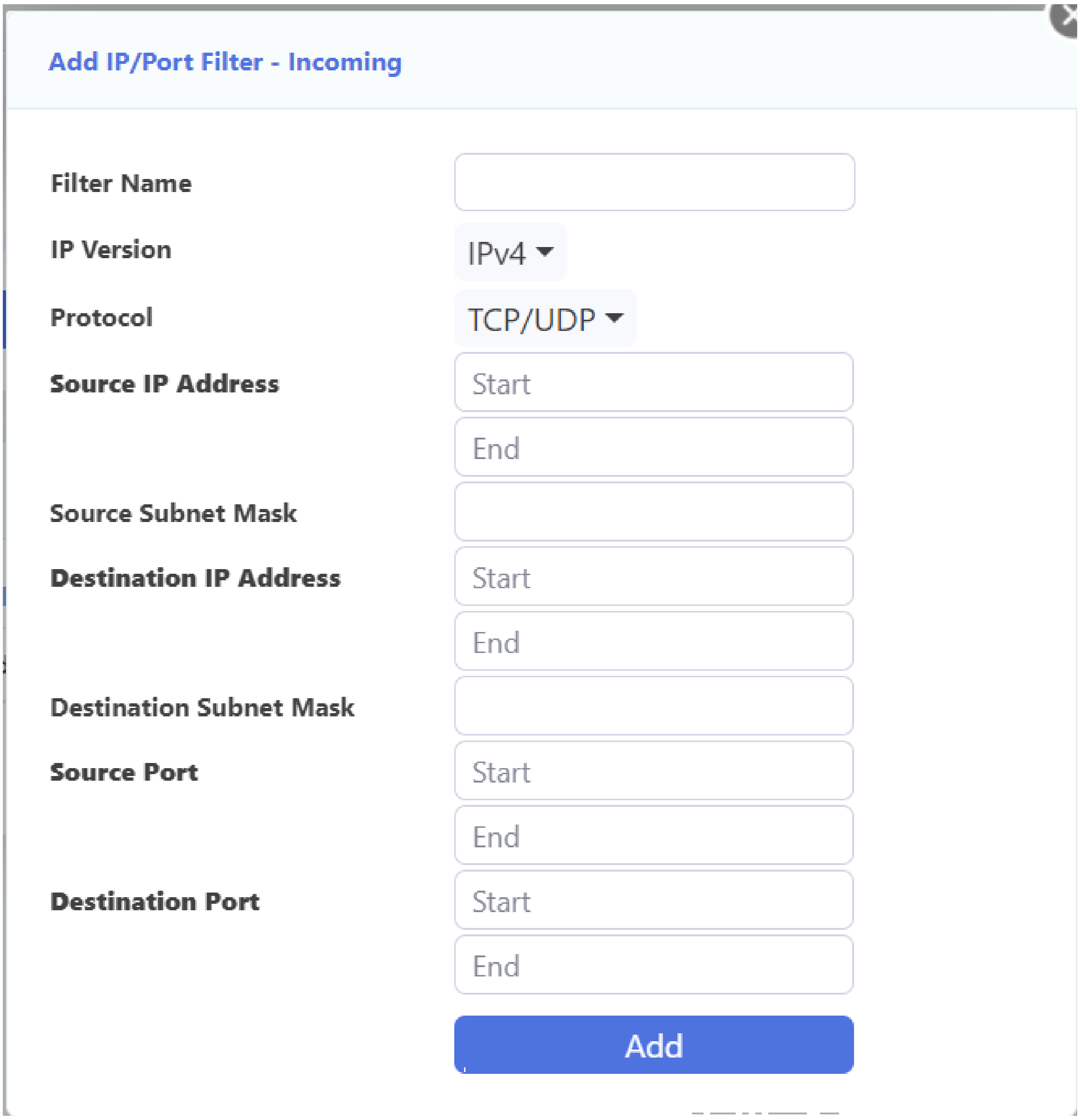
Click submit to enable/disable IP/Port filtering function. When white list is not empty, white list works instead of black list.

BlackList Config

When black list enabled, default allow all LAN upstreams, add black list filter rules to prevent specified LAN upstreams

Name	Protocol	Source IP Address	Source Subnet Mask	Source Port	Destination IP Address	Destination Subnet Mask	Destination Port	IP Version

Figure 3-4-5: Ip / Port Filter



Add IP/Port Filter - Incoming

Filter Name

IP Version: IPv4

Protocol: TCP/UDP

Source IP Address: Start / End

Source Subnet Mask

Destination IP Address: Start / End

Destination Subnet Mask

Source Port: Start / End

Destination Port: Start / End

Figure 3-4-6: Port Filter -Incoming

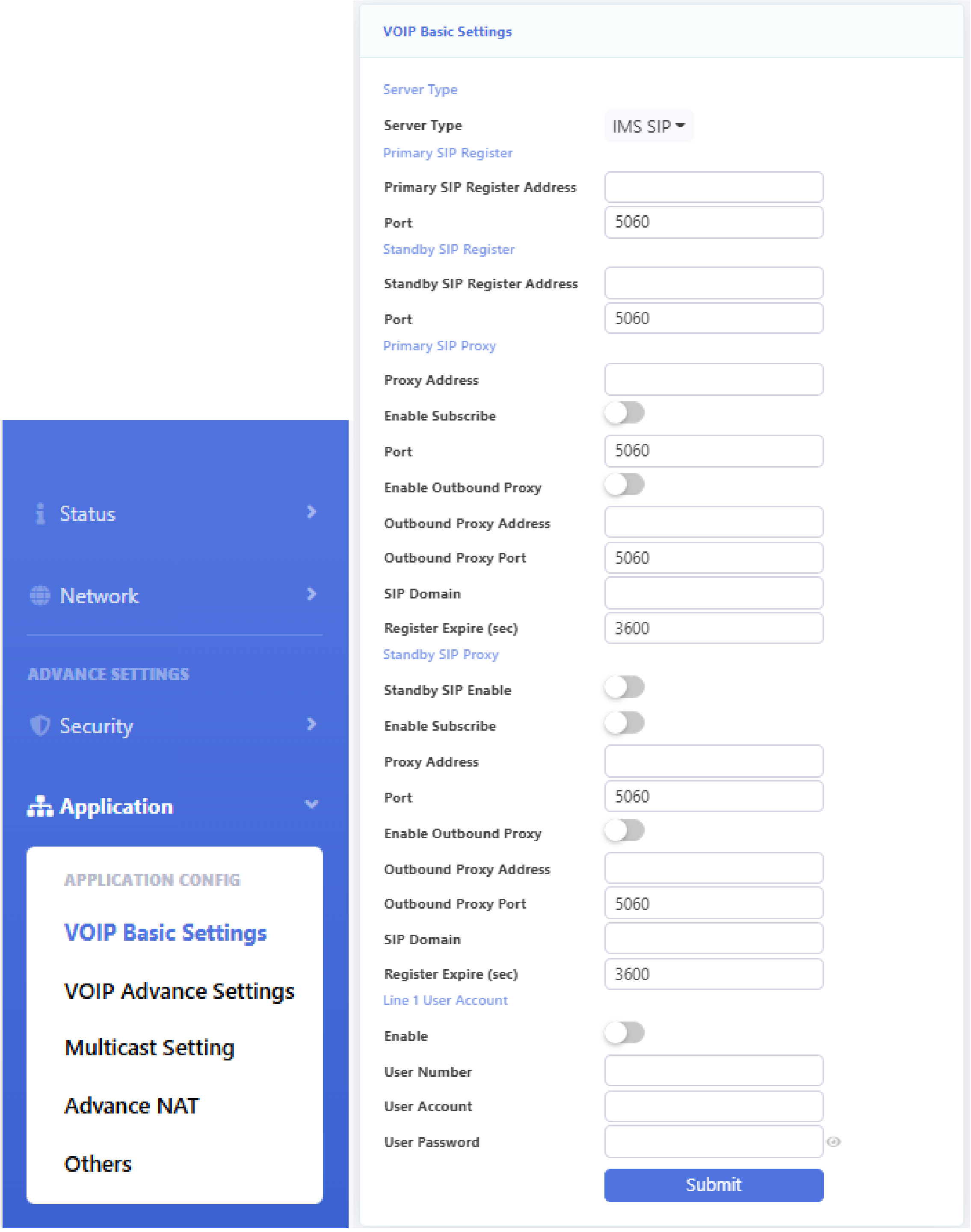
Parameter	Illustration
IP Address Filtering	Switch of IP/port filtering.
Filter Mode	Black List: Rule in the list will be forbidden and others will be accessed. White List: Rule in the list will be accessed and others will be forbidden.
Filter Rule Settings	
Filter Name	Input filter name.
IP Version	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 VoIP Basic Settings

This page allows you to do VoIP basic configurations.



VOIP Basic Settings

Server Type

Server Type	IMS SIP

Primary SIP Register

Primary SIP Register Address	
Port	5060

Standby SIP Register

Standby SIP Register Address	
Port	5060

Primary SIP Proxy

Proxy Address	
Enable Subscribe	○
Port	5060
Enable Outbound Proxy	○
Outbound Proxy Address	
Outbound Proxy Port	5060
SIP Domain	
Register Expire (sec)	3600

Standby SIP Proxy

Standby SIP Enable	○
Enable Subscribe	○
Proxy Address	
Port	5060
Enable Outbound Proxy	○
Outbound Proxy Address	
Outbound Proxy Port	5060
SIP Domain	
Register Expire (sec)	3600

Line 1 User Account

Enable	○
User Number	
User Account	
User Password	

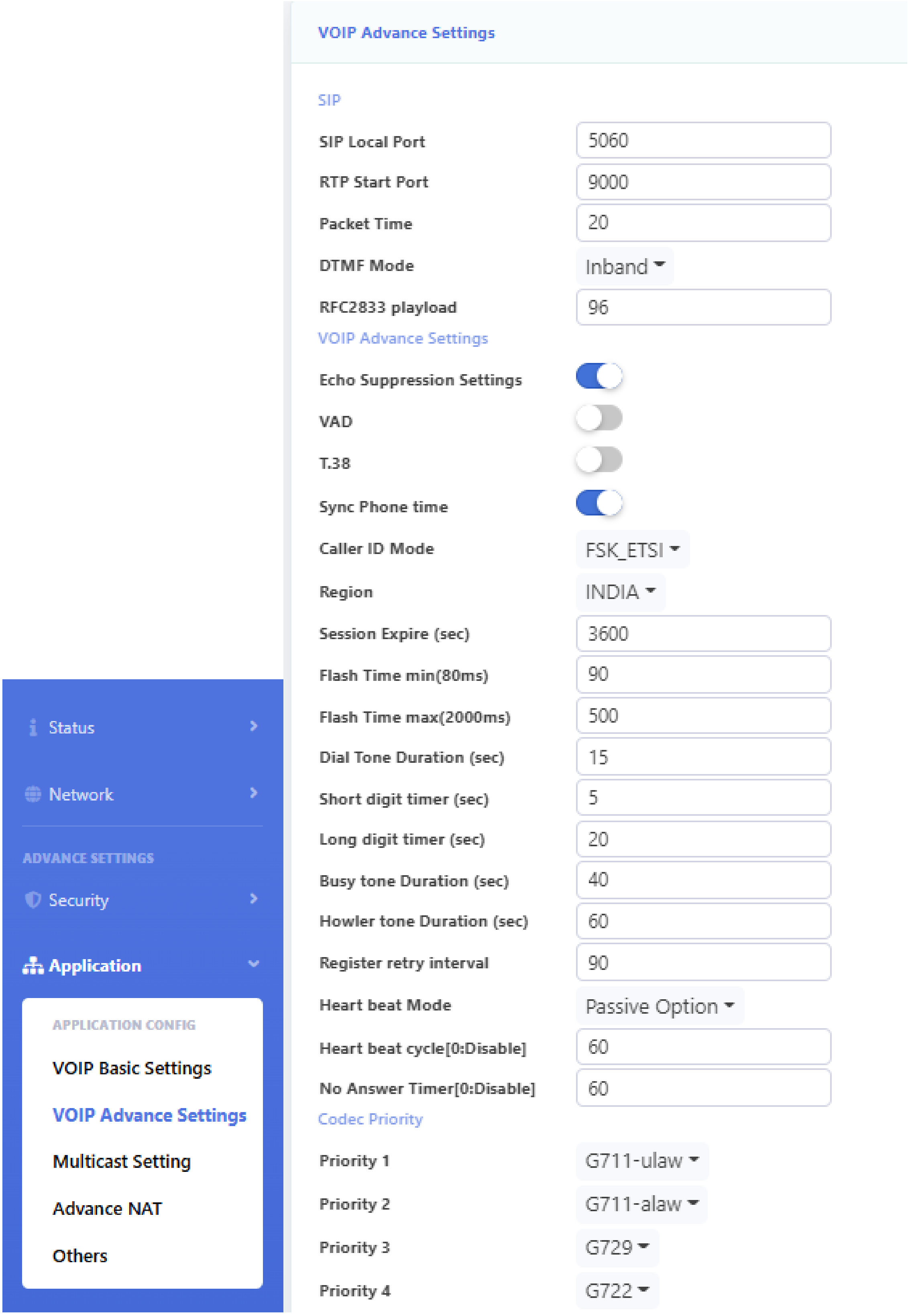
Figure 3-5-1: VoIP Basic Configuration

Parameter	Illustration
Server Type	SIP server type, soft switch and IMS.
Primary SIP Register Address	Primary SIP register server address.
Standby SIP Register Address	Secondary SIP register address.
Port	The port of SIP protocol, default port is 5060.
Primary SIP Proxy	Primary SIP proxy server IP address.
Enable Subscribe	To enable subscribe.
Enable Outbound Proxy	To enable outbound proxy.
Outbound Proxy Address	Outbound proxy server IP address.
SIP Domain	Primary SIP proxy server domain.
Register Expire	Register expire of SIP account.
Standby SIP Enable	To enable standby SIP proxy.
Enable	Enable: Enable VoIP function. Disable: Disable VoIP function.
User Number	Enter phone number as it should appear on caller ID.
User Account	Enter the registration ID of the user with the registrar.
User Password	Enter the password used for authentication with the registrar.

For VOIP WAN connection, service mode must contain VOIP.

3.5.2 VoIP Advance Settings

This page shows advanced VoIP settings, including SDP parameters and additional services.



VOIP Advance Settings

SIP

SIP Local Port	5060
RTP Start Port	9000
Packet Time	20
DTMF Mode	Inband ▾
RFC2833 playload	96

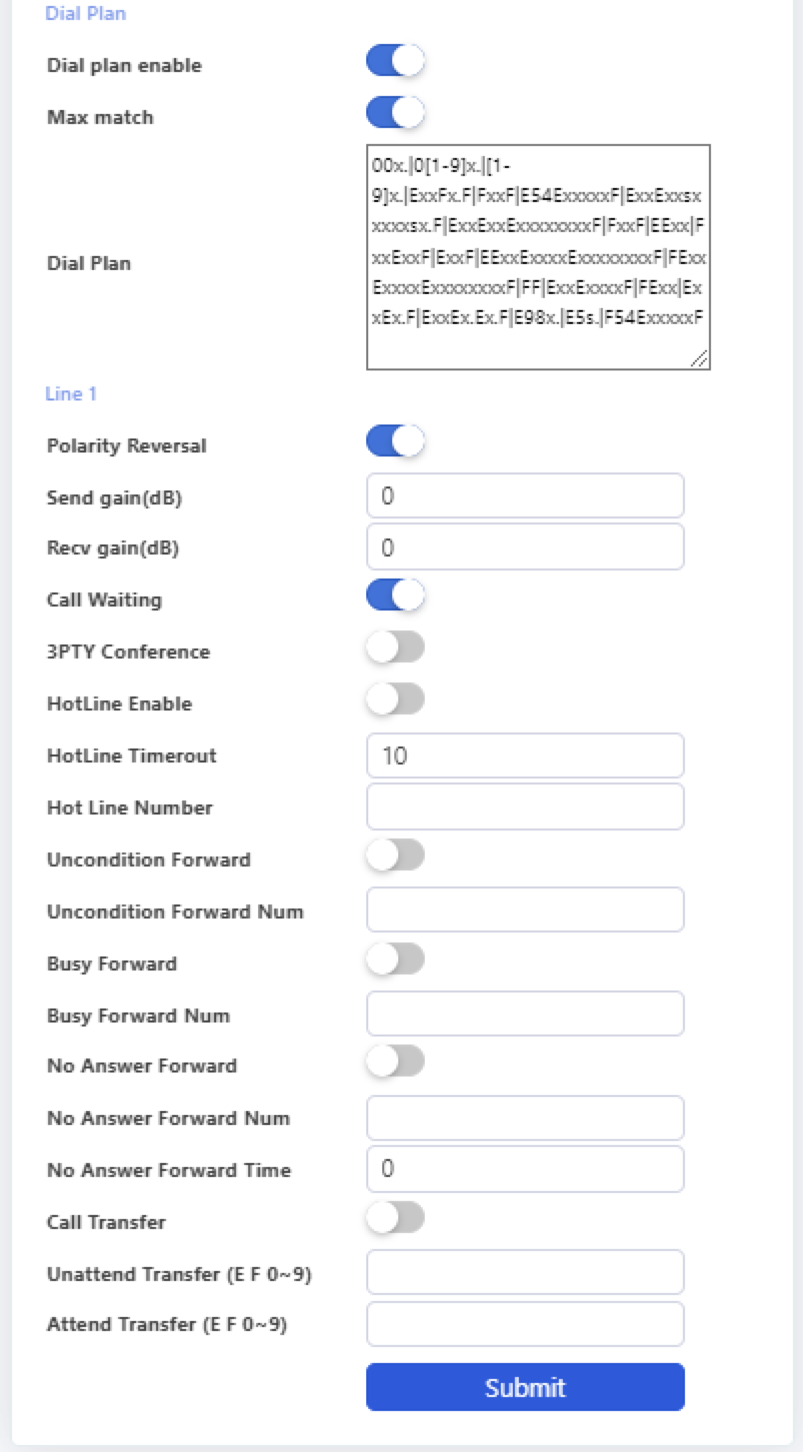
VOIP Advance Settings

Echo Suppression Settings	●
VAD	○
T.38	○
Sync Phone time	●
Caller ID Mode	FSK_ETSI ▾
Region	INDIA ▾
Session Expire (sec)	3600
Flash Time min(80ms)	90
Flash Time max(2000ms)	500
Dial Tone Duration (sec)	15
Short digit timer (sec)	5
Long digit timer (sec)	20
Busy tone Duration (sec)	40
Howler tone Duration (sec)	60
Register retry interval	90
Heart beat Mode	Passive Option ▾
Heart beat cycle[0:Disable]	60
No Answer Timer[0:Disable]	60

Codec Priority

Priority 1	G711-ulaw ▾
Priority 2	G711-alaw ▾
Priority 3	G729 ▾
Priority 4	G722 ▾

Figure 3-5-2-a: VoIP Advance Settings



Dial Plan

Dial plan enable	●
Max match	●
Dial Plan	00x.|0[1-9]x.|[1-9]x.|ExxFx.F|FxxF|E54ExxxxxF|ExxExxsxxxxxsx.F|ExxExxExxxxxxxxF|FxxF|EExx|FxxExxF|ExxF|EExxExxxxExxxxxxxxF|FExxExxxxExxxxxxxxF|FF|ExxExxxxF|FExx|ExxEx.F|ExxEx.Ex.F|E98x.|E5s.|F54ExxxxxF

Line 1

Polarity Reversal	●
Send gain(dB)	0
Recv gain(dB)	0
Call Waiting	●
3PTY Conference	○
HotLine Enable	○
HotLine Timerout	10
Hot Line Number	
Uncondition Forward	○
Uncondition Forward Num	
Busy Forward	○
Busy Forward Num	
No Answer Forward	○
No Answer Forward Num	
No Answer Forward Time	0
Call Transfer	○
Unattend Transfer (E F 0~9)	
Attend Transfer (E F 0~9)	

Figure 3-5-2-b: VoIP Advance Settings

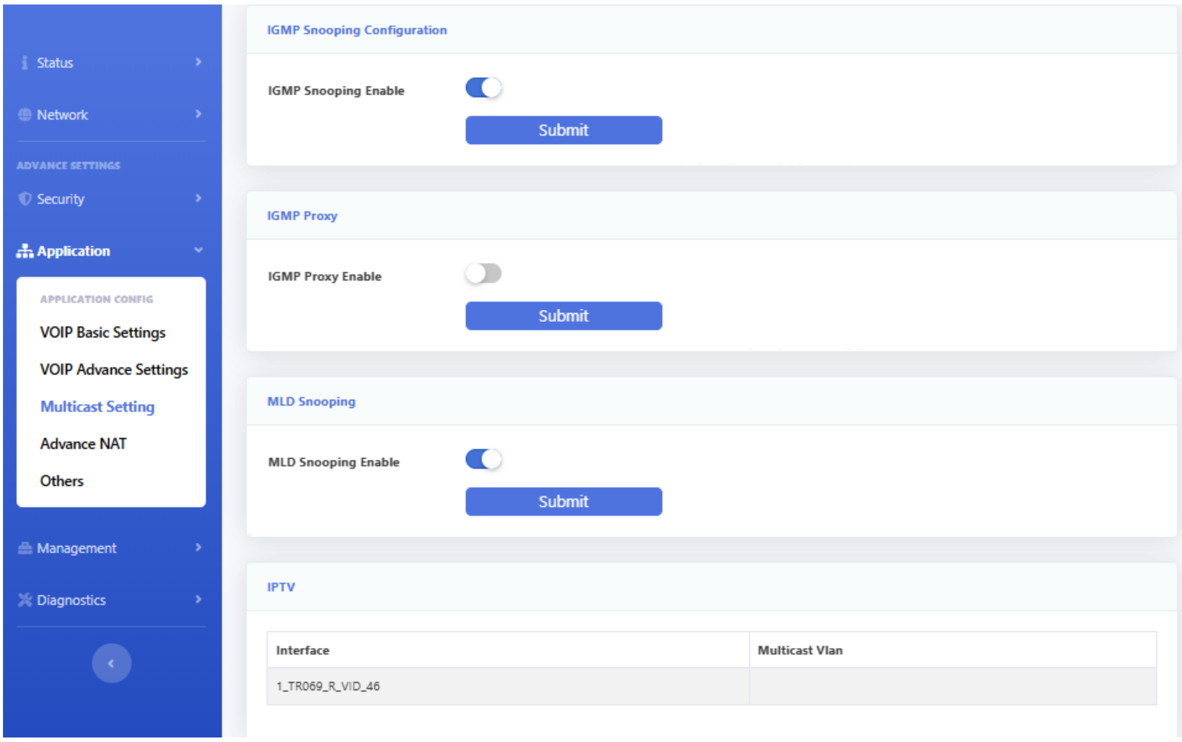
Parameter	Illustration
SIP Local Port	Set local port of SIP messages.
RTP Start Port	Set beginning port of RTP messages.
Packet Time	Set packet time of RTP messages, in millisecond.
DTMF Mode	Set DTMF mode.
RFC2833 Payload	Set the value of payload for RFC2833 mode.

Echo Suppression Settings	Enable or disable echo suppression function.
VAD	Enable or disable voice activation detection function.
T.38	Enable or disable T.38 fax mode.
Sync Phone time	Enable or disable sync phone time
Caller ID mode	Set caller ID mode.
Region	Set tone of country. Different country or region may use different tone.
Session Expire	Set session expire time.
Flash Time	Set flash time of phone.
Dial Tone Duration	Set the off-hook dialing expire time, default value is 10. (range: 10s~20s).
Short Digit Timer	Set the short digit timer value, default value is 5. (range: 4s~30s).
Long Digit Timer	Set the long digit timer value, default value is 5. (range: 4s~30s).
Busy tone Duration	Set the busy tone time, default value is 40. (range: 30s~180s).
Howler tone Duration	Set the howler tone time, default value is 60. (range: 30s~180s).
Register retry interval	Set register failed and retry interval.
Heart beat mode	Set heartbeat mode.
Heart beat cycle	Set heartbeat cycle.
No Answer Timer	Set no answer ring time. 0 means no time limit.
Codec Priority	The parameter set the ITU-T coding standard of the voice. The coding technology supported by this equipment is G.711 A law, G.711 Mu law and G.729 and so on. Users can choose one or several coding mode, but one of those modes must be chosen as the priority.
Dial plan enable	Enable or disable dial plan.
Max match	Enable or disable max match of dial plan.
Dial Plan	Set dial rule of device.
Polarity Reversal	Enable or disable polarity reversal function.
Send gain	Set codec send gain.
Recv gain	Ser codec receive gain.
Call waiting	Enable or disable call waiting.
3PTY Conference	Enable or disable 3PTY conference.
HotLine Enable	Enable or disable hotline function.
HotLine Timerout	Set hotline timeout.
HotLine Number	Set hotline number.
Uncondition Forward	Enable or disable un-condition forward.
Uncondition Forward Num	Set un-condition forward number.

Busy Forward	Enable or disable busy forward.
Busy Forward Num	Set busy forward number.
No Answer Forward	Enable or disable no answer forward.
No Answer Forward Num	Set no answer forward number.
No Answer Forward Time	Set no answer forward time.
Call transfer	Enable or disable call transfer function.
Unattend Transfer	Set unattend transfer number.
Attend Transfer	Set attend transfer number.

3.5.3 Multicast Setting

This page allows you to configure multicast-related parameter.



IGMP Snooping Configuration

IGMP Snooping Enable: on

IGMP Proxy

IGMP Proxy Enable: off

MLD Snooping

MLD Snooping Enable: on

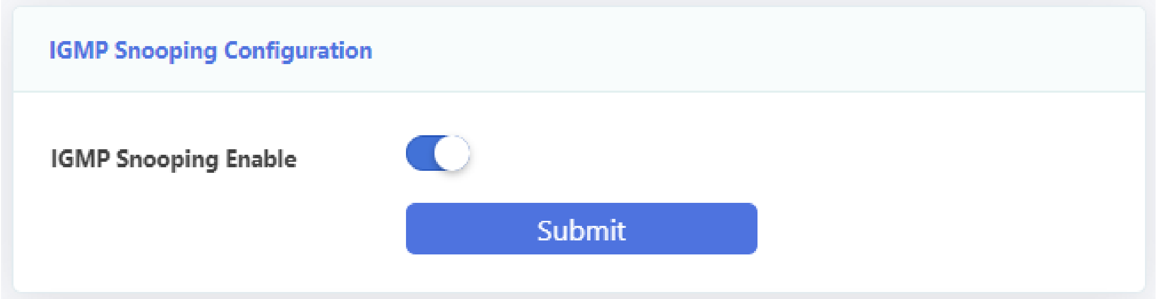
IPTV

Interface	Multicast Vlan
1_TR069_R_VID_46	

Figure 3-5-3: Multicast Setting

3.5.3.1 IGMP Snooping Configuration

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

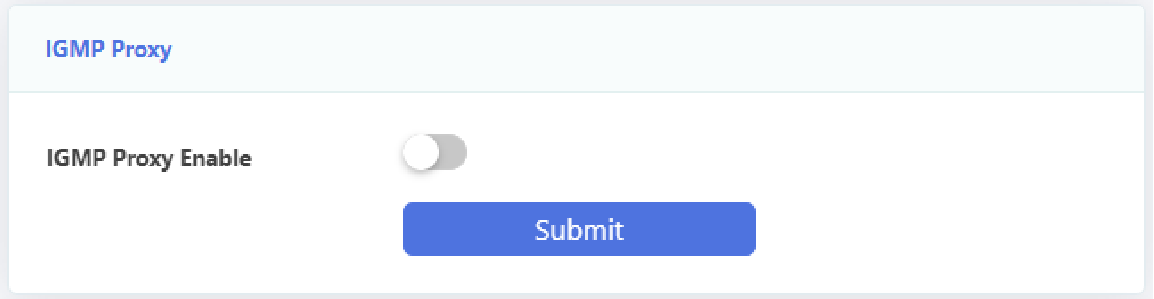


IGMP Snooping Configuration

Figure 3-5-4: IGMP Snooping

3.5.3.2 IGMP Proxy

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

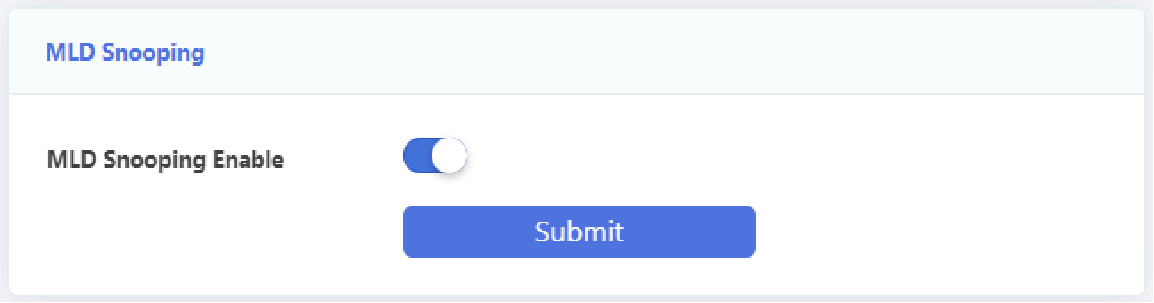


IGMP Proxy

Figure 3-5-5: IGMP Proxy

3.5.3.3 MLD Snooping

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

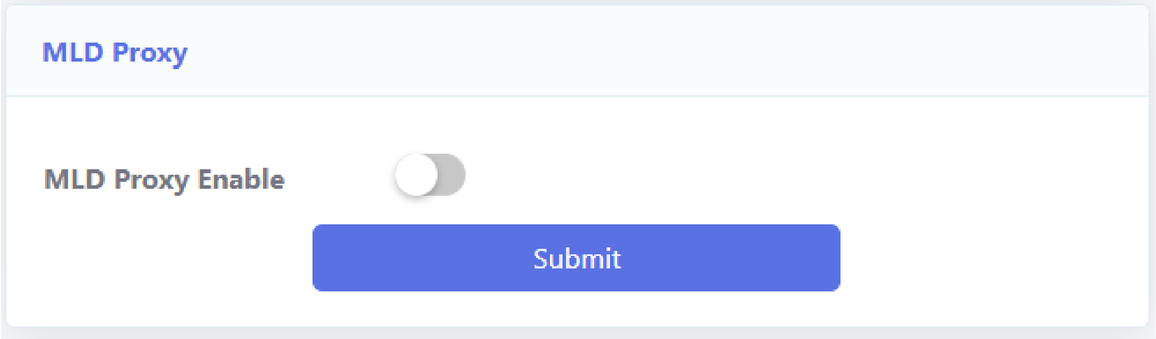


MLD Snooping

Figure 3-5-6: MLD Snooping

3.5.3.4 MLD Proxy

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



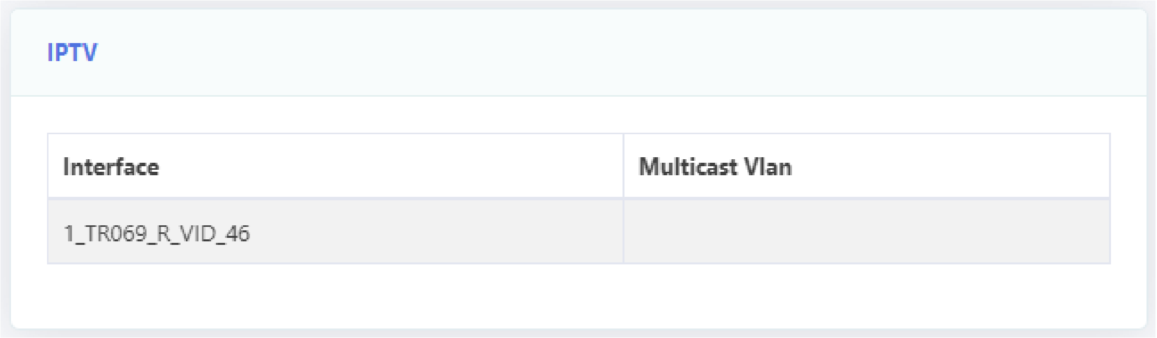
MLD Proxy

MLD Proxy Enable

Figure 3-5-7: MLD Proxy

3.5.3.5 IPTV

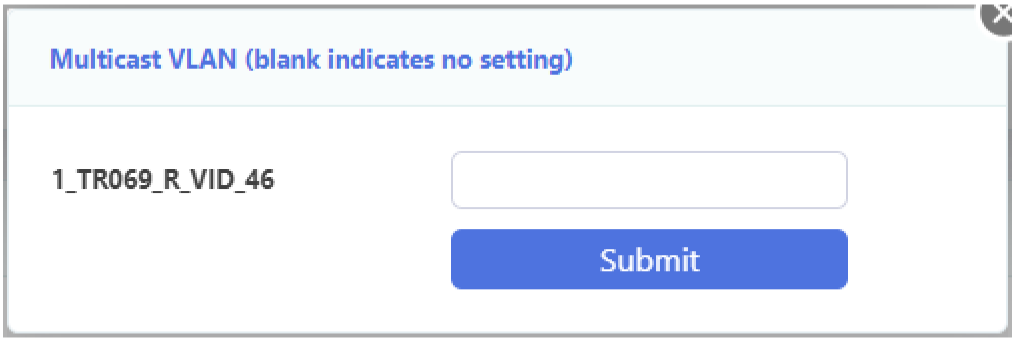
This page allows you to configure multicast VLAN for WAN connections. Click the corresponding WAN name to add VLAN.



IPTV

Interface	Multicast Vlan
1_TR069_R_VID_46	

Figure 3-5-8:IPTV



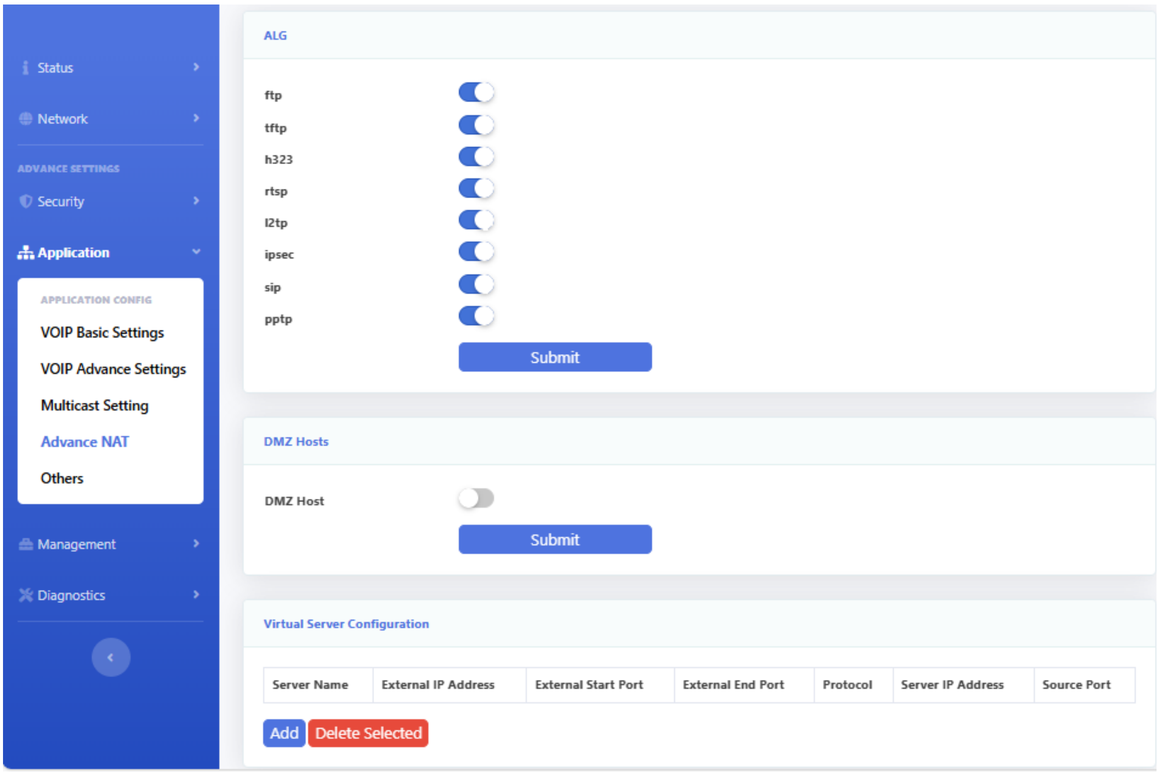
Multicast VLAN (blank indicates no setting)

1_TR069_R_VID_46

Figure 3-5-9: Multicast VLAN

3.5.4 Advance NAT

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



ALG

ftp
tftp
h323
rtsp
l2tp
ipsec
sip
pptp

DMZ Hosts

DMZ Host

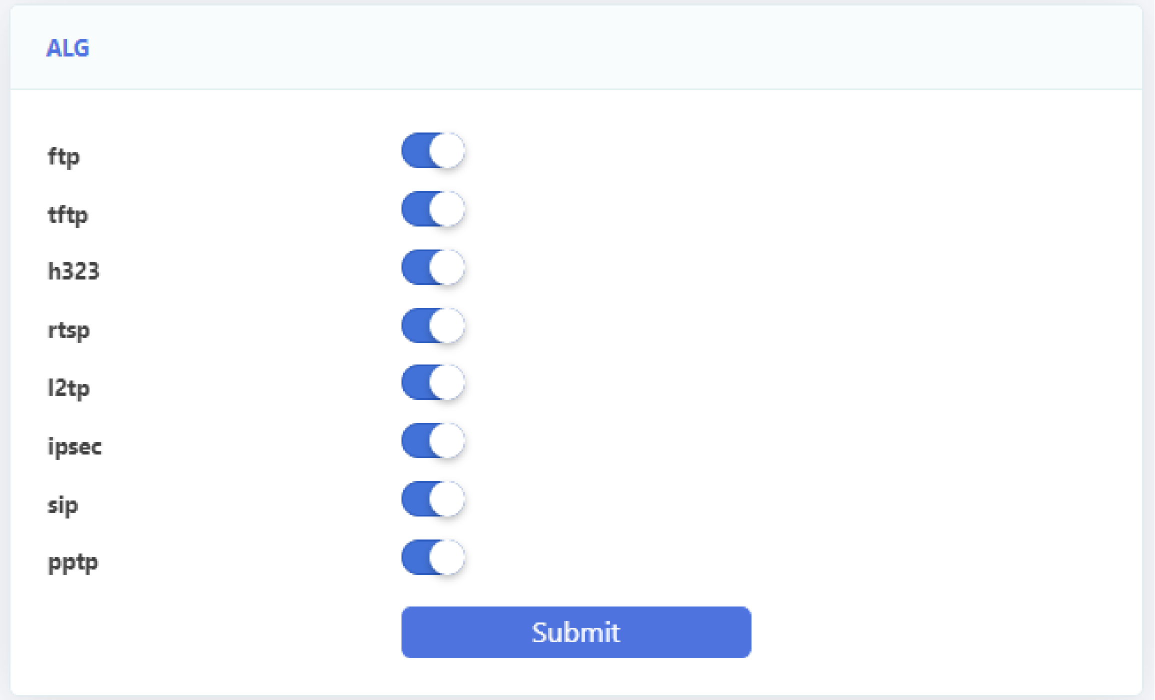
Virtual Server Configuration

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

Figure 3-5-10: Advance NAT

3.5.4.1 ALG

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



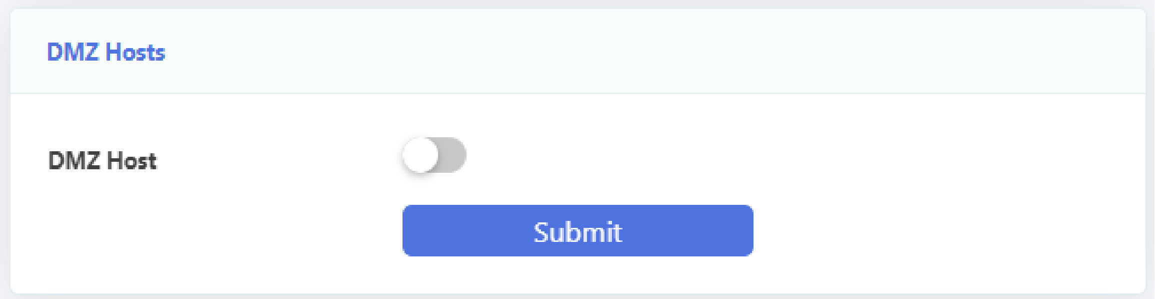
ALG

ftp
tftp
h323
rtsp
l2tp
ipsec
sip
pptp

Figure 3-5-11: ALG configuration

3.5.4.2 DMZ Hosts

This page allows you to configure DMZ server.



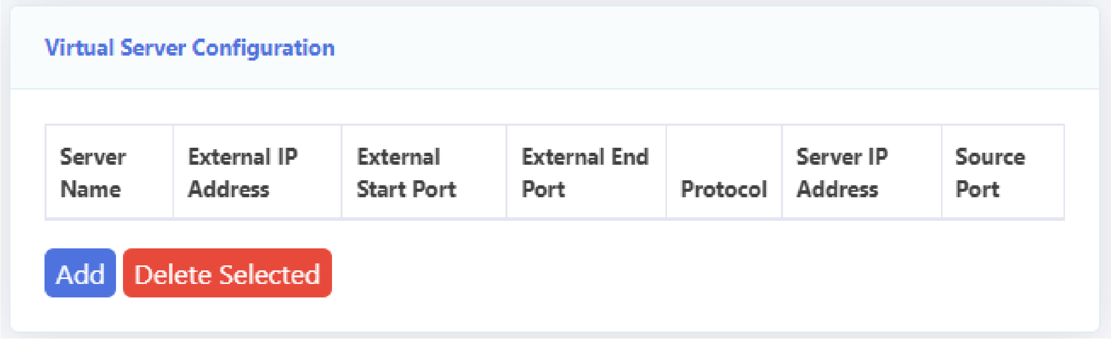
DMZ Hosts

DMZ Host ○

Figure 3-5-12: DMZ configuration

3.5.4.3 Virtual Server Configuration

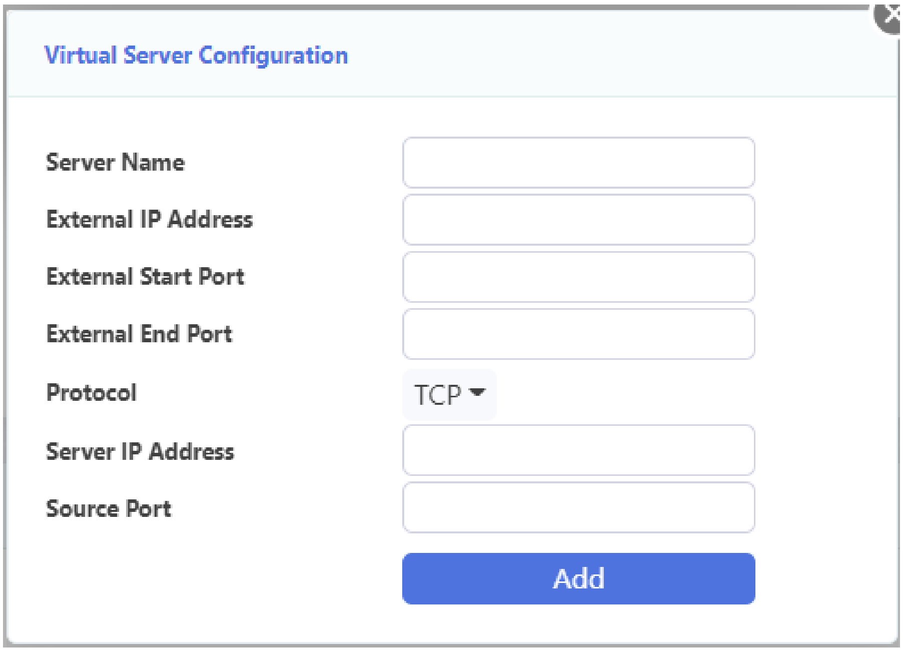
This page allows you to configure virtual server. After you click the "Add" button, you will see the configuration page.



Virtual Server Configuration

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

Figure 3-5-13: Add Virtual Server



Virtual Server Configuration

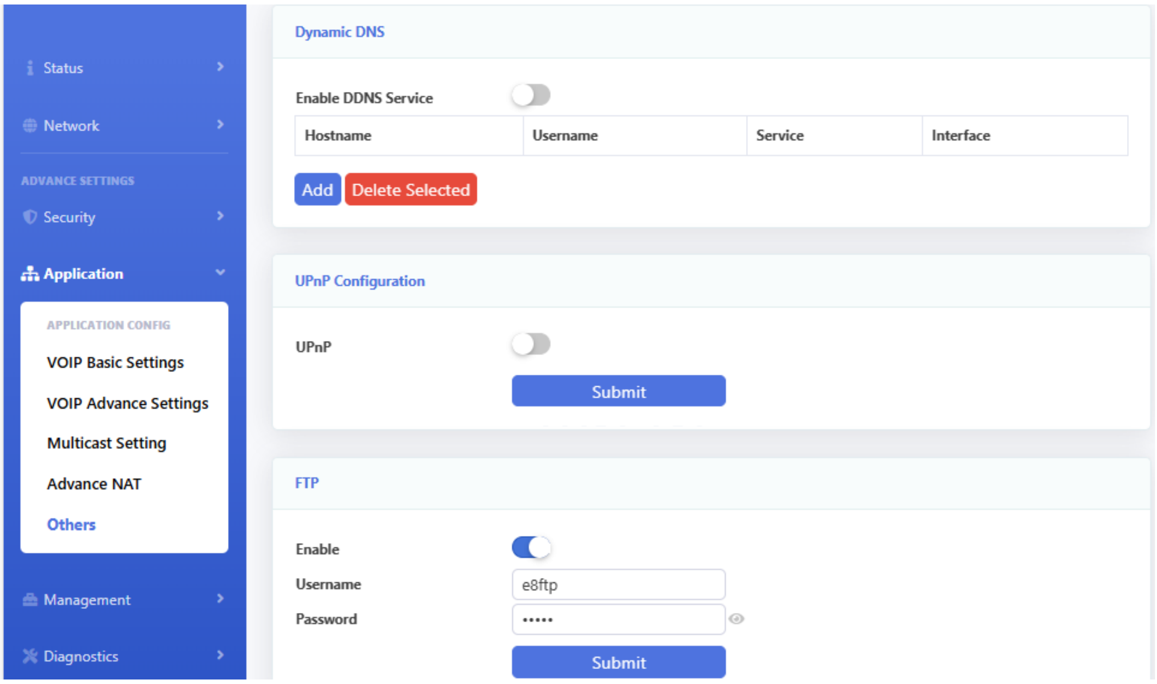
Server Name	
External IP Address	
External Start Port	
External End Port	
Protocol	TCP
Server IP Address	
Source Port	

Figure 3-5-14: Virtual Server configuration

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

3.5.5 Others

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



Dynamic DNS

Enable DDNS Service

Hostname	Username	Service	Interface

UPnP Configuration

UPnP

FTP

Enable

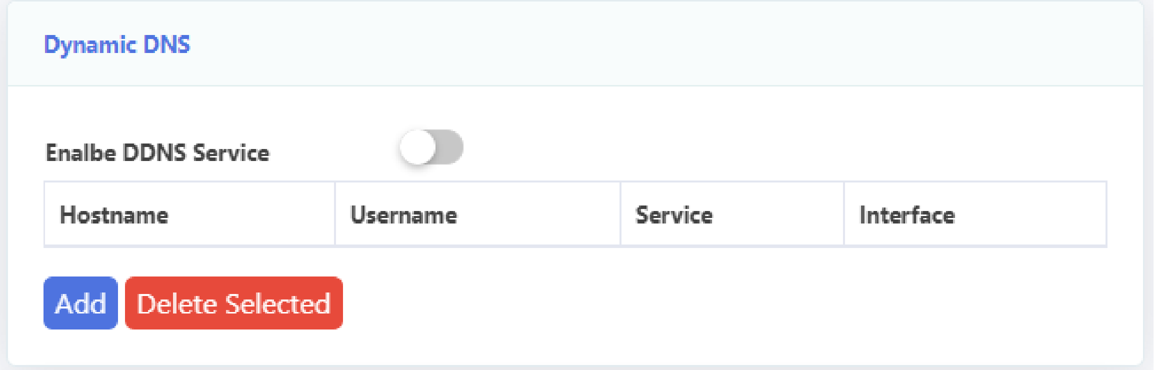
Username e8ftp

Password •••••

Figure 3-5-15: Other

3.5.5.1 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.

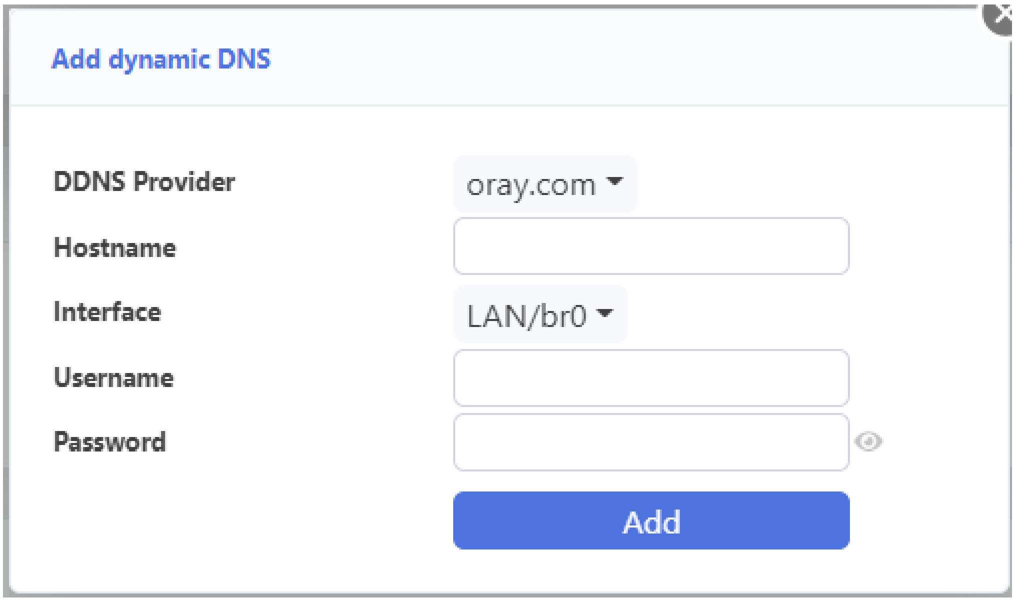


Dynamic DNS

Enalbe DDNS Service

Hostname	Username	Service	Interface

Figure 3-5-16: Add DDNS



Add dynamic DNS

DDNS Provider: oray.com

Hostname:

Interface: LAN/br0

Username:

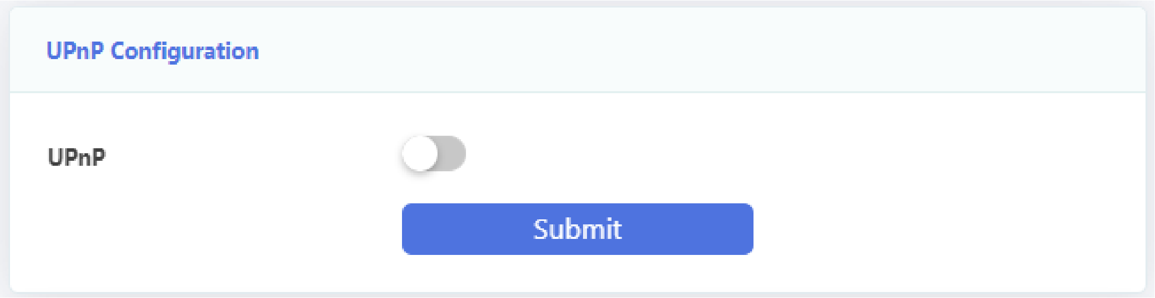
Password:

Figure 3-5-17: 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.

3.5.5.2 UPNP Configuration

This page is used to configure UPNP.



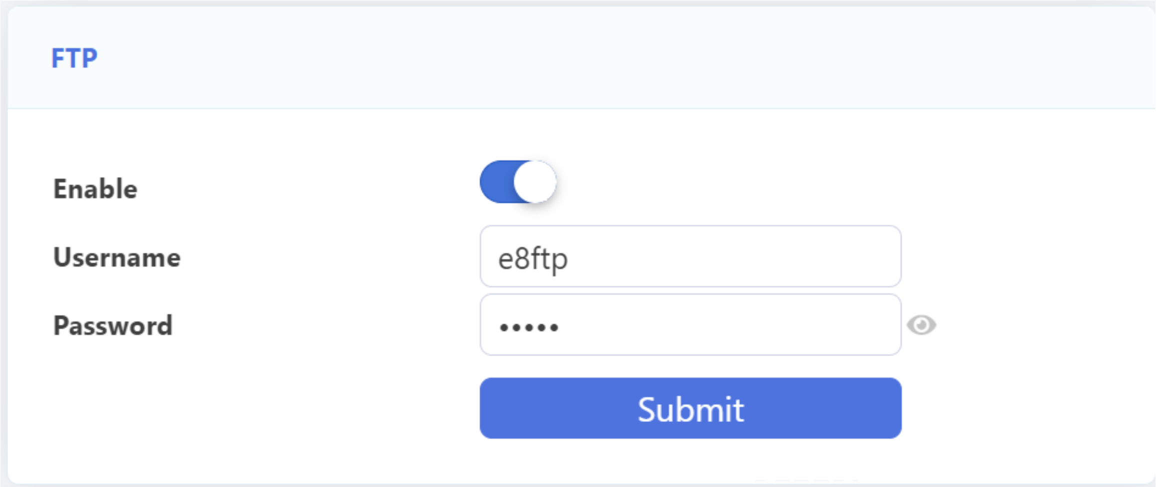
UPnP Configuration

UPnP: ○ off

Figure 3-5-18: UPNP configuration

3.5.5.3 FTP

This page is used to configure FTP.



FTP

Enable: ●

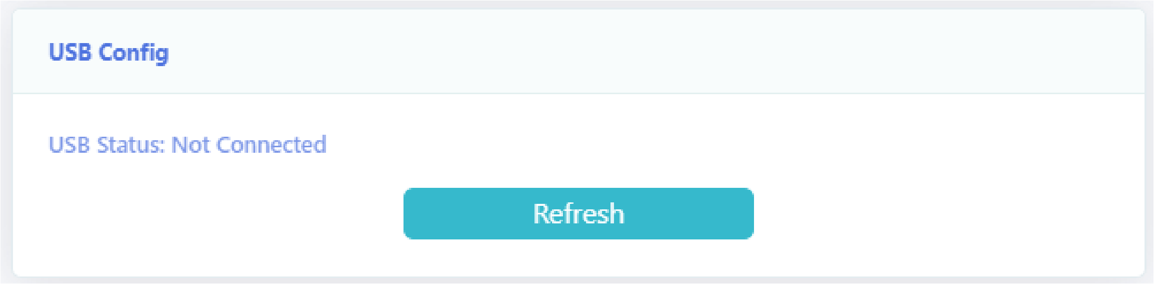
Username: e8ftp

Password: •••••

Figure 3-5-19: FTP configuration

3.5.5.4 USB Config

This page is used to configure USB.



USB Config

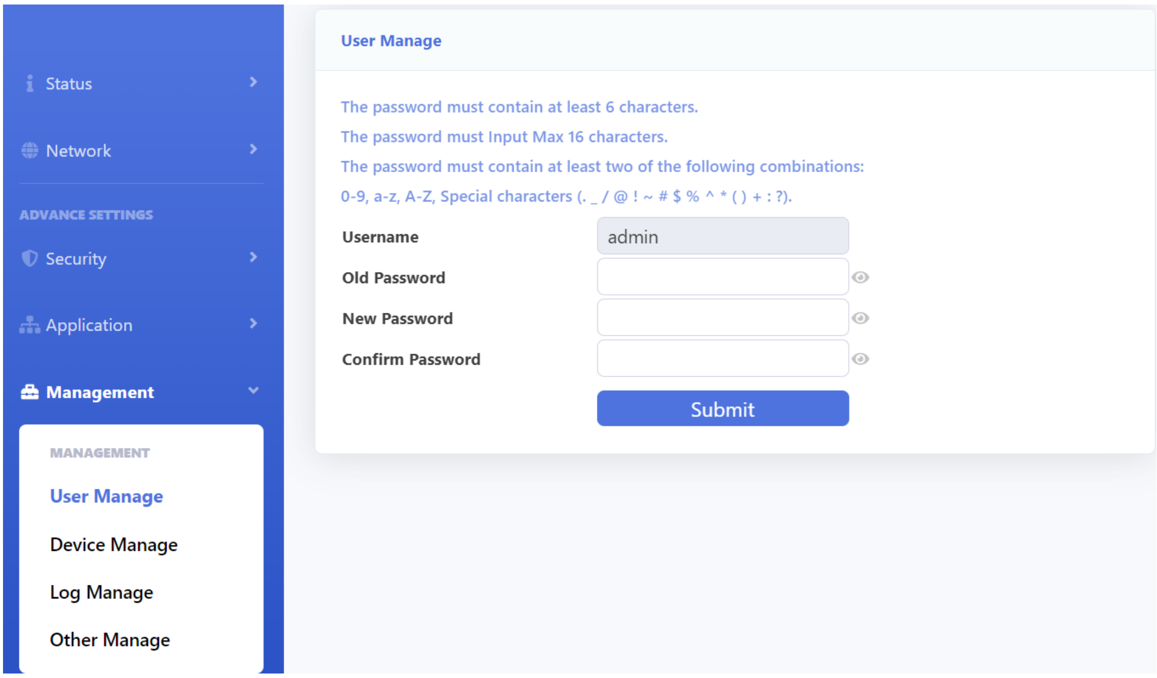
USB Status: Not Connected

Figure 3-5-20: USB configuration

3.6 Management

3.6.1 User Manage

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



User Manage

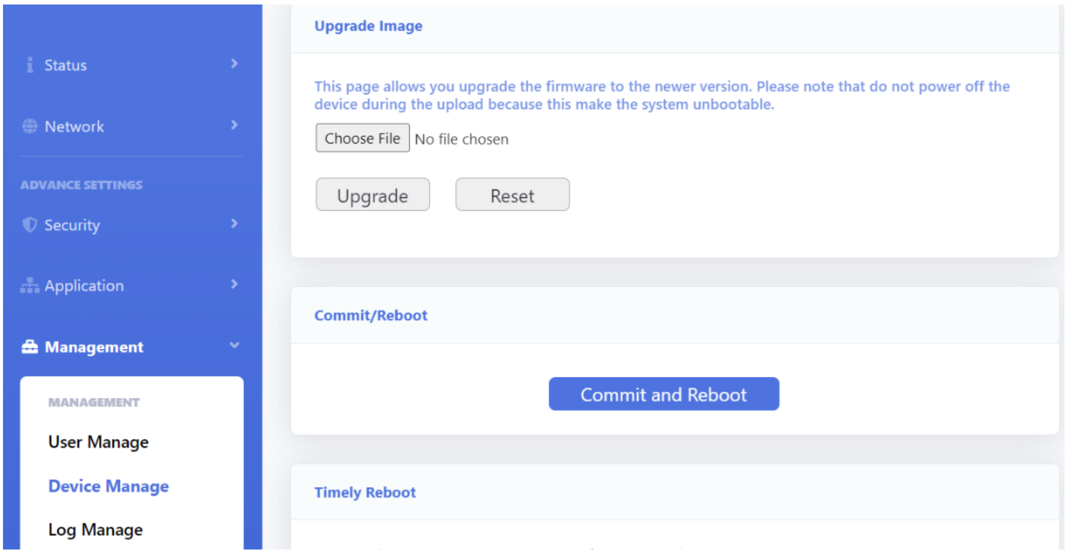
The password must contain at least 6 characters.
The password must Input Max 16 characters.
The password must contain at least two of the following combinations:
0-9, a-z, A-Z, Special characters (. _ / @ ! ~ # $ % ^ * ( ) + : ?).

Username: admin
Old Password:
New Password:
Confirm Password:

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



Upgrade Image

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

No file chosen

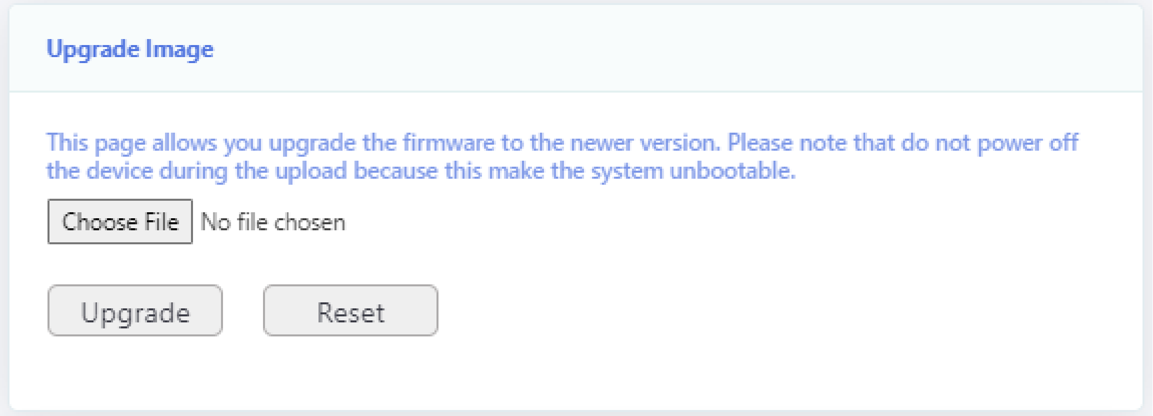
Commit/Reboot

Timely Reboot

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.



Upgrade Image

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

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.

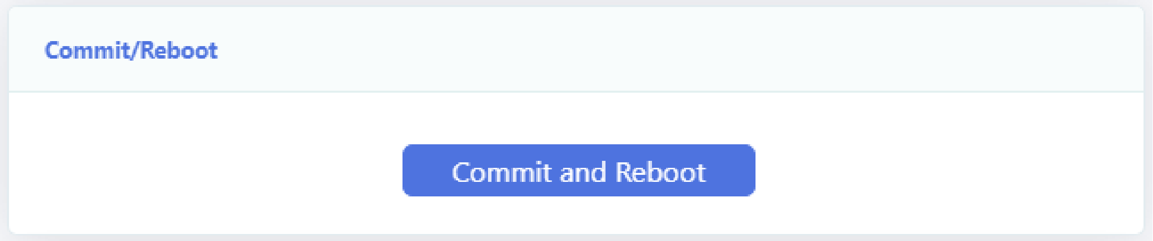
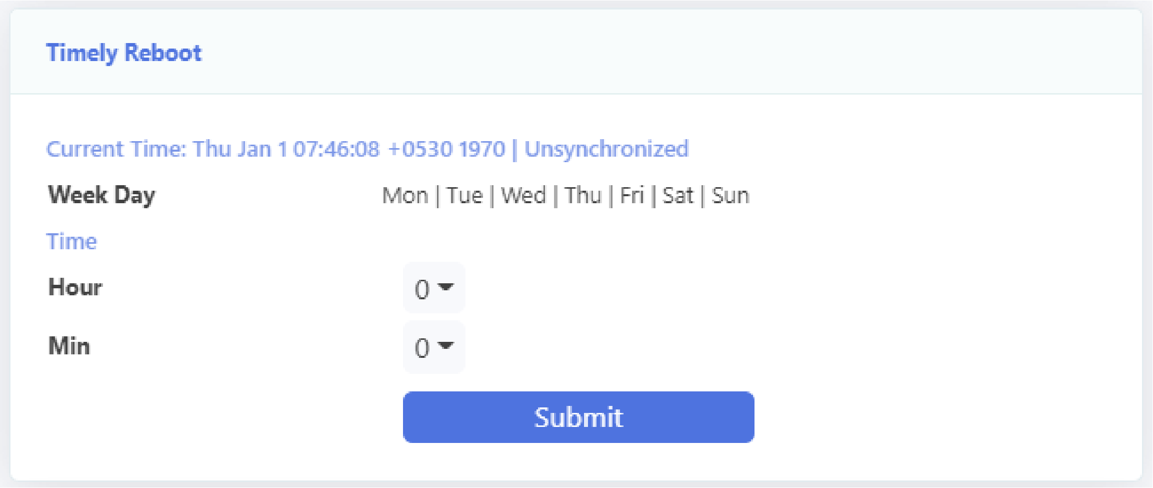


Figure 3-6-4: Device reboot

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.



Timely Reboot

Current Time: Thu Jan 1 07:46:08 +0530 1970 | Unsynchronized

Week Day Mon | Tue | Wed | Thu | Fri | Sat | Sun

Time

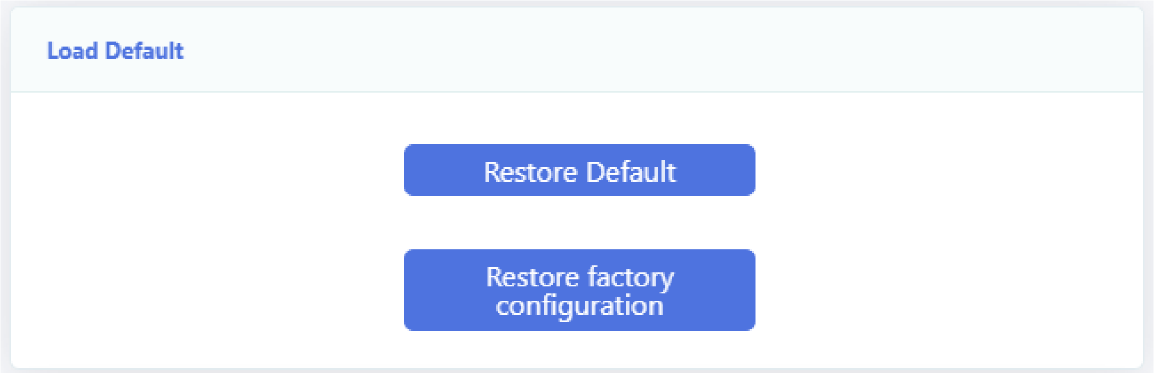
Hour 0

Min 0

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.



Load Default

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.

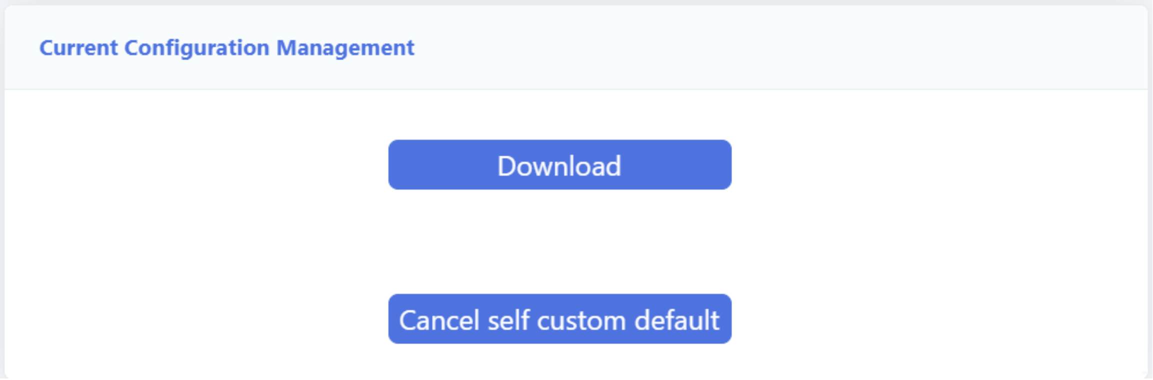

Current Configuration Management

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 .

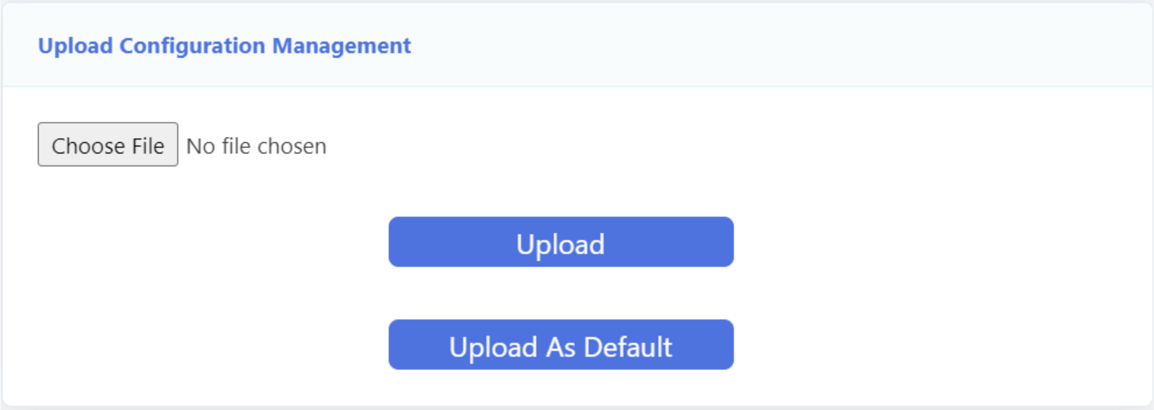
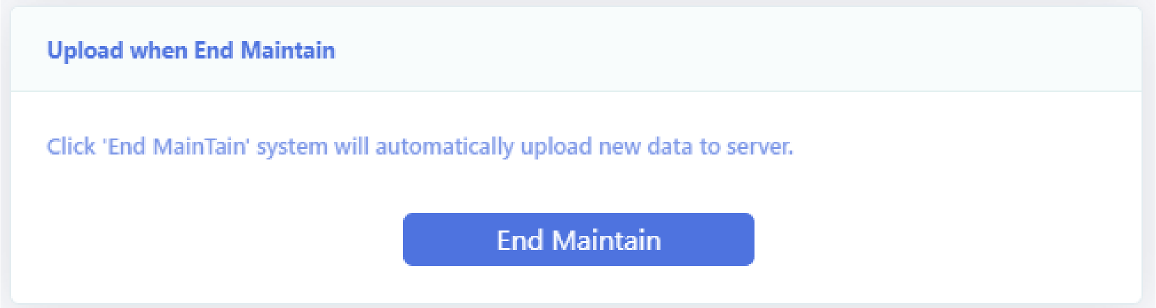

Upload Configuration Management

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.

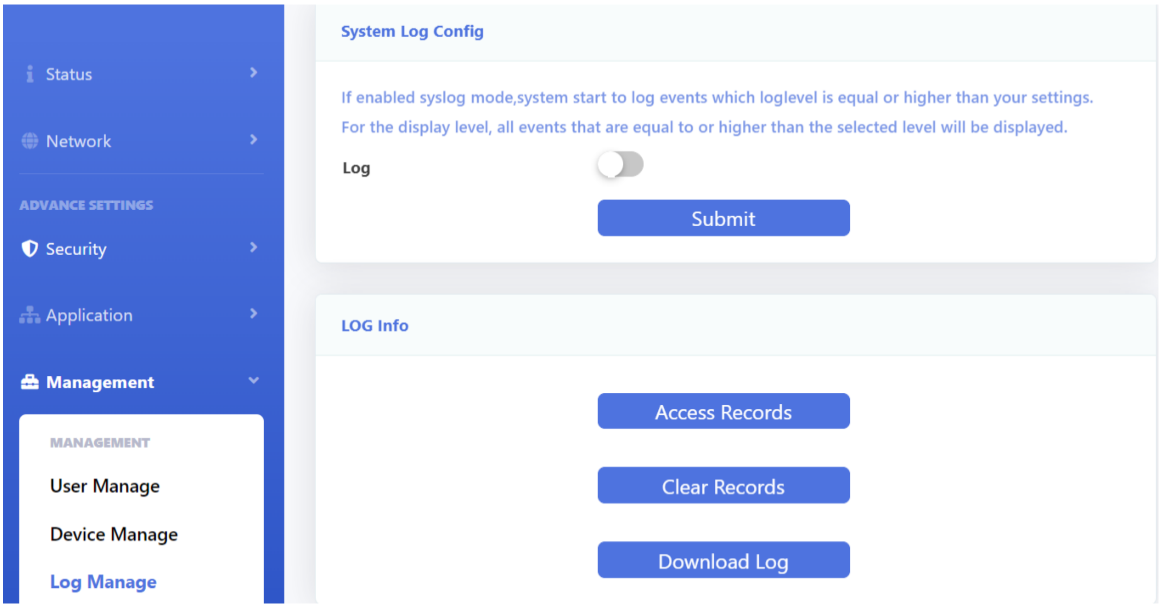

Upload when End Maintain

Click 'End MainTain' system will automatically upload new data to server.

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



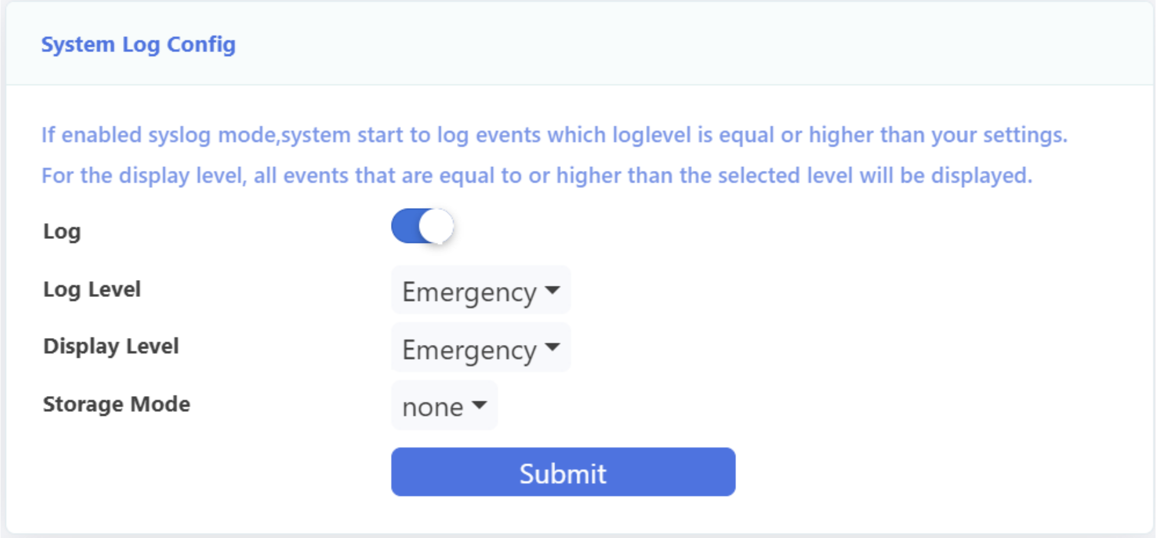
If enabled syslog mode,system start to log events which loglevel is equal or higher than your settings.
For the display level, all events that are equal to or higher than the selected level will be displayed.

Log

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.



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

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.

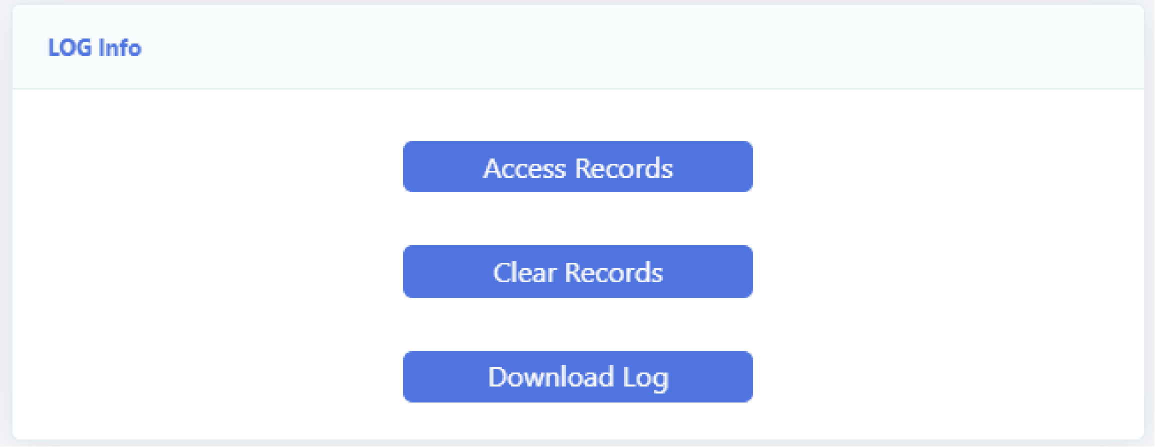


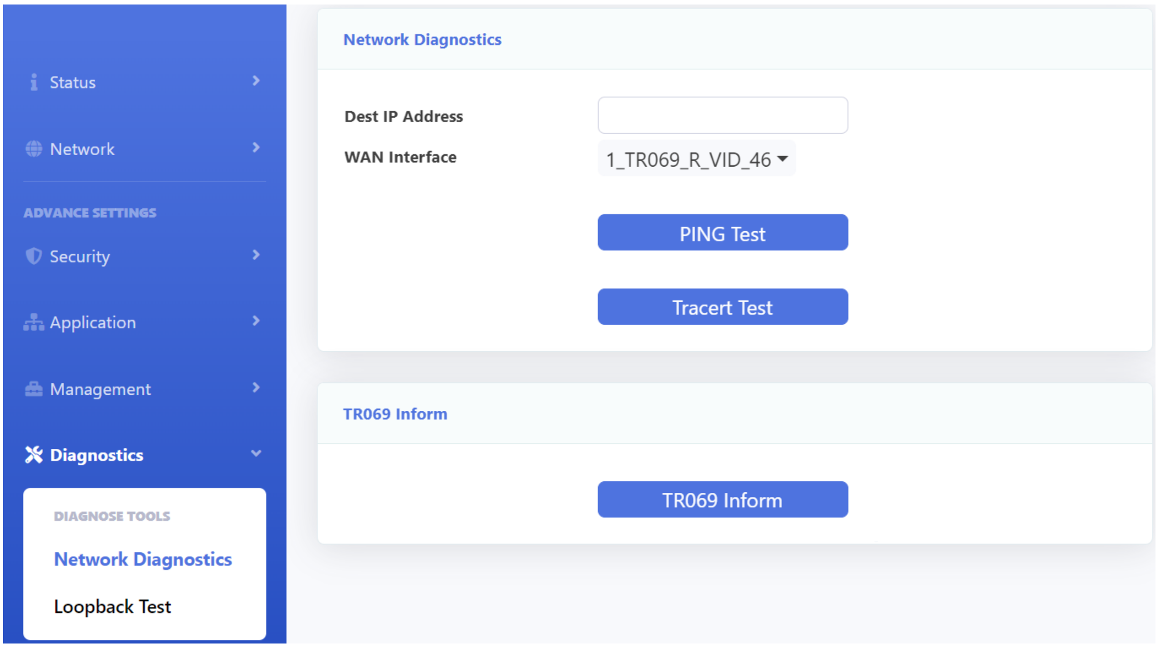
Figure 3-6-12: Log Info

3.7 Diagnostics

3.7.1 Network diagnostics

3.7.1.1 Network diagnostics

This page is used for ping test and tracert 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.



Dest IP Address
WAN Interface 1_TR069_R_VID_46

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.

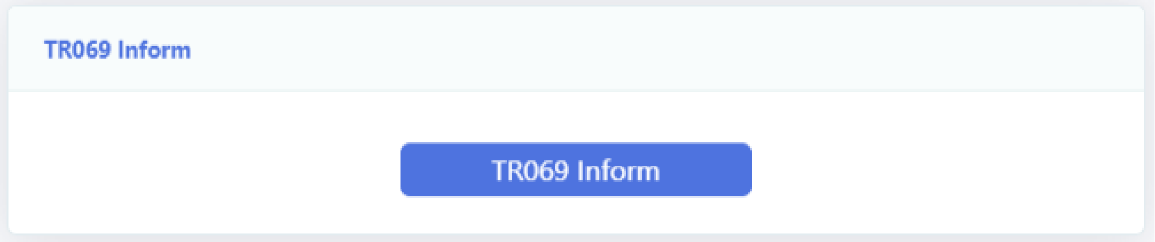
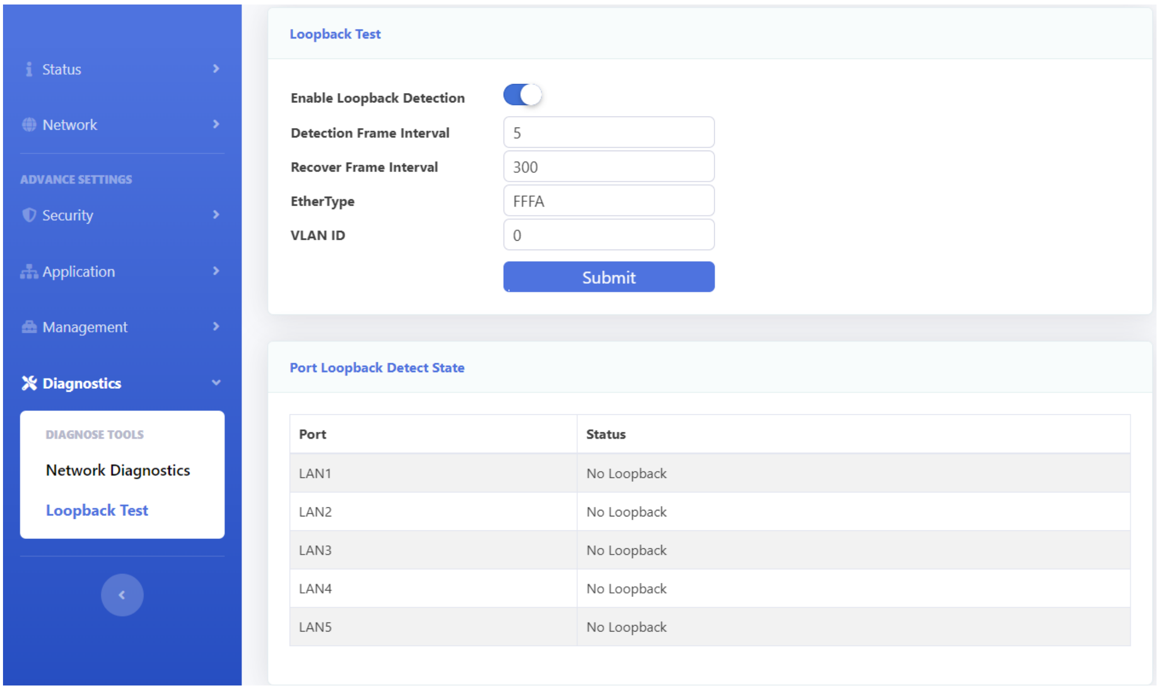


Figure :3-7-2 TR069 Inform

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: 5

Recover Frame Interval: 300

EtherType: FFFA

VLAN ID: 0

Submit

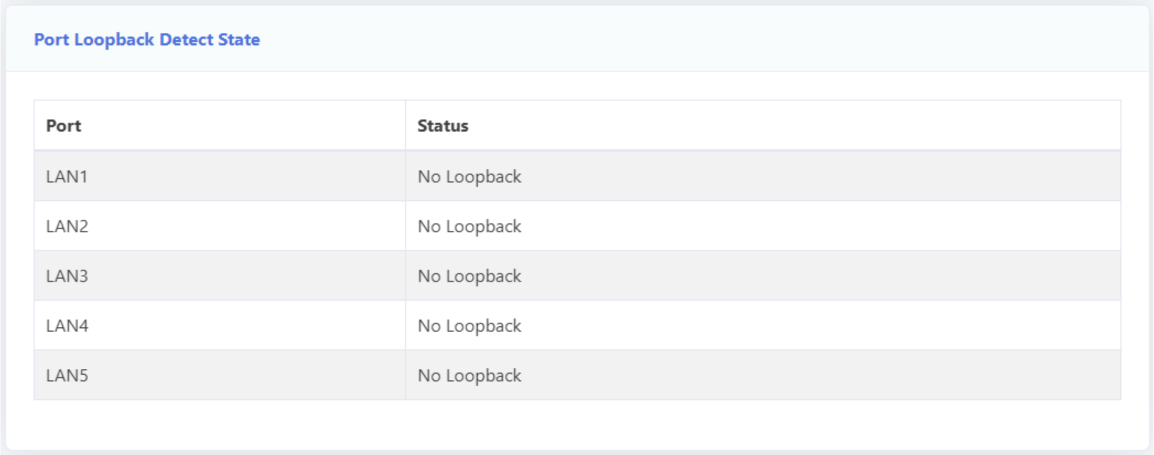
Port Loopback Detect State

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

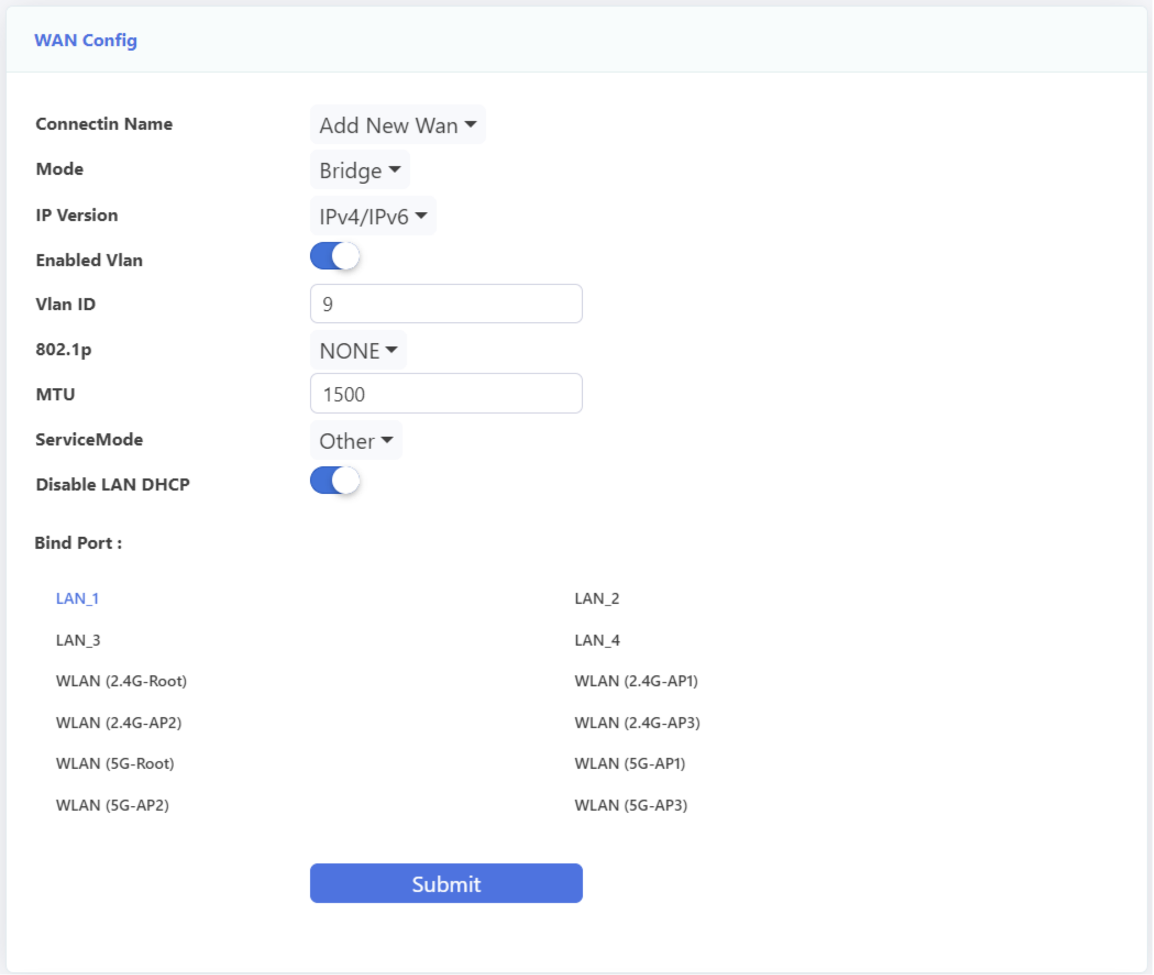
Before configuring, make sure ONU has registered and been authorized successfully. Connect PC to one LAN port of ONU directly with twisted cable.

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.



WAN Config

Connectin Name	Add New Wan
Mode	Bridge
IP Version	IPv4/IPv6
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
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

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

2) Surf the Internet

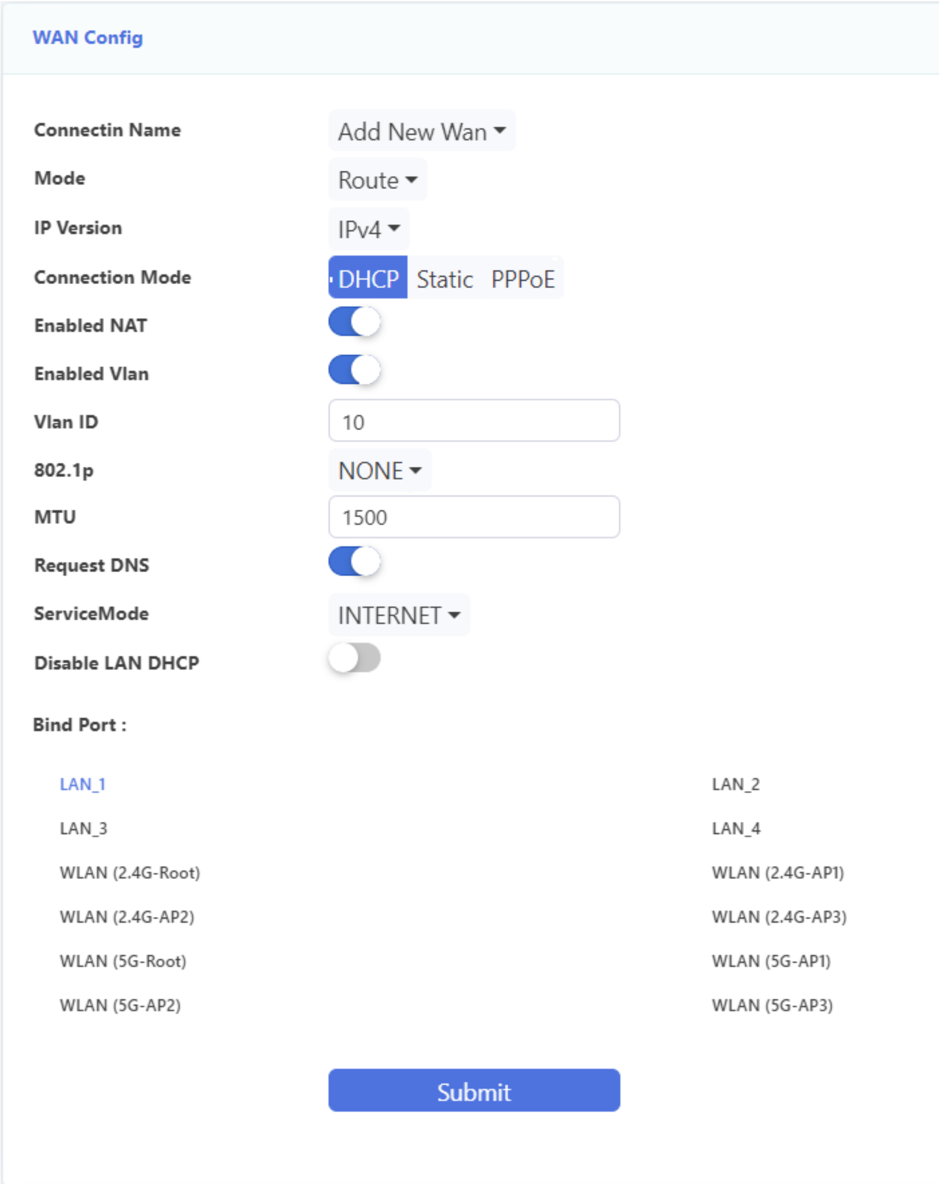
Connect PC to LAN 1 port. After get IP address from DHCP server in the network, the PC can surf the Internet.

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.



WAN Config

Connectin Name: Add New Wan

Mode: Route

IP Version: IPv4

Connection Mode: DHCP 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
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

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

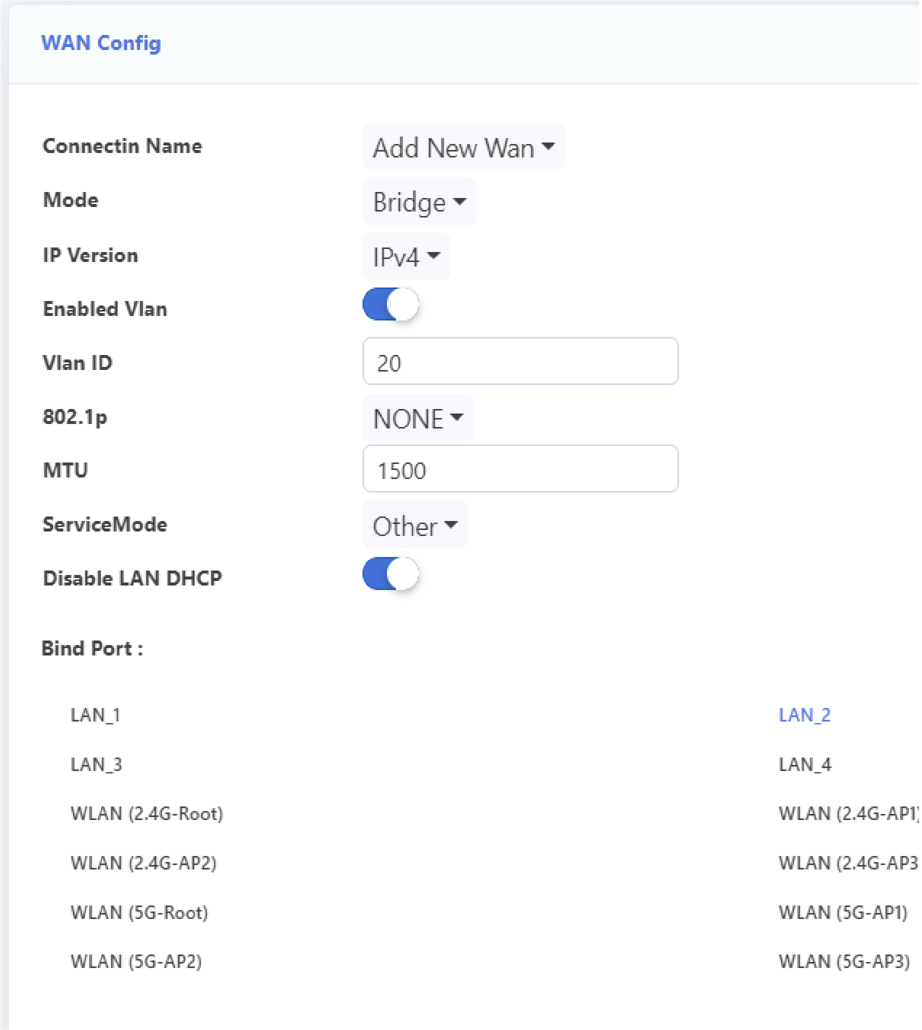
Before configuring, make sure ONU has registered and been authorized successfully. Connect PC to one LAN port of ONU directly with twisted cable.

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.



WAN Config

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

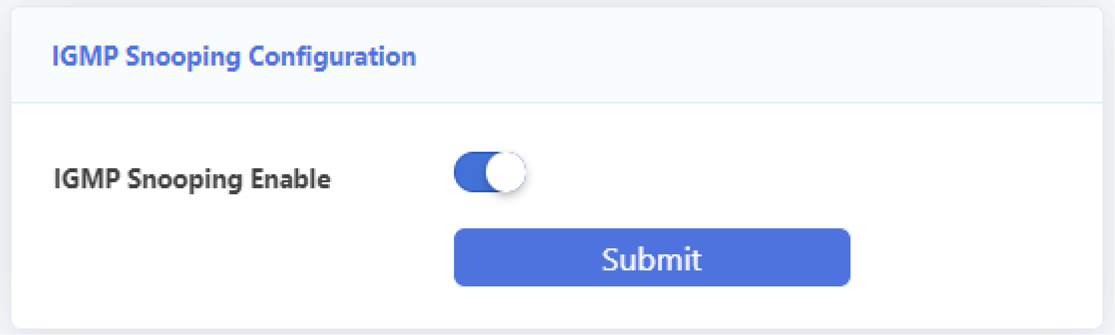
Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

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.



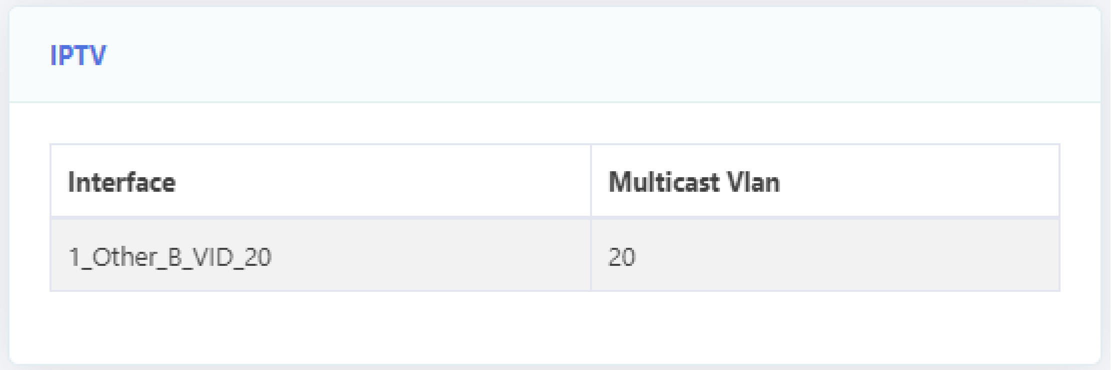
IGMP Snooping Configuration

IGMP Snooping Enable ●

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.



IPTV

Interface	Multicast Vlan
1_Other_B_VID_20	20

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.

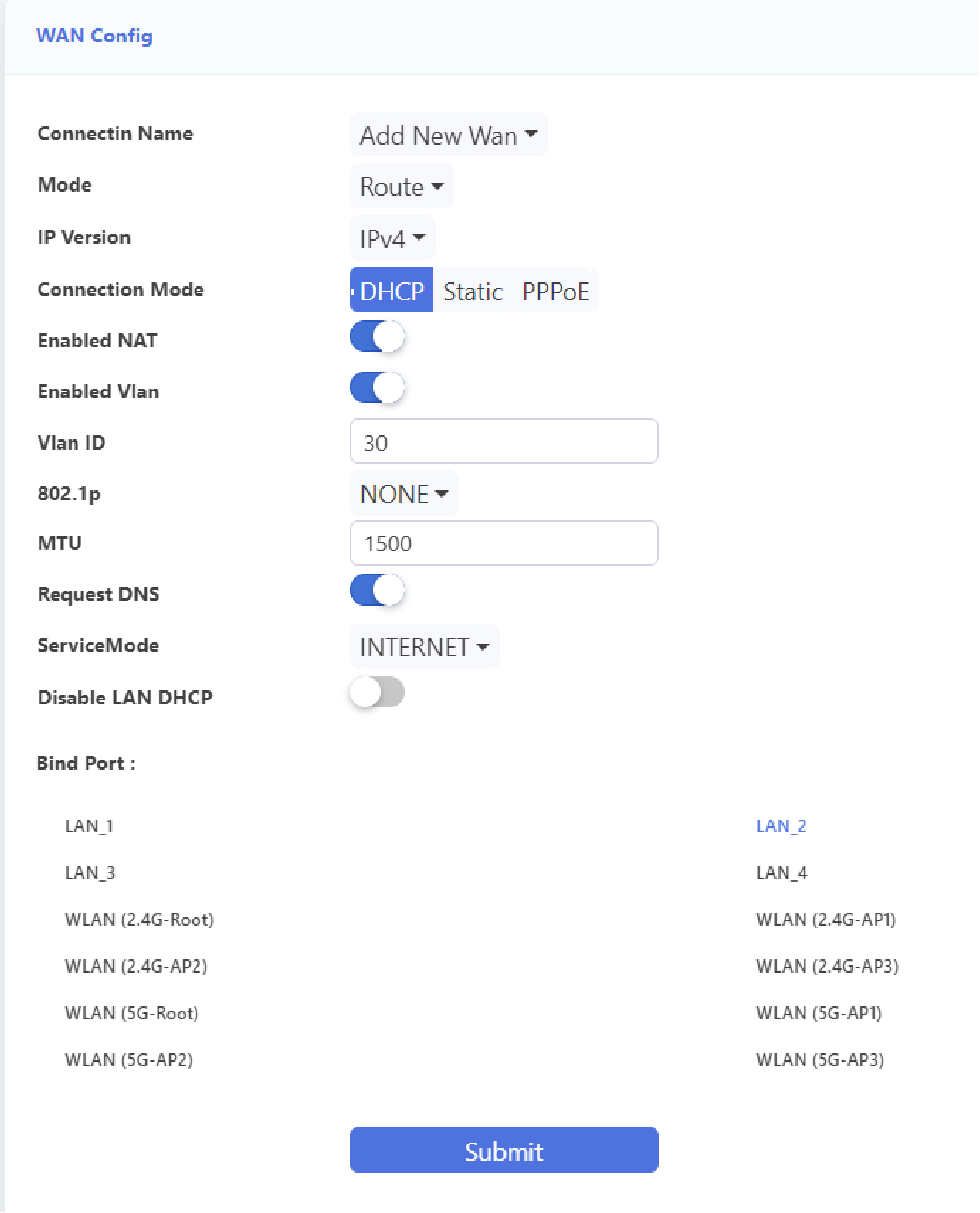
4.2.2.2 Route mode for IGMP

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.



WAN Config

Connectin Name	Add New Wan
Mode	Route
IP Version	IPv4
Connection Mode	DHCP Static PPPoE
Enabled NAT	●
Enabled Vlan	●
Vlan ID	30
802.1p	NONE
MTU	1500
Request DNS	●
ServiceMode	INTERNET
Disable LAN DHCP	○

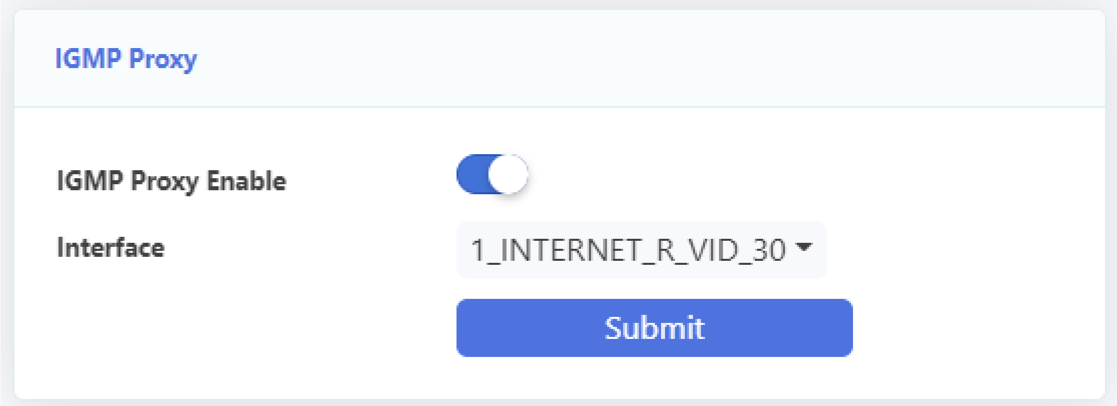
Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

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.



IGMP Proxy

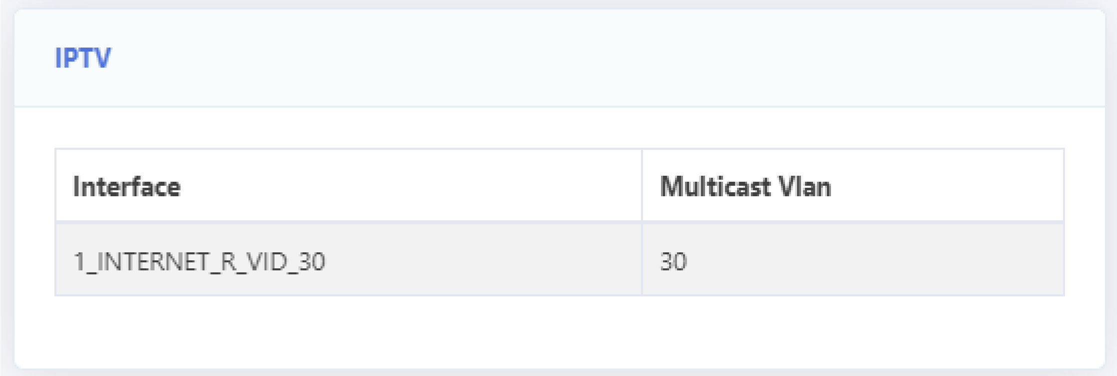
IGMP Proxy Enable: ●

Interface: 1_INTERNET_R_VID_30

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.



IPTV

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 VoIP service

HGU supports SIP protocol for VoIP service. This example introduces how to configure VoIP service on webpage.

4.3.1 Requirement

HGU works on route mode. Its IP address is 192.168.6.199, VLAN ID is 3000.

SIP server is 192.168.6.6, proxy server is 192.168.6.6.

Phone numbers are 6666.

username and the password are the same as phone numbers.

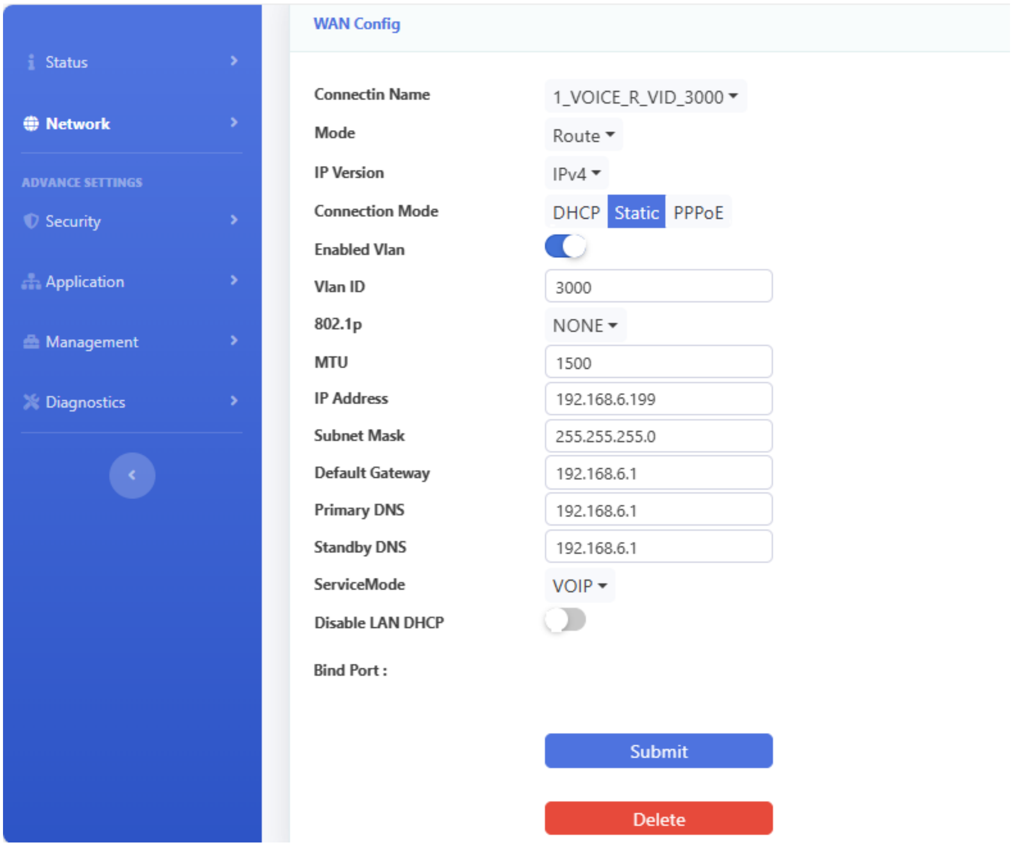
4.3.2 Steps

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

1) Add a WAN connection

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

- ✧ Protocol mode is IPv4.
- ✧ Static IP address.
- ✧ Enable VLAN and VLAN ID is 3000.
- ✧ IP address is 192.168.6.199.
- ✧ Subnet mask is 255.255.255.0.
- ✧ Default gateway is 192.168.6.1.
- ✧ Primary DNS is 192.168.6.1.
- ✧ Standby DNS is 192.168.6.1.
- ✧ Service mode is VOIP.
- ✧ Other parameters keep default.



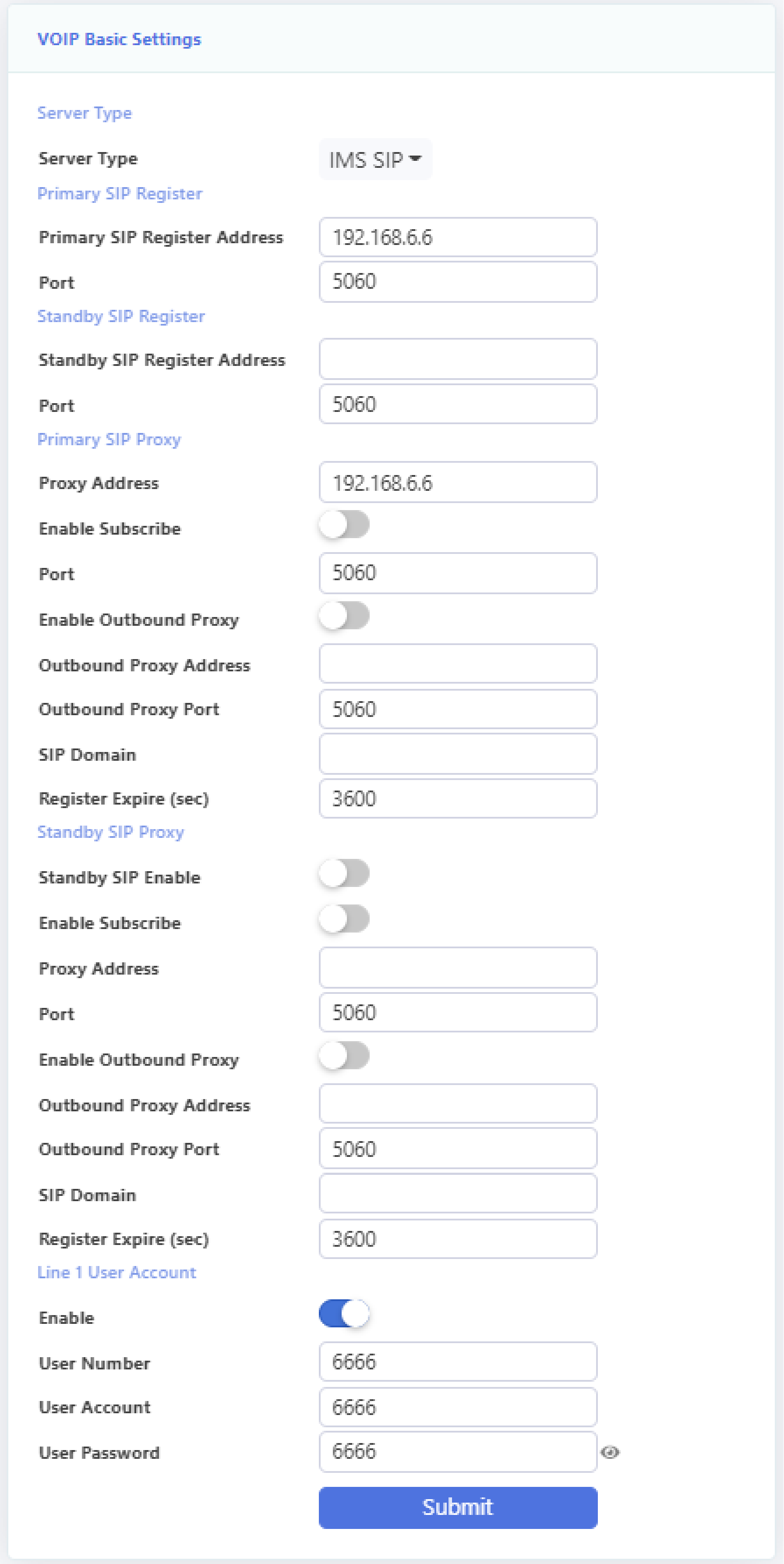
Connectin Name	1_VOICE_R_VID_3000
Mode	Route
IP Version	IPv4
Connection Mode	DHCP [✓ Static] PPPoE
Enabled Vlan	●
Vlan ID	3000
802.1p	NONE
MTU	1500
IP Address	192.168.6.199
Subnet Mask	255.255.255.0
Default Gateway	192.168.6.1
Primary DNS	192.168.6.1
Standby DNS	192.168.6.1
ServiceMode	VOIP
Disable LAN DHCP	○
Bind Port :	

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

2) Configure VoIP general parameters

Choose “Application > VoIP Basic Settings” in navigation menu. Set up VoIP general parameters as following shows.

- ✧ Choose which region VoIP service is used for. Different regions have different Dial tones, ringing tones etc.
- ✧ Proxy server and registering server both are 192.168.6.6. Protocol ports both are 5060.
- ✧ Enable phone 1. Fill in phone number, username and password.



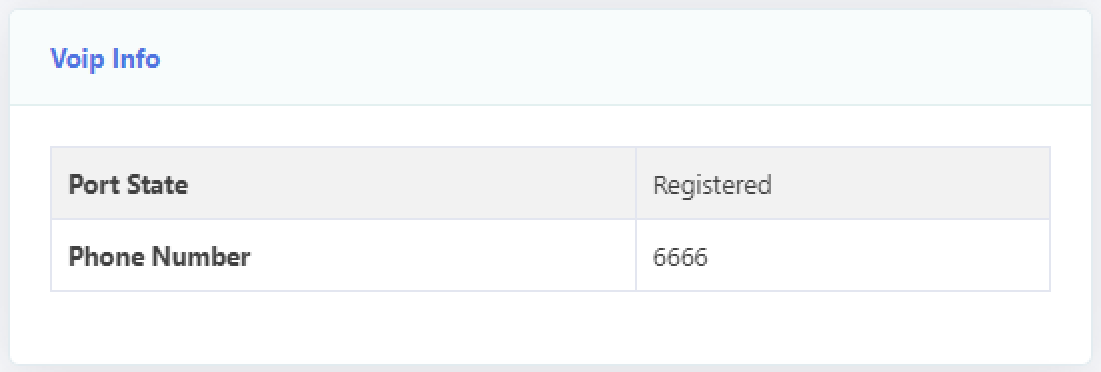
VOIP Basic Settings

Server Type	
Server Type	IMS SIP
Primary SIP Register	
Primary SIP Register Address	192.168.6.6
Port	5060
Standby SIP Register	
Standby SIP Register Address	
Port	5060
Primary SIP Proxy	
Proxy Address	192.168.6.6
Enable Subscribe	○
Port	5060
Enable Outbound Proxy	○
Outbound Proxy Address	
Outbound Proxy Port	5060
SIP Domain	
Register Expire (sec)	3600
Standby SIP Proxy	
Standby SIP Enable	○
Enable Subscribe	○
Proxy Address	
Port	5060
Enable Outbound Proxy	○
Outbound Proxy Address	
Outbound Proxy Port	5060
SIP Domain	
Register Expire (sec)	3600
Line 1 User Account	
Enable	●
User Number	6666
User Account	6666
User Password	6666

Figure 4-3-2: VoIP Basic settings

3) Look up register status

Choose “Status > WAN Info > VoIP Info” in navigation menu. You can use VoIP service when register status is successful.



Voip Info

Port State	Registered
Phone Number	6666

Figure 4-3-3: VoIP registering status

4.4 Internet and IPTV service mixed

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

4.4.1 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.

4.4.2 Steps

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

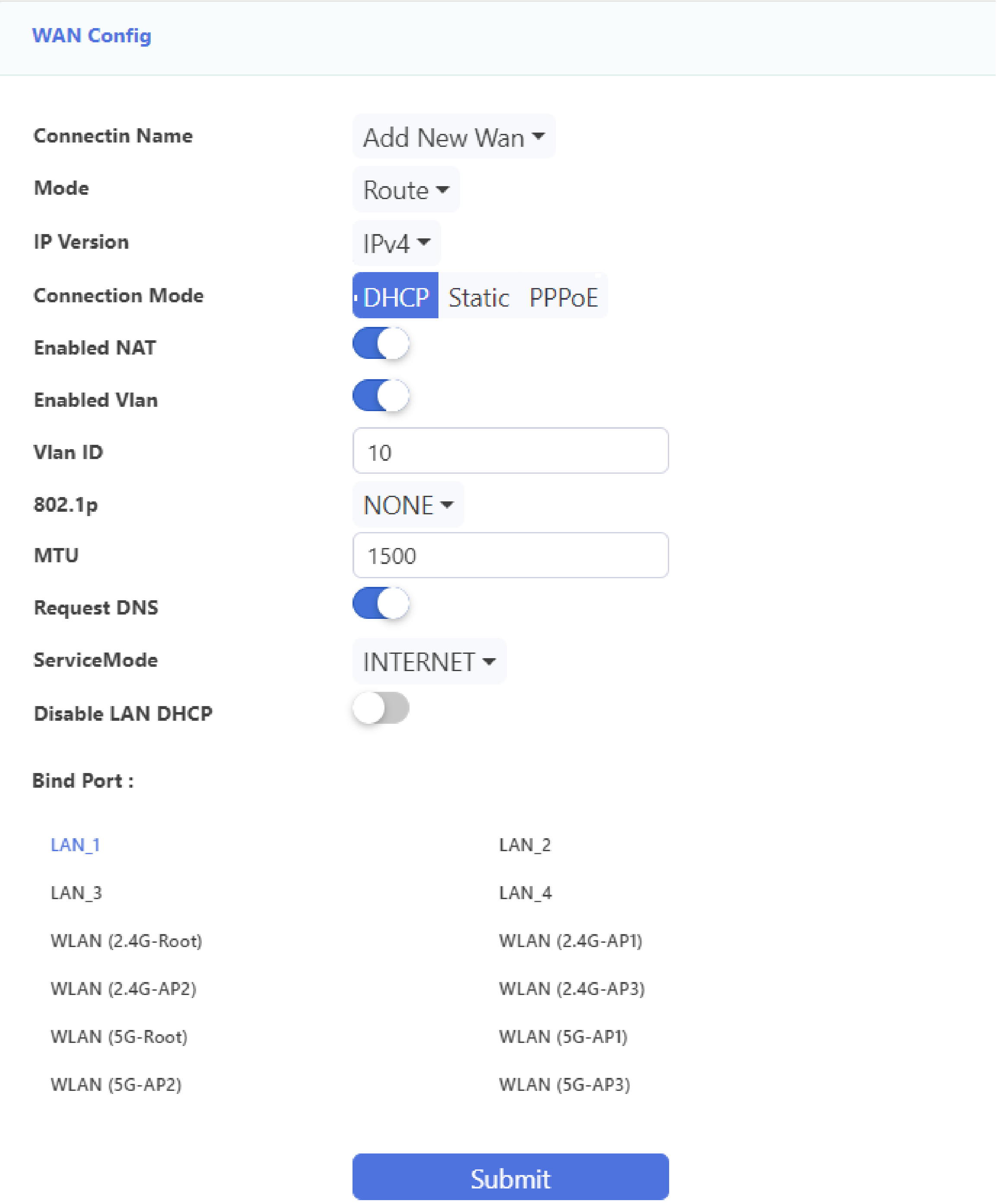
4.4.2.1 Route and bridge mode for mixed service

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: on

Enabled Vlan: on

Vlan ID: 10

802.1p: NONE

MTU: 1500

Request DNS: on

ServiceMode: INTERNET

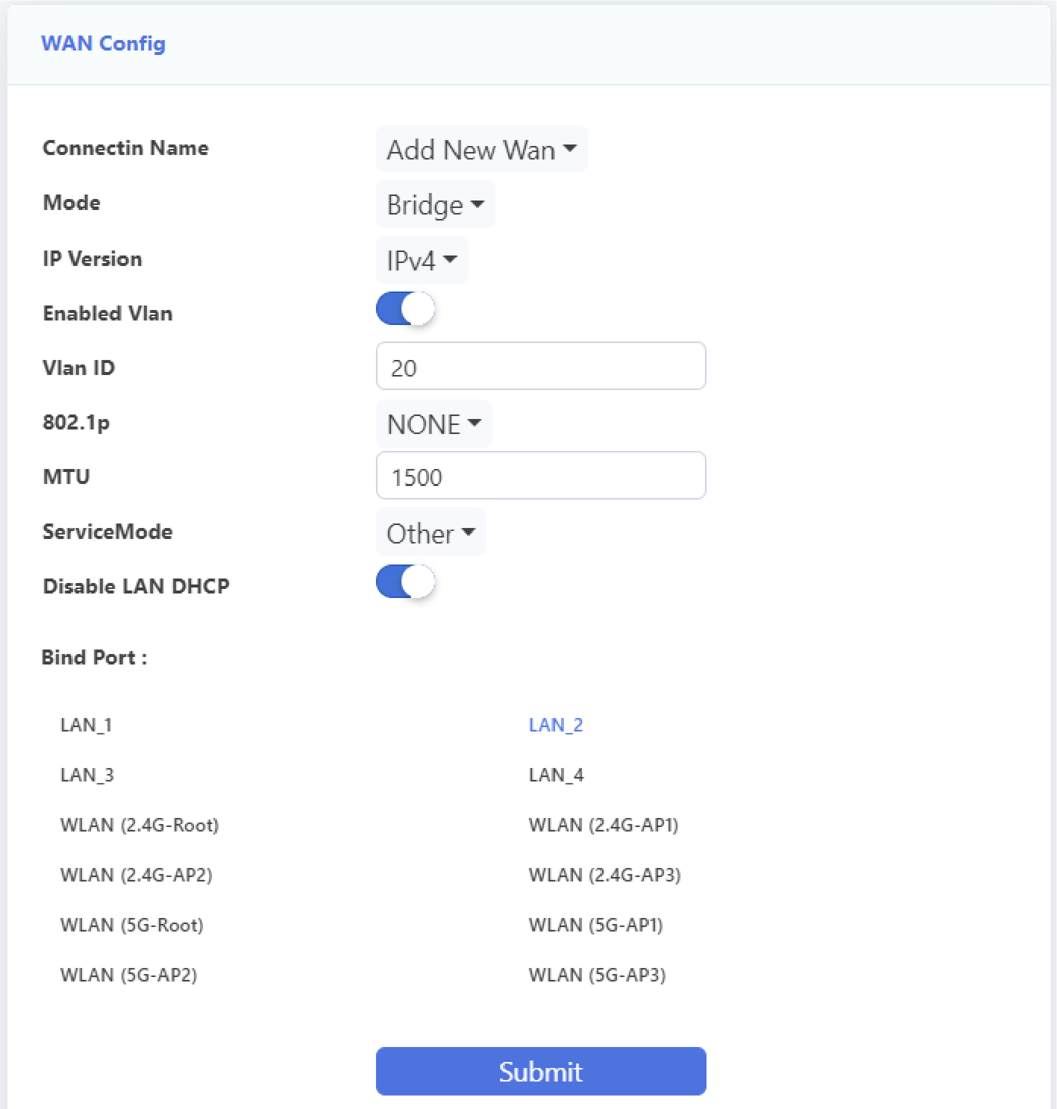
Disable LAN DHCP: off

Bind Port :

[✓ LAN_1]	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

Figure 4-4-1: 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.



WAN Config

Connectin Name: Add New Wan

Mode: Bridge

IP Version: IPv4

Enabled Vlan: ●

Vlan ID: 20

802.1p: NONE

MTU: 1500

ServiceMode: Other

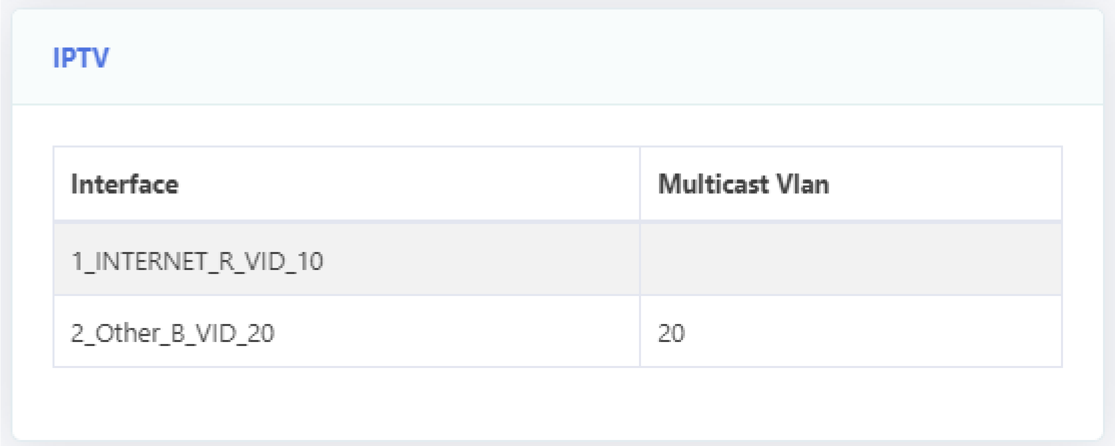
Disable LAN DHCP: ●

Bind Port :

Figure 4-4-2: 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.



IPTV

Interface	Multicast Vlan
1_INTERNET_R_VID_10	
2_Other_B_VID_20	20

Figure 4-4-3: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

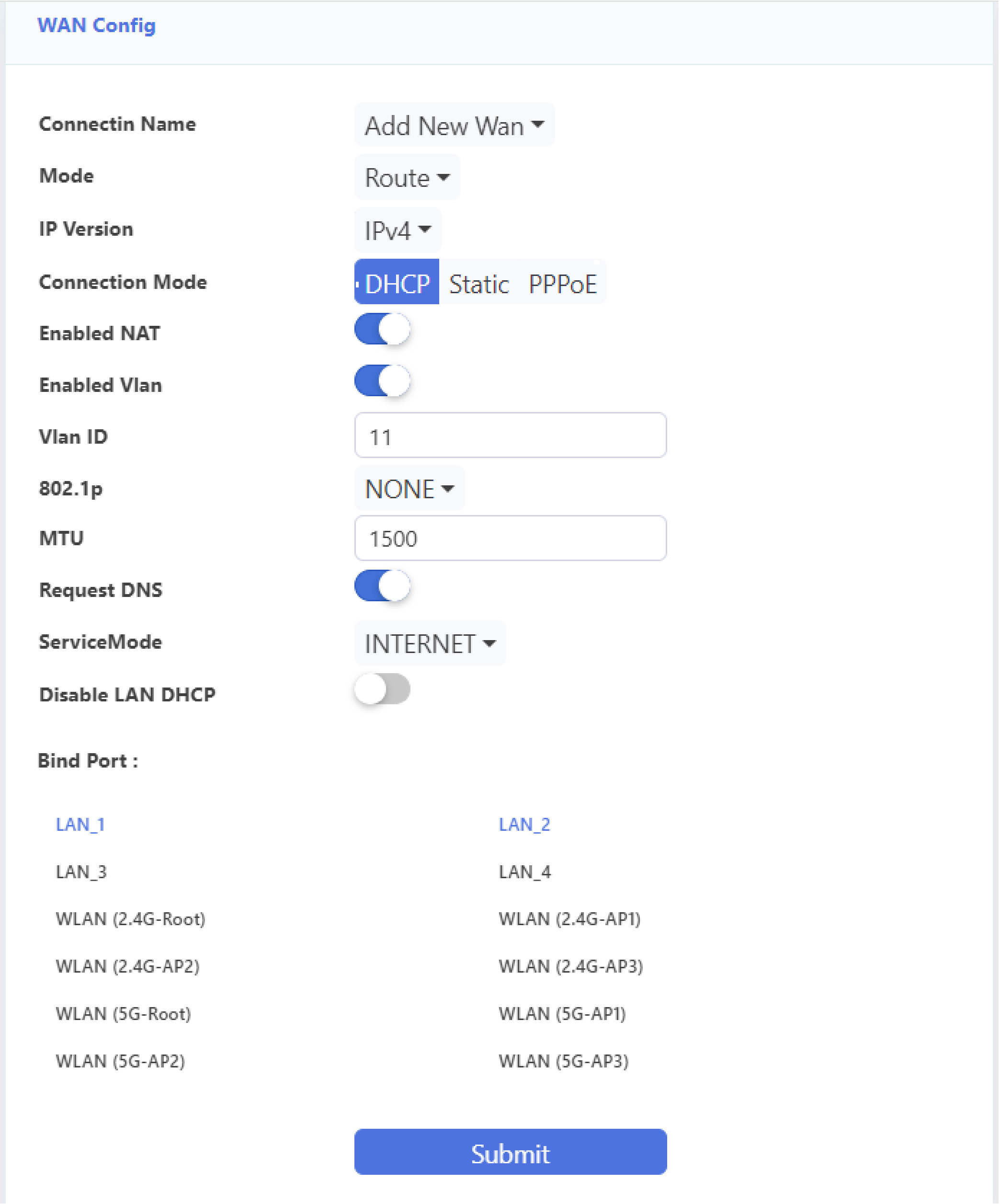
Connect STB to LAN port 2. After STB gets an IP address from ISP via DHCP, you can watch IPTV.

4.4.2.2 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.



WAN Config

Connectin Name	Add New Wan
Mode	Route
IP Version	IPv4
Connection Mode	DHCP Static PPPoE
Enabled NAT	●
Enabled Vlan	●
Vlan ID	11
802.1p	NONE
MTU	1500
Request DNS	●
ServiceMode	INTERNET
Disable LAN DHCP	○

Bind Port :

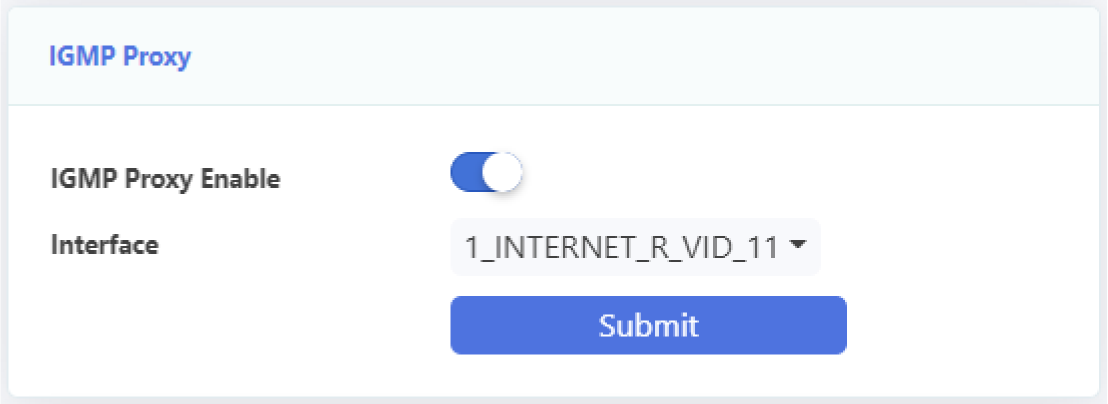
LAN_1	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

Submit

Figure 4-4-4: 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 .



IGMP Proxy

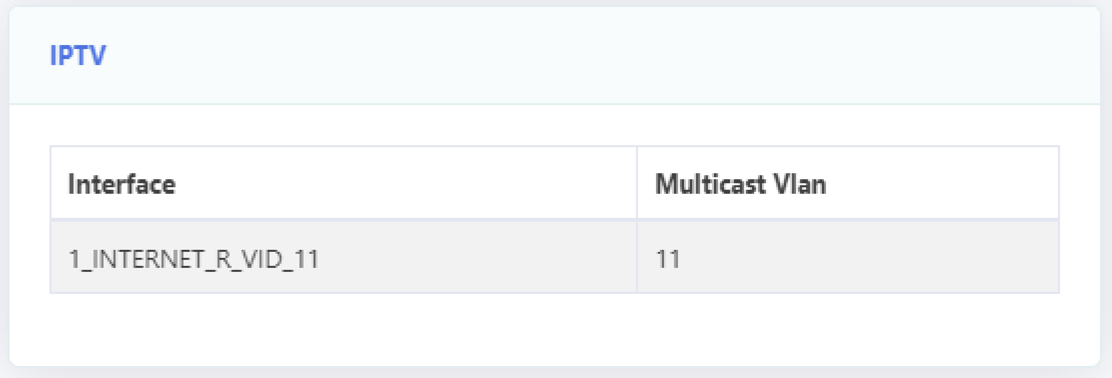
IGMP Proxy Enable ●

Interface: 1_INTERNET_R_VID_11

Figure 4-4-5: Enable IGMP proxy

3) Add Multicast VLAN

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



IPTV

Interface	Multicast Vlan
1_INTERNET_R_VID_11	11

Figure 4-4-6: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.

4.5 Internet, IPTV and VOIP service mixed

4.5.1 Requirement

LAN 1 is used for Internet service, VLAN is 10;

LAN 2 is used for IPTV service, including VOD（unicast）and multicast, VLAN both are 1100;

VOIP VLAN is 3000, VOIP IP address is 192.168.6.19, and SIP server is 192.168.6.33. The proxy server is 192.168.6.33 too;

Username and password of SIP account: 12345678,12345678.

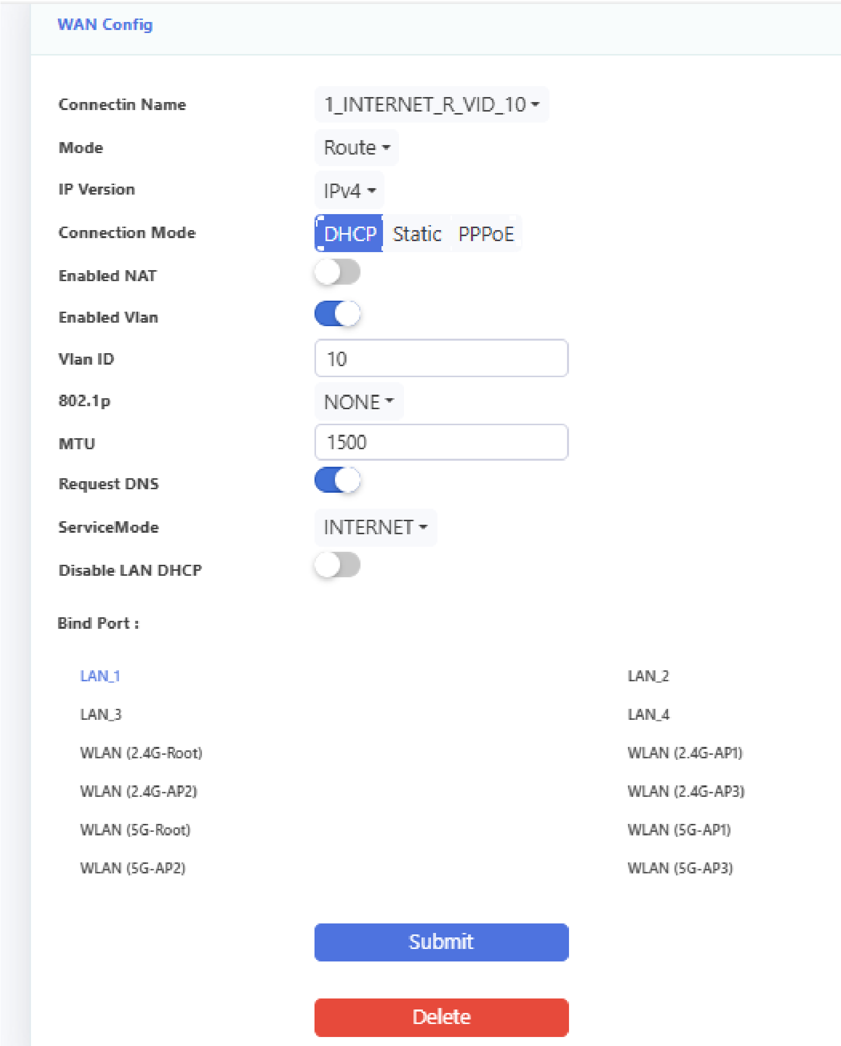
4.5.2 Steps

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

1) Add WAN connection

Choose "Network > WAN > WAN Config" in navigation menu. Add a route mode WAN connection for Internet service as the following parameters.

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



WAN Config

Connectin Name: 1_INTERNET_R_VID_10

Mode: Route

IP Version: IPv4

Connection Mode: [✓ DHCP] Static PPPoE

Enabled NAT: ○

Enabled Vlan: ●

Vlan ID: 10

802.1p: NONE

MTU: 1500

Request DNS: ●

ServiceMode: INTERNET

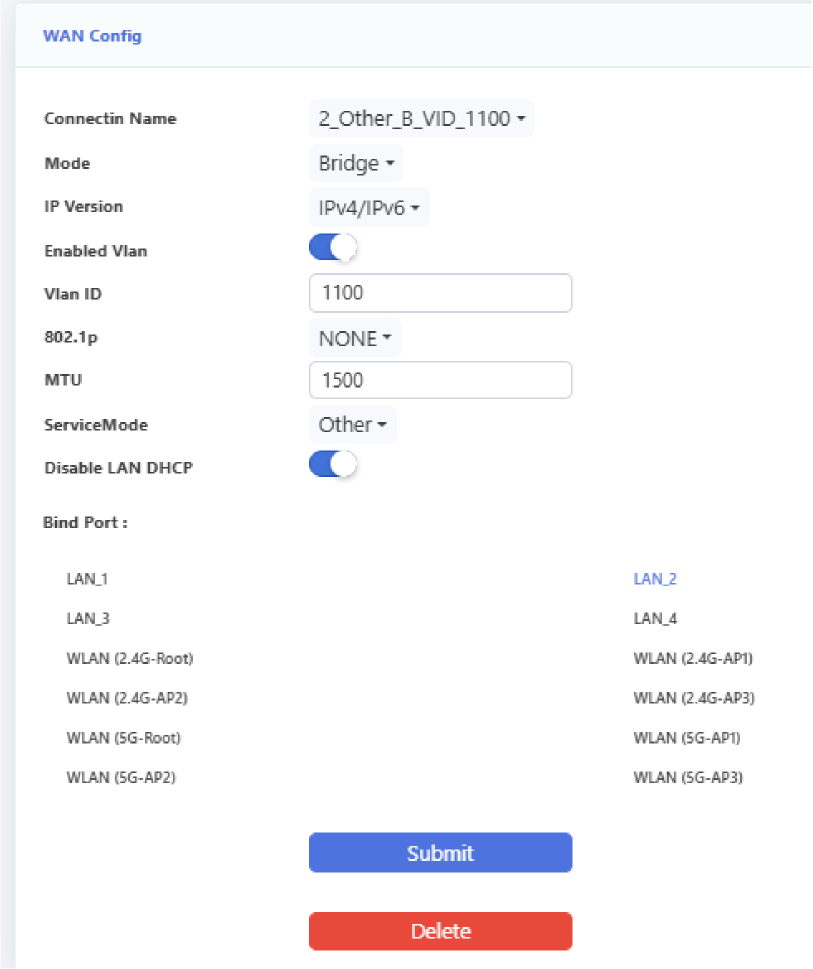
Disable LAN DHCP: ○

Bind Port :

[✓ LAN_1]	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

Figure 4-5-1: Add a WAN connection for Internet service

Add a bridge mode WAN connection for IPTV service. Enable VLAN and its VLAN ID is 1100. Service mode is other. Bind LAN 2.



WAN Config

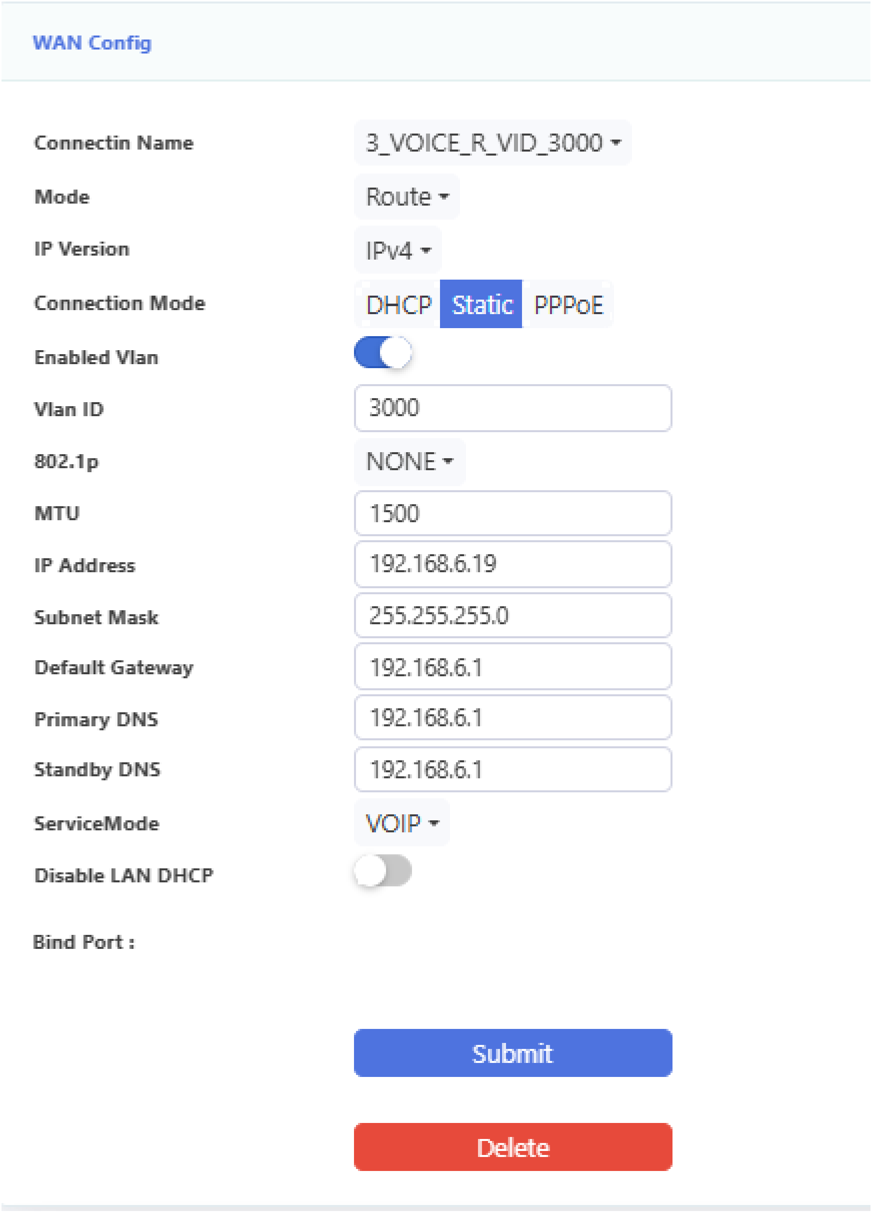
Connectin Name	2_Other_B_VID_1100 ▾
Mode	Bridge ▾
IP Version	IPv4/IPv6 ▾
Enabled Vlan	●
Vlan ID	1100
802.1p	NONE ▾
MTU	1500
ServiceMode	Other ▾
Disable LAN DHCP	●

Bind Port :

LAN_1	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

Figure 4-5-2: Add a WAN connection for IPTV service

Add a route mode WAN connection for VOIP service. Choose IPv4 and static; fill up the IP address, mask, gateway, DNS etc. Enable VLAN, VLAN ID is 3000. Service mode is VOIP.



WAN Config

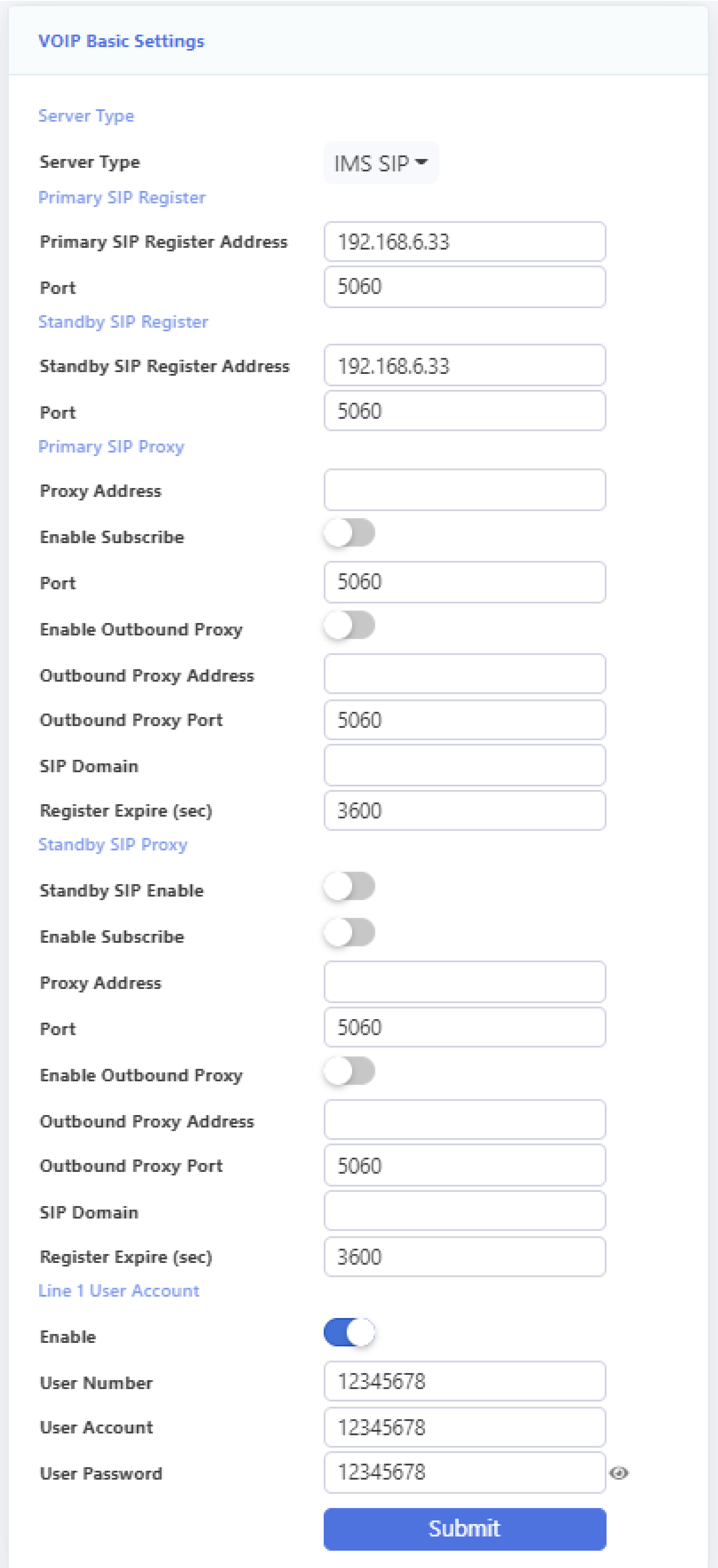
Connectin Name	3_VOICE_R_VID_3000 ▾
Mode	Route ▾
IP Version	IPv4 ▾
Connection Mode	DHCP [✓ Static] PPPoE
Enabled Vlan	●
Vlan ID	3000
802.1p	NONE ▾
MTU	1500
IP Address	192.168.6.19
Subnet Mask	255.255.255.0
Default Gateway	192.168.6.1
Primary DNS	192.168.6.1
Standby DNS	192.168.6.1
ServiceMode	VOIP ▾
Disable LAN DHCP	○
Bind Port :	

Figure 4-5-3: Add a WAN connection for VOIP service

2) Configure VOIP general parameters

Choose "Application > VOIP Basic Settings" in navigation menu. Configure VOIP general parameters as the following shows.

- ✧ "Region" contains many countries or regions. Different regions have their own dial tone and ringing tone, etc.
- ✧ "Proxy server" and "Registering server" both are 192.168.6.33, port is 5060;
- ✧ Fill up phone number, username and password of each line.
- ✧ Choose packing time, default is 20ms.



VOIP Basic Settings

Server Type

Server Type	IMS SIP

Primary SIP Register

Primary SIP Register Address	192.168.6.33
Port	5060

Standby SIP Register

Standby SIP Register Address	192.168.6.33
Port	5060

Primary SIP Proxy

Proxy Address	
Enable Subscribe	○
Port	5060
Enable Outbound Proxy	○
Outbound Proxy Address	
Outbound Proxy Port	5060
SIP Domain	
Register Expire (sec)	3600

Standby SIP Proxy

Standby SIP Enable	○
Enable Subscribe	○
Proxy Address	
Port	5060
Enable Outbound Proxy	○
Outbound Proxy Address	
Outbound Proxy Port	5060
SIP Domain	
Register Expire (sec)	3600

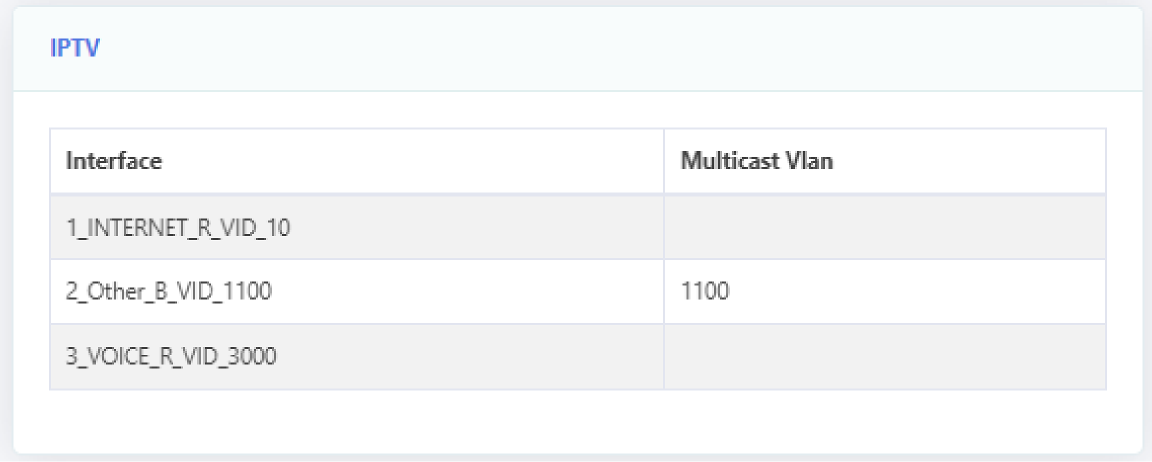
Line 1 User Account

Enable	●
User Number	12345678
User Account	12345678
User Password	12345678

Figure 4-5-4: VOIP general settings

3) Add IGMP snooping VLAN

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



IPTV

Interface	Multicast Vlan
1_INTERNET_R_VID_10	
2_Other_B_VID_1100	1100
3_VOICE_R_VID_3000	

Figure 4-5-5:Add multicast VLAN.

4) Surf the Internet

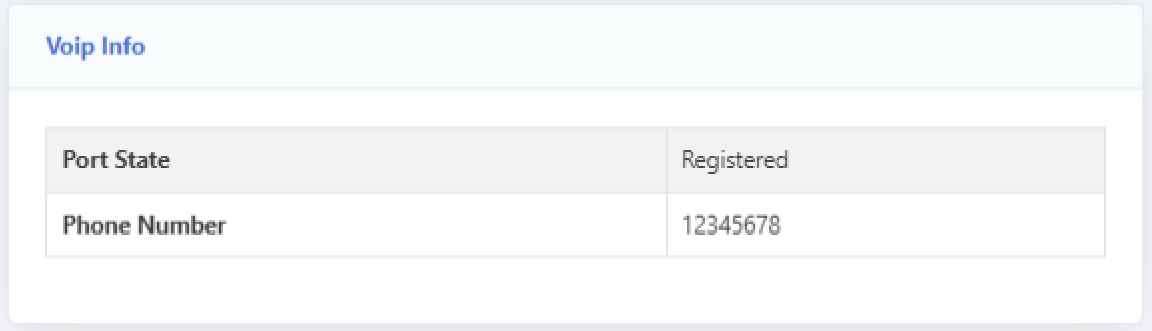
Connect PC to LAN port 1. The PC gets an IP address from HGU and HGU gets an IP address from DHCP server in the network, and then you can surf the Internet.

5) Watch IPTV

After STB gets an IP address from ISP via DHCP, you can watch IPTV.

6) Look up register status

Choose “Status >WAN Info > VoIP Info” in navigation menu. You can use VoIP service when register status is successful.



Voip Info

Port State	Registered
Phone Number	12345678

Figure 4-5-6: VOIP information

4.6 WLAN service

HGU supports wireless access service. This example introduces how to configure WLAN service when HGU works on Route mode.

4.6.1 Requirement

1) HGU works on Route mode, HGU gets IP by DHCP mode,VLAN ID is 11.
2) Only enable SSID 1, its name is “xyz”. Network authentication method is WPA-PSK, and encryption method is TKIP+AES.

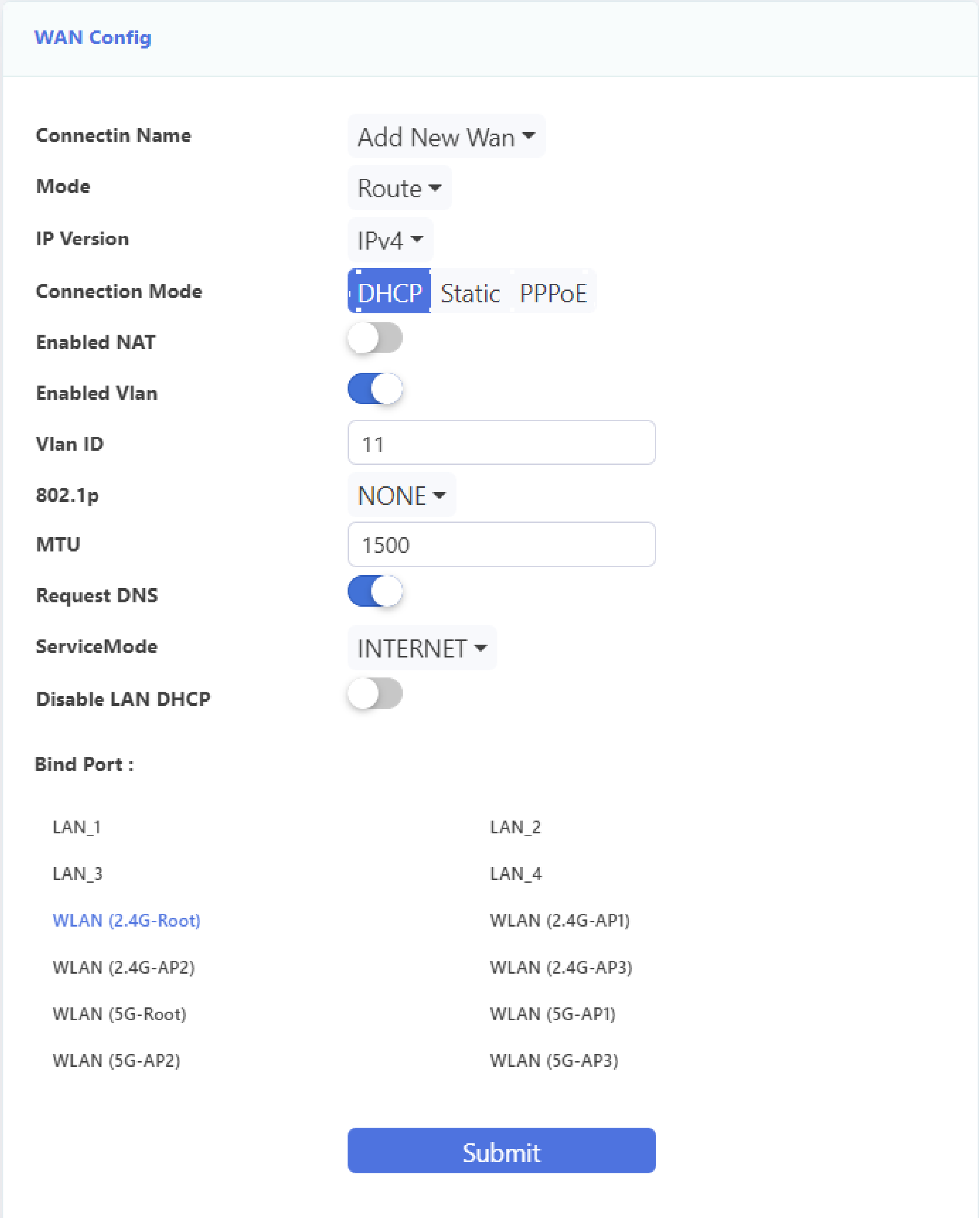
4.6.2 Steps

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

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.
- ✧ Obtain IP address by DHCP.
- ✧ Enable VLAN and VLAN ID is 11.
- ✧ Service mode is INTERNET and bind WLAN(AP0-2.4G).
- ✧ 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	11
802.1p	NONE
MTU	1500
Request DNS	●
ServiceMode	INTERNET
Disable LAN DHCP	○

Bind Port :

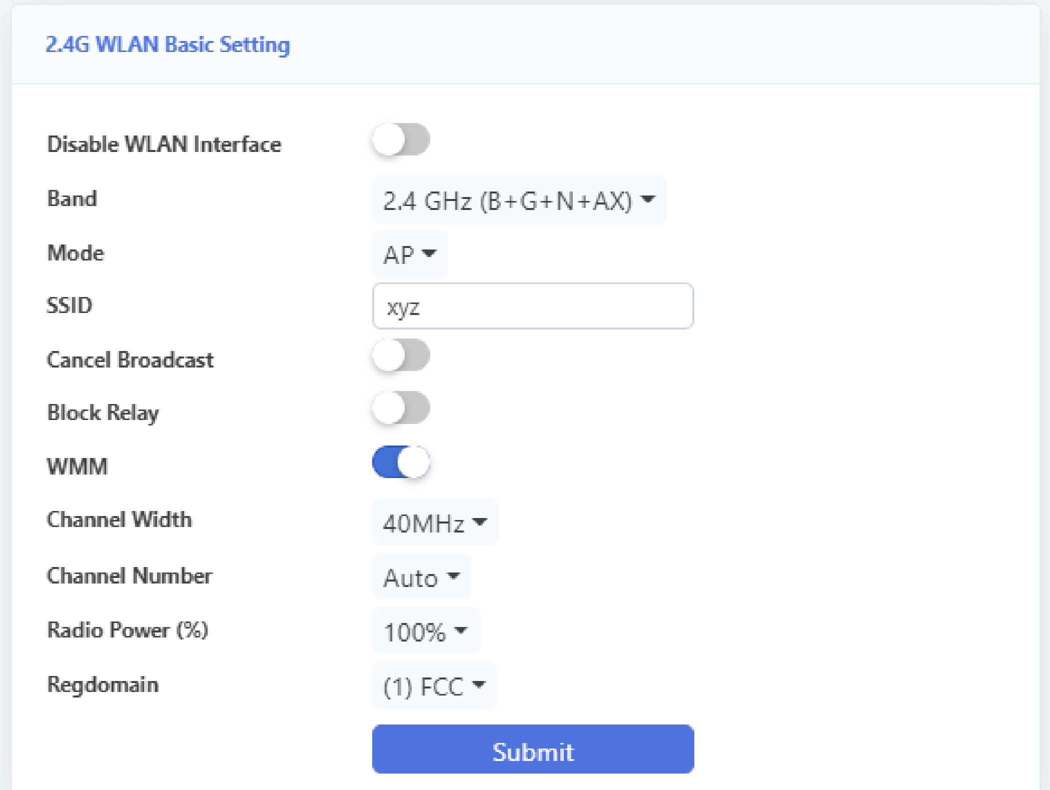
LAN_1	LAN_2
LAN_3	LAN_4
WLAN (2.4G-Root)	WLAN (2.4G-AP1)
WLAN (2.4G-AP2)	WLAN (2.4G-AP3)
WLAN (5G-Root)	WLAN (5G-AP1)
WLAN (5G-AP2)	WLAN (5G-AP3)

✧

Figure 4-6-1: Add a route WAN connection

2) Configure WLAN basic parameters

Choose “Network > 2.4G > 2.4G WLAN Basic Setting” in navigation menu. Enable wireless and modify SSID1’s name to xyz. For other parameters, just configure the suitable ones if necessary.



2.4G WLAN Basic Setting

Disable WLAN Interface

Band: 2.4 GHz (B+G+N+AX)

Mode: AP

SSID: xyz

Cancel Broadcast

Block Relay

WMM

Channel Width: 40MHz

Channel Number: Auto

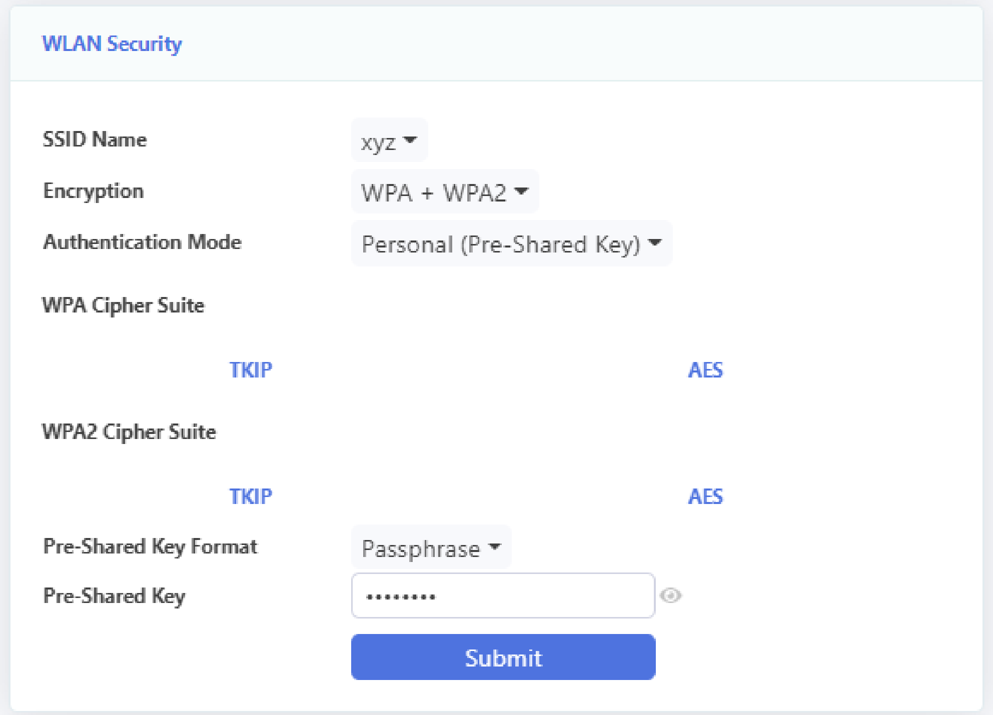
Radio Power (%): 100%

Regdomain: (1) FCC

Figure 4-6-2: WLAN basic settings

3) Configure network authentication

Choose “Network > 2.4G > WLAN Security” in navigation menu. Select the SSID, and set up WPA+WPA2 for its network authentication method and AES for its encryption method. Fill a password in passphrase textbox.



WLAN Security

SSID Name: xyz

Encryption: WPA + WPA2

Authentication Mode: Personal (Pre-Shared Key)

WPA Cipher Suite

TKIP AES

WPA2 Cipher Suite

TKIP AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ••••••••

Figure 4-6-3: WLAN security settings

4) Surf the Internet

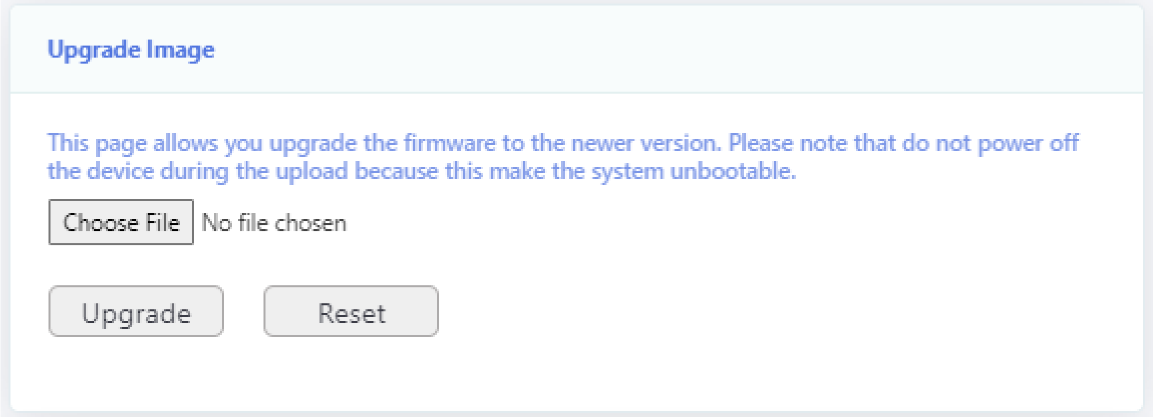
Search SSID named xyz with a laptop, double-click to connect and enter the correct password.

If client has WPS function, you can connect client to AP by pressing Pair button in HGU. When the WPS indicator blinks, press WPS button in client simultaneously. They will connect after a short time.

4.7 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. HGU will restart automatically after updated. The whole process needs about 2 minutes.



Upgrade Image

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

Figure 4-7-1: 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:** FXS indicators are not lit?

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

   (2) SIP accounts aren’t registered.

5. **Q:** PC can’t visit web UI?

   A: (1) PC and HGU 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.

6. **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.

7. **Q:** Customer can’t use the VoIP service.

   A: (1) The phone or the wire is damaged.

   (2) SIP accounts aren’t registered.

   (3) Dial plan is wrong.

8. **Q:** HGU stops to work after working for some time.

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

   (2) The device overheats.