



# User Manual

TONT-4600A ONT 1XPON+4LAN+1USB3.0+Wi-Fi6

Article		Article no.	
TONT-4600A	HGU ONT 1 XPON +4LAN + 1USB3.0 + Wi-Fi6	308704	
Version	V1.0	Date	2025/08
		EN	

## Table of content

<b>1</b>	<b>Safety Instructions .....</b>	<b>4</b>
<b>2</b>	<b>Introduction.....</b>	<b>6</b>
2.1	Product description .....	6
2.2	Detailed features .....	6
2.3	Ordering information.....	6
2.4	Installation schematic example .....	7
2.5	Front panel.....	7
2.6	Rear panel .....	8
2.7	LEDs.....	9
2.8	First installation .....	10
2.9	Setup connection .....	10
<b>3</b>	<b>Configuration.....</b>	<b>11</b>
3.1	Login.....	11
3.2	Status .....	11
3.2.1	Device Info .....	11
3.2.2	PON Info .....	12
3.2.3	WAN Info .....	13
3.2.4	LAN Info .....	15
3.3	Network.....	16
3.3.1	WAN .....	16
3.3.2	LAN .....	19
3.3.3	VLAN .....	21
3.3.4	2.4G Basic Settings .....	22
3.3.5	2.4G Adv Settings .....	24
3.3.6	5G Basic Settings .....	25
3.3.7	5G Adv Settings .....	27
3.3.8	Mesh Settings .....	28
3.3.9	Remote Management .....	29
3.3.10	QoS Settings .....	31
3.3.11	Time Settings .....	33
3.3.12	Route Settings .....	34
3.4	Security.....	35
3.4.1	Firewall .....	35
3.4.2	MAC Filtering .....	37
3.4.3	IP/Port Filtering .....	37
3.4.4	URL Filtering .....	39
3.4.5	Parental Control .....	39
3.5	Application.....	41
3.5.1	VoIP Basic Settings .....	41
3.5.2	VoIP Adv Settings .....	43
3.5.3	Multicast Setting .....	47
3.5.4	NAT Settings .....	48
3.5.5	MQTT Settings .....	51
3.5.6	USB Storage .....	52
3.6	Management .....	54
3.6.1	User Manage .....	54
3.6.2	Device Manage .....	54
3.6.3	Log Manage .....	56
3.6.4	Mode Manage .....	57
3.7	Diagnostics.....	58
3.7.1	Network diagnostics .....	58
3.7.2	Loopback Detect .....	59

3.7.3	Self-Diagnosis	60
<b>4</b>	<b>Examples</b>	<b>62</b>
4.1	Internet service	62
4.1.1	Requirement	62
4.1.2	Steps	62
4.2	IPTV service	63
4.2.1	Requirement	63
4.2.2	Steps	64
4.3	VoIP service	66
4.3.1	Requirement	66
4.3.2	Steps	66
4.4	Internet and IPTV service mixed	68
4.4.1	Requirement	68
4.4.2	Steps	68
4.5	Internet, IPTV and VOIP service mixed	71
4.5.1	Requirement	71
4.5.2	Steps	71
4.6	WLAN service	74
4.6.1	Requirement	74
4.6.2	Steps	74
4.7	Update image	76
<b>5</b>	<b>FAQ</b>	<b>77</b>
<b>6</b>	<b>Technical Specifications</b>	<b>78</b>
<b>7</b>	<b>EU Declaration of Conformity</b>	<b>79</b>
<b>8</b>	<b>Conditions of warranty</b>	<b>79</b>

## 1 Safety Instructions



**Read these instructions carefully before connecting the unit**

### ATTENTION

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

### CAUTION

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



#### **To prevent fire, short circuit or shock hazard:**

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



#### **To avoid any risk of overheating:**

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

**To avoid any risk of electrical shocks:**

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

**Warning**

CLASS 1 LASER PRODUCT

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

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

Concerning fibre optic cables:

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

**Maintenance**

Only use a dry soft cloth to clean the cabinet.



Do not use solvent.



For repairing and servicing, refer to qualified personnel.

**Dispose according to your local authority's recycling processes**

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

## 2 Introduction

### 2.1 Product description

TONT-4600 (4\*GE, Wi-Fi6, XPON, HGU ONT) is a broadband access device specially designed to meet the needs of fixed network operators for FTTH. This ONT is based on a high-performance chip solution, supporting XPON dual mode technology (EPON and GPON). With Wi-Fi speeds of up to 3000Mbps, it also supports IEEE 802.11b/g/n/ac/ax Wi-Fi 6 technology and other Layer 2/Layer 3 features, providing data services for carrier grade FTTH applications.

In addition, the ONT also supports the OAM/OMCI protocol and various services of the ONT can be configured and managed on the TRIAX TOLT.

The ONT has high reliability, is easy to manage and maintain and has QoS guarantees for various services. It conforms to a series of international technical standards such as IEEE802.3ah and ITU-T G.984

With a bottom disc fibre structure design to tidy fibre cable, it can be placed on a desktop or wall-mounted, adapting effortlessly to various locations.

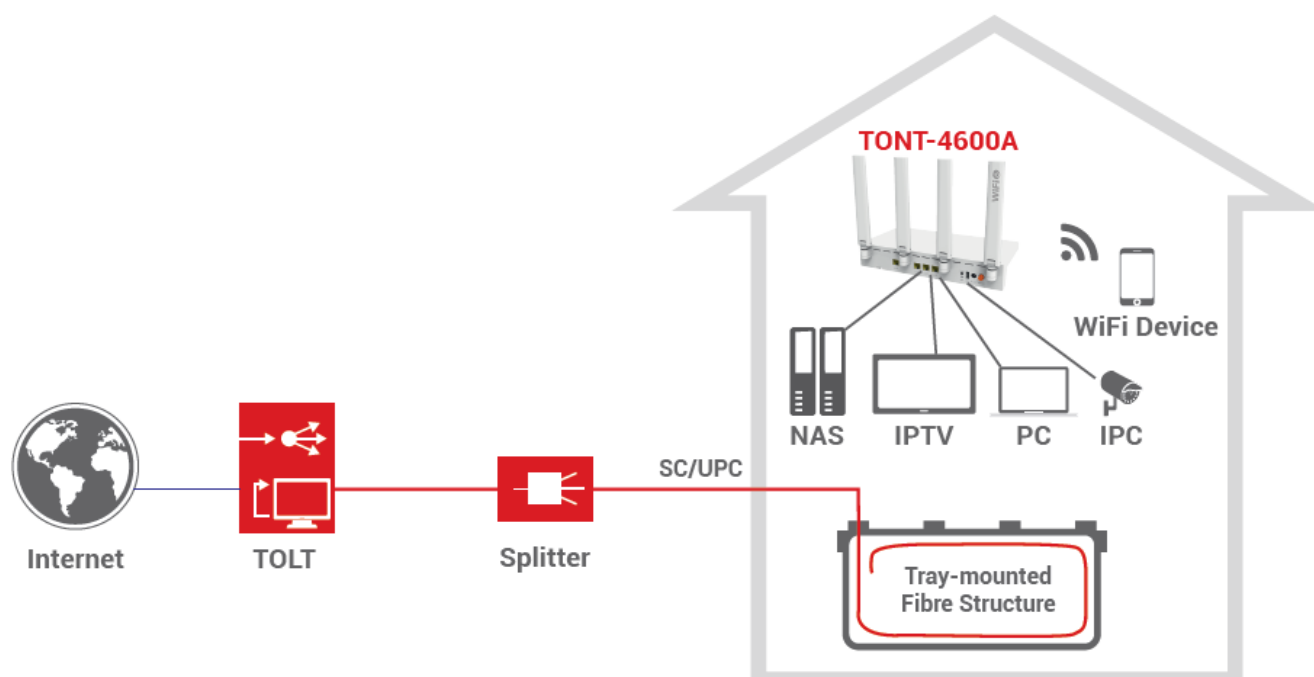
### 2.2 Detailed features

- Detect and exchange PON mode automatically
- 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 802.11ax Wi-Fi(2T2R), 802.11n Wi-Fi(2T2R) and 802.11ac(2T2R) function
- Support NAT, Firewall function
- Support IPv4 and IPv6 dual stack
- The WAN port supports bridge, router and bridge/router mixed mode
- High performance solution
- Next-Gen Gigabit Wi-Fi6 2.4GHz & 5GHz Dual Band Speed up to 3Gbps
- USB3.0 Interface for Shared Storage/Printer
- Fibre cable management tray

### 2.3 Ordering information

Product Name	Article No.	Product Description	Accessories
TONT-4600A	308704	1*XPON + 4*GE + 1USB3.0 + Wi-Fi6	AC-DC power adapter, DC12V/1.5A

## 2.4 Installation schematic example



## 2.5 Front panel



## 2.6 Rear panel



Name	Function
PON	Connect to OLT by SC type fibre connector, single mode optical fibre cable
LAN1-4	Connect to PC or other devices with Ethernet port by Cat cable, RJ-45 connector
FXS	Connect to the telephone with FXS port by telephone wire
WPS	Press WPS button for 4 ~ 7 seconds, HGU starts to pair 2.4G Press WPS button over 7 seconds, HGU starts to pair 5G
RST	Press RST button for less than 6 seconds, device reboots Press RST button for more than 6 seconds but less than 18 seconds, device restores to parts of factory default configuration (like LAN IP, password, SSID, etc...) Press RST button for more than 18 seconds, device restores to factory default configuration
USB	USB3.0 port, connect to USB storage device
DC 12V	Connect with supplied power adapter, DC 12V, 1.5A
ON/OFF	Power supply switch



## 2.7 LEDs



Name	Status	Function
PWR	ON OFF	The device is powered The device is not powered
PON	ON OFF BLINK	The device is registered to the PON system The device is not registered to the PON system The device registration is in progress
LOS	OFF BLINK	The device is receiving optical signal The device does not receive optical signal
WAN	ON OFF	WAN connection No WAN connection
LAN4 LAN3 LAN2 LAN1	ON OFF BLINK	Port is connected properly (LINK) Port is not connected properly Port is sending or/and receiving data (ACT)
2.4G 5G	ON OFF BLINK	WiFi is turned ON WiFi is turned OFF WiFi is turned ON with ongoing data transmission
WPS	OFF BLINK	WiFi is not pairing WiFi is pairing
USB	ON	USB device is connected, but without ongoing data transmission.
	OFF	Device is powered OFF or USB device is not connected.
	Blink	The port is with ongoing data transmission.

## 2.8 First installation

1. Connect the optical fibre cable to the unit:
  - Remove the protective cap of the optical fibre
  - Clean the end of the optical fibre with an optical fibre end cleaner
  - Remove the protective cap of the ONU optical interface (PON interface)
  - Connect the fibre 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 fibre clean
  - Make sure there are no tight bends in the fibre 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 protective cap to guard against dust and moisture when the fibre is not used
2. Apply power to the unit, push the power button
  3. After the ONT is power ON, indicators should light up as for normal operation. Check whether the PWR interface status LED is continuously on. If it is, the connection is normal; otherwise, there is either problem of 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 fibre. 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:

- ONT installed on a horizontal surface (Bench top):
  - o put the ONT 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
- ONT installed on a vertical surface (Hanging on a wall):
  - o you can install the ONT on a vertical surface by using the mounting holes on the bottom of the ONU chassis and two flat-head wood screws
  - o Insert the screws into the wall. The screw positions must be in the same horizontal line and the distance between them must be 145mm. Reserved at least 6mm between the screw caps and the wall
  - o Hang the ONT on the screws through the mounting holes

## 2.9 Setup connection

- Set up wired connection, connect PC with ONT Ethernet port by RJ-45 CAT5 cable.
- Set up wireless connection: connect to the wireless according to the device label information.

## 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 Username and Password

Password: the default login username and password that are given on the product label

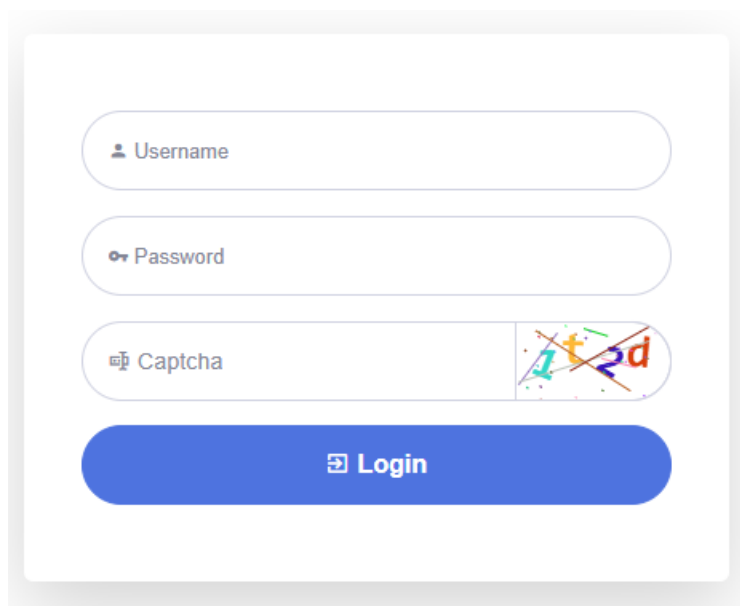
The image shows a web-based login interface. It consists of three input fields stacked vertically: 'Username' with a person icon, 'Password' with a key icon, and 'Captcha' with a colorful distorted text image. Below these fields is a large blue button labeled 'Login' with a right-pointing arrow icon.

Figure 3-1-1: Login

### 3.2 Status

This part shows the main information of 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 network device topology.

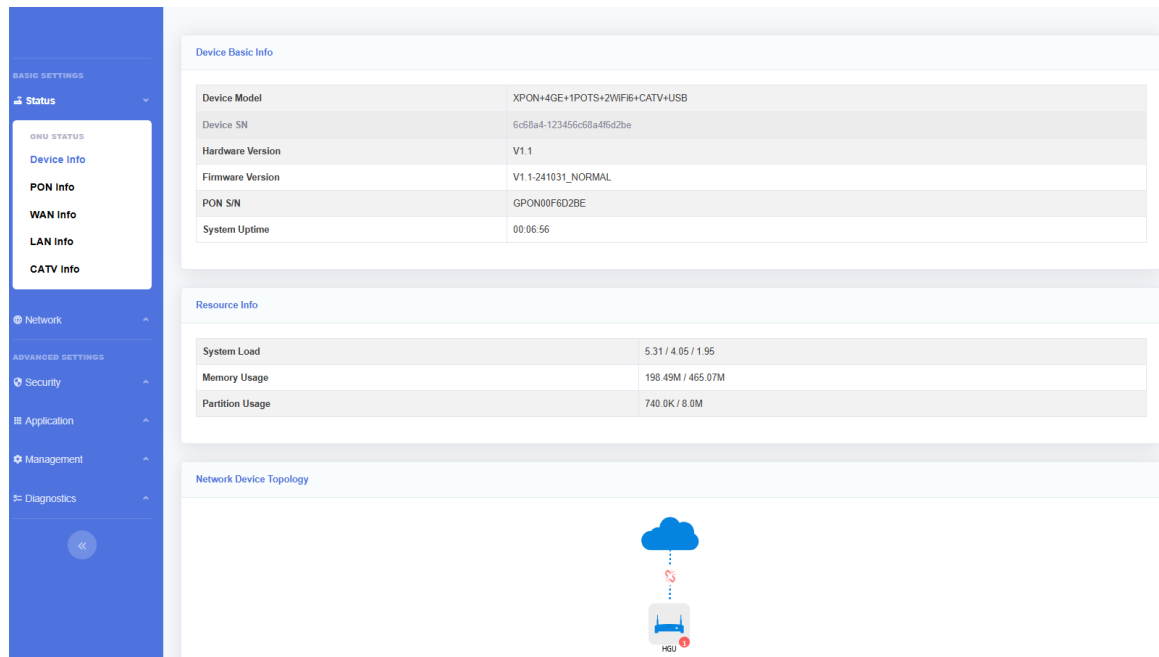


Figure 3-2-1: Device Information

### 3.2.2 PON Info

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

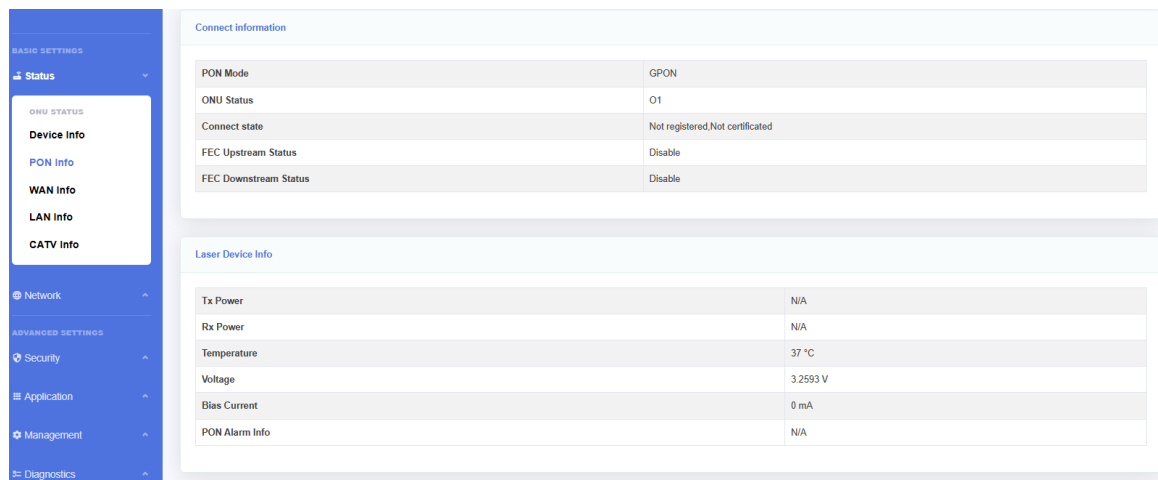


Figure 3-2-2: PON Info

#### 3.2.2.1 Connect information

This page shows the GPON or EPON connection information and FEC information.

Connect information	
PON Mode	GPON
ONU Status	O1
Connect state	Not registered,Not certificated
FEC Upstream Status	Disable
FEC Downstream Status	Disable

Figure 3-2-3: Connection Info

### 3.2.2.2 Laser Device Info

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

Laser Device Info	
Tx Power	N/A
Rx Power	N/A
Temperature	37 °C
Voltage	3.2593 V
Bias Current	0 mA
PON Alarm Info	N/A

Figure 3-2-4: Laser Device Info

### 3.2.2.3 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

Figure 3-2-5: Link Performance Info

### 3.2.3 WAN Info

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

BASIC SETTINGS

⌵

Status

ONU STATUS

Device Info

PON Info

WAN Info

LAN Info

CATV Info

⌵

Network

ADVANCED SETTINGS

Security

Application

Management

Diagnostics

⏪

IPv4 WAN Info

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

IPv4 Network Info

Service Interface	Default Gateway	Primary DNS	Standby DNS
-------------------	-----------------	-------------	-------------

IPv6 WAN Info

Service Interface	VLAN ID	Protocol	MLD	Status	IP Address	Prefix
-------------------	---------	----------	-----	--------	------------	--------

IPv6 Network Info

Service Interface	Default Gateway	Primary DNS	Standby DNS
-------------------	-----------------	-------------	-------------

Remote Manage Info

Connection	NONE
ACS connect request state	NONE
ACS config state	NONE

Figure 3-2-6: WAN Info

### 3.2.3.1 IPv4 Connection Info

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

IPv4 WAN Info

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

IPv4 Network Info

Service Interface	Default Gateway	Primary DNS	Standby DNS
-------------------	-----------------	-------------	-------------

Figure 3-2-7: IPv4 WAN Info

### 3.2.3.2 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 3-2-8: IPv6 WAN Info

### 3.2.3.3 Remote Manage Info

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

Remote Manage Info	
Connection	no inform
ACS connect request state	ACS request success
ACS config state	ACS set success

Figure 3-2-9: Remote Manage Info

### 3.2.3.4 VoIP Info

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

VoIP Info	
Port State	Inactive
Phone Number	
Register Fail Reason	

Figure 3-2-10: VoIP Info

### 3.2.4 LAN Info

This page shows the user information for WLAN and LAN, including WLAN interface, connected wireless client, WLAN and LAN packets, etc.

BASIC SETTINGS

Status

ONU STATUS

Device Info

PON Info

WAN Info

LAN Info

CATV Info

Network

ADVANCED SETTINGS

Security

Application

Management

Diagnostics

LAN Interface Status

Interface	Device Name	MAC Address	IP Address	IPv6 Address	MTU
Local Bridge	br-lan	6C:68:A4:F6:D2:BE	192.168.1.1	fdca:7552:3232::1	1500

LAN Send and Recv

Interface	Device Name	Status	Rate	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dropped (Send)
Port 1	eth0.1	Not Connected	-	0	0	0	0	0	0	0	0
Port 2	eth0.2	Not Connected	-	0	0	0	0	0	0	0	0
Port 3	eth0.3	Connected	100	1764	217765	0	0	2082	1626410	0	0
Port 4	eth0.4	Not Connected	-	0	0	0	0	0	0	0	0

VLAN Status

Interface	Device Name	Port VID	Tagged VID	Untagged VID
Local Bridge	br-lan	1	-	1
Port 1	eth0.1	1	-	1
Port 2	eth0.2	1	-	1
Port 3	eth0.3	1	-	1
Port 4	eth0.4	1	-	1
WLAN AP1-2.4G	ra0	1	-	1
WLAN AP1-5G	rai0	1	-	1

Figure 3-2-11: LAN Info

#### 3.2.4.1 LAN Interface Status

This page shows LAN address and LAN gateway.

LAN Interface Status					
Interface	Device Name	MAC Address	IP Address	IPv6 Address	MTU
Local Bridge	br-lan	6C:68:A4:F6:D2:BE	192.168.1.1	fdca:7552:3232::1	1500

Figure 3-2-12: LAN Interface Status

#### 3.2.4.2 LAN Send and Recv

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

LAN Send and Recv												
Interface	Device Name	Status	Rate	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dropped (Send)	
Port 1	eth0.1	Not Connected	-	0	0	0	0	0	0	0	0	
Port 2	eth0.2	Not Connected	-	0	0	0	0	0	0	0	0	
Port 3	eth0.3	Connected	100	1764	217765	0	0	2082	1626410	0	0	
Port 4	eth0.4	Not Connected	-	0	0	0	0	0	0	0	0	

Figure 3-2-13: LAN Send and Recv

#### 3.2.4.3 VLAN Status

This page shows the VLAN Status of each LAN interface.

VLAN Status				
Interface	Device Name	Port VID	Tagged VID	Untagged VID
Local Bridge	br-lan	1	-	1
Port 1	eth0.1	1	-	1
Port 2	eth0.2	1	-	1
Port 3	eth0.3	1	-	1
Port 4	eth0.4	1	-	1
WLAN AP1-2.4G	ra0	1	-	1
WLAN AP1-5G	rai0	1	-	1

Figure 3-2-14: VLAN Status

#### 3.2.4.4 WLAN Interface Status

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

WLAN Interface Status							
Interface	Device Name	SSID	BSSID	Broadcast	Encryption	Channel	Mode
WLAN AP1-2.4G	ra0	FTTH-D2BE	00:0C:43:26:60:00	Visible	Enabled	Auto	2.4 GHz (B+G+N+AX)
WLAN AP1-5G	rai0	FTTH-5G-D2BE	02:0C:43:46:60:00	Visible	Enabled	Auto	5 GHz (A+N+AC+AX)

Figure 3-2-15: WLAN Interface Status

#### 3.2.4.5 WLAN Send and Receive

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

WLAN Send and Recv									
Interface	Device Name	Packets (Recv)	Bytes (Recv)	Errors (Recv)	Dropped (Recv)	Packets (Send)	Bytes (Send)	Errors (Send)	Dropped (Send)
WLAN AP1-2.4G	ra0	0	0	0	0	0	0	0	0
WLAN AP1-5G	rai0	0	0	0	0	0	0	0	0

Figure 3-2-16: WLAN Interface Statistics

#### 3.2.4.6 Active DHCP Clients

This page shows the lease information of the DHCP server.

Active DHCP Clients			
Hostname	MAC Address	IP Address	Lease Time

Figure 3-2-17: Active DHCP Clients

## 3.3 Network

### 3.3.1 WAN

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



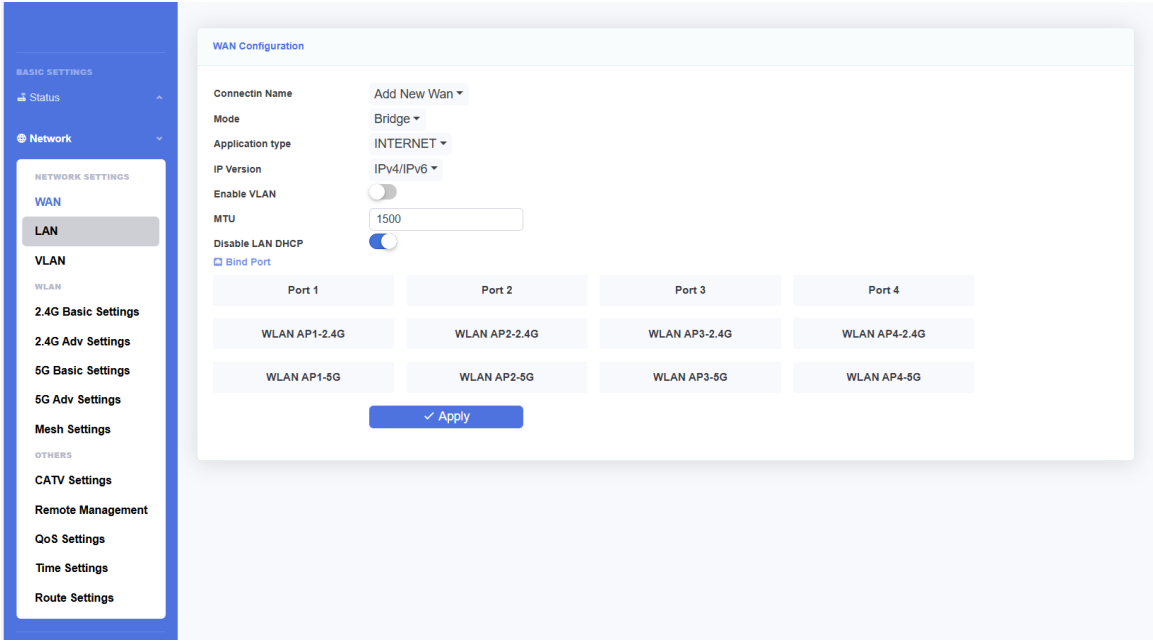


Figure 3-3-1: WAN

3.3.1.1 WAN Configuration

This page allows you to add or modify WAN connections, it is recommended not to configure more than 8 WAN connections.

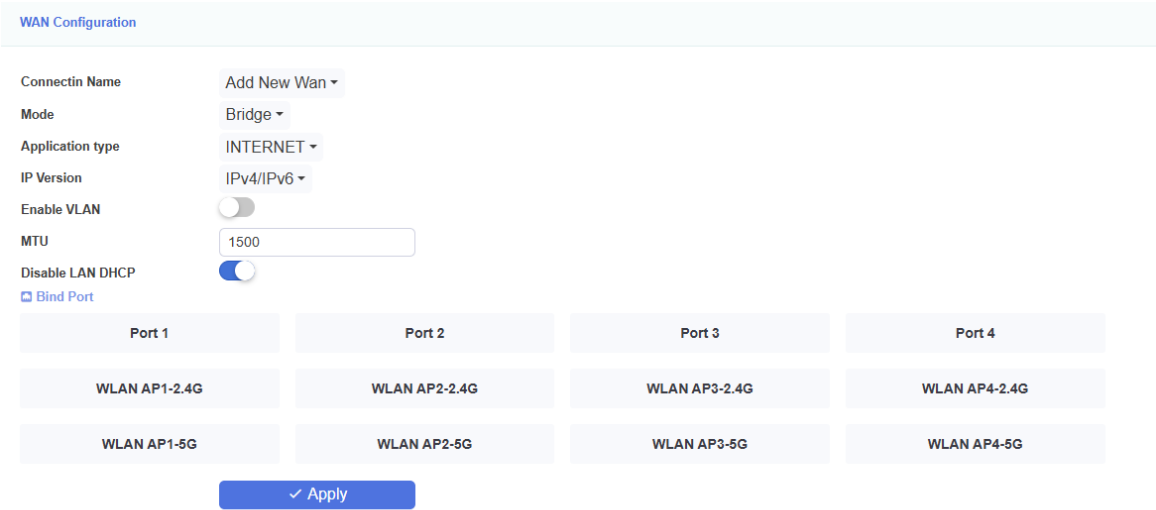


Figure 3-3-2: WAN Configuration

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	<p>Bridge: The LAN ports you have selected in this WAN connection and PON port are in the bridge mode.</p> <p>Route: The LAN ports you have selected in this WAN connection and PON port are in the route mode.</p>
Service Mode	<p>Service mode indicates what the wan connection is used for.</p> <p>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.</p>
IP Version	<p>IPv4: WAN connections use IPv4 protocol.</p> <p>IPv6: WAN connections use IPv6 protocol.</p> <p>IPv4 / IPv6: WAN connections use both IPv4 and IPv6 protocol.</p>
Connection Mode	<p>DHCP: Automatically obtain an IP address from your ISP</p> <p>Static: Set the IP address manually</p> <p>PPPoE: Select this option if your ISP uses PPPoE</p>
Disable LAN DHCP	<p>Checked: LAN DHCP will not work at the port which binds with the WAN.</p> <p>Unchecked: LAN DHCP will work at the port which binds with the WAN.</p>
Enable NAT	<p>checked: enable NAT function</p> <p>unchecked: disable NAT function</p>
Enable VLAN	<p>unchecked: In this wan connection, the packets transmitted by the PON port without VLAN tag.</p> <p>checked: In this wan connection, the packets transmitted by the PON port with VLAN tag.</p> <p>VLAN ID: input the VLAN ID you want to set.</p> <p>802.1p: select the port priority you want to set.</p>
MTU	<p>MTU: max transfer unit.</p> <p>Default Value: 1492 in route PPPoE mode, 1500 in other modes.</p>
Request DNSv4	<p>Enable: DHCP server assigns DNS.</p> <p>Disable: set DNS manually.</p>
Bind Port	Showing which LAN port or SSID the wan connection has included.

3.3.2 LAN

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

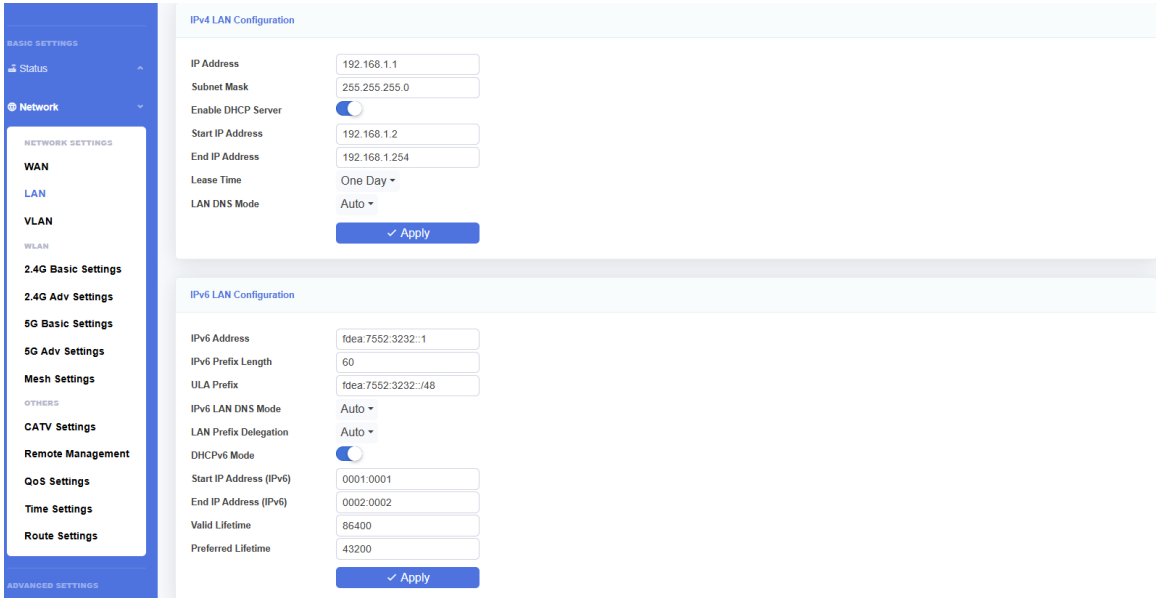


Figure 3-3-3: LAN

3.3.2.1 IPv4 LAN Configuration

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

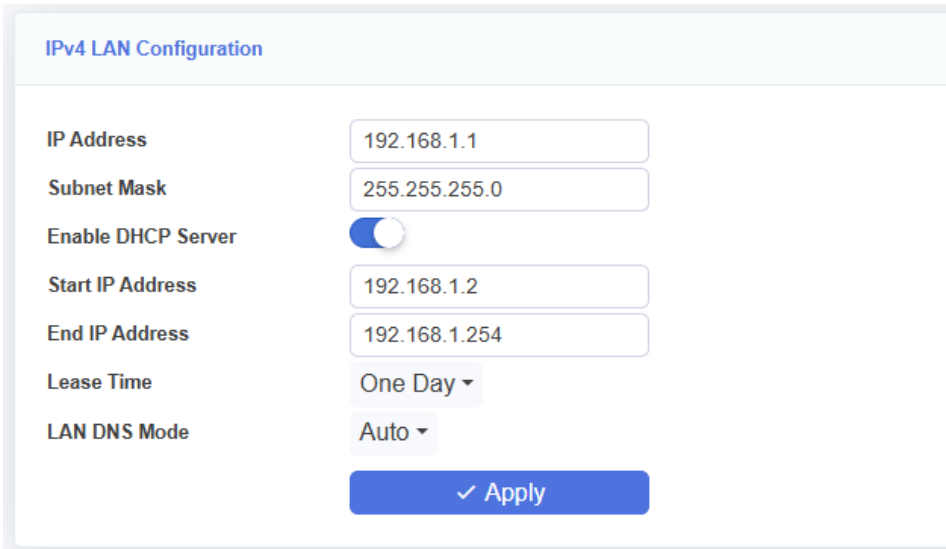


Figure 3-3-4: IPv4 LAN Configuration

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

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

### 3.3.2.2 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.

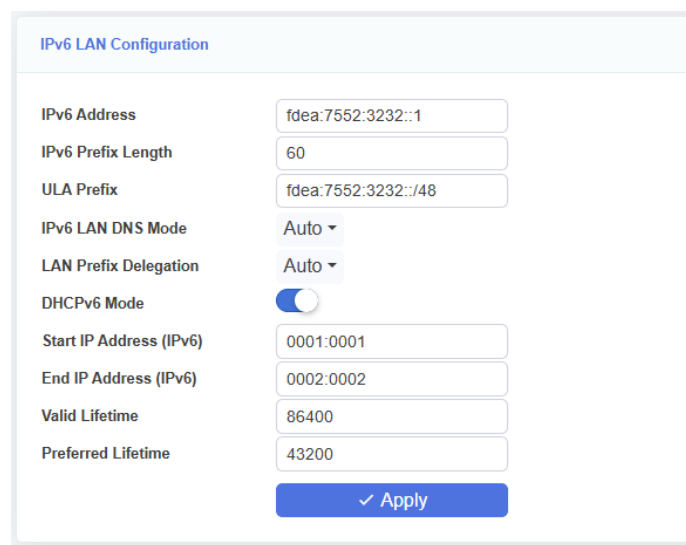


Figure 3-3-5: IPv6 LAN Configuration

### 3.3.2.3 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.

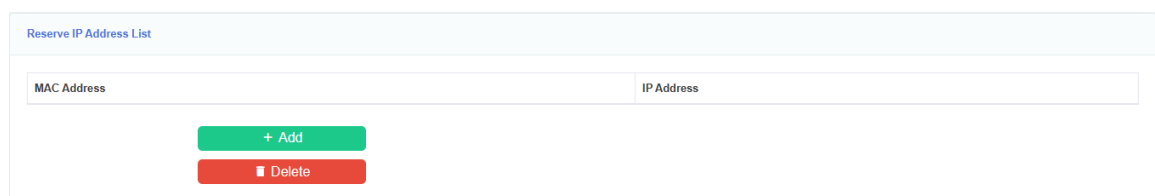


Figure 3-3-6: Reserve IP Address List

### 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

200

✓ Apply

Figure 3-3-7: RA Configuration

3.3.3 VLAN

This page is used to configure rule of LAN interface VLAN.

RADIO SETTINGS

Status

Network

NETWORK SETTINGS

WAN

LAN

VLAN

WLAN

Bridge VLAN Filtering Config

Enable VLAN Filtering

VLAN ID	Port VID	Tagged Port	Untagged Port
1	br-lan / eth0.1 / eth0.2 / eth0.3 / eth0.4 / ra0 / ra0	-	br-lan / eth0.1 / eth0.2 / eth0.3 / eth0.4 / ra0 / ra0

+ Add / Edit

Delete

✓ Apply

Add VLAN

Local Bridge (br-lan)

VLAN ID

2 - 4095

VLAN Mode

Untagged

Port 1 (eth0.1)

VLAN Mode

Disable

Port 2 (eth0.2)

VLAN Mode

Disable

Port 3 (eth0.3)

VLAN Mode

Disable

Port 4 (eth0.4)

VLAN Mode

Disable

WLAN AP1-2.4G (ra0)

VLAN Mode

Disable

WLAN AP2-2.4G (ra1)

VLAN Mode

Disable

WLAN AP3-2.4G (ra2)

VLAN Mode

Disable

VLAN Mode

Disable

VLAN Mode

Disable

WLAN AP1-2.4G (ra0)

VLAN Mode

Disable

WLAN AP2-2.4G (ra1)

VLAN Mode

Disable

WLAN AP3-2.4G (ra2)

VLAN Mode

Disable

WLAN AP4-2.4G (ra3)

VLAN Mode

Disable

WLAN AP1-5G (rai0)

VLAN Mode

Disable

WLAN AP2-5G (rai1)

VLAN Mode

Disable

WLAN AP3-5G (rai2)

VLAN Mode

Disable

WLAN AP4-5G (rai3)

VLAN Mode

Disable

VLAN Mode

Disable

✓ Apply

Figure 3-3-8: VLAN

Interface	Illustration
Local Bridge (br-lan)	LAN IP access interface, must ensure Untagged vlan traffic
Port 1(eth0.1) Port 2(eth0.2) ... WLAN AP3-5G(rai2) WLAN AP4-5G(rai3)	LAN port interface. In other to choose which LAN port to configure the VLAN rule.

Parameters	Illustration
VLAN Mode	Configure different VLAN rules for HGU interfaces
Tagged	Only can transmit traffic with specific VLAN Tag
Untagged	Only can transmit traffic without VLAN Tag
Disable	Not control interface VLAN rules
Untagged+Pvid	When traffic without VLAN Tag, add the Pvid value as VLAN Tag
Tagged+Pvid	Only can transmit traffic with specific VLAN Tag and when traffic without VLAN Tag, add the Pvid value as VLAN Tag

### 3.3.4 2.4G Basic Settings

This page is used to configure WIFI (2.4G) parameters. On each page, after configured you should click “Submit” button to save it. The device supports WiFi6, if the end device also supports WiFi6, it is recommended to configure the Band to 2.4GHz (B+G+N+AX).

Figure 3-3-9: 2.4G Basic Settings

#### 3.3.4.1 2.4G Basic Setting

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

2.4G Basic Settings

Disable WLAN Interface

☐

Band Steering

☐

Band

2.4 GHz (B+G+N+AX) ▾

SSID

FTTH-D2BE

Cancel Broadcast

☐

Block Relay

☐

WMM

☒

Channel Width

40MHz ▾

Channel Number

Auto ▾

Radio Power (%)

100% ▾

Regdomain

(8) CN ▾

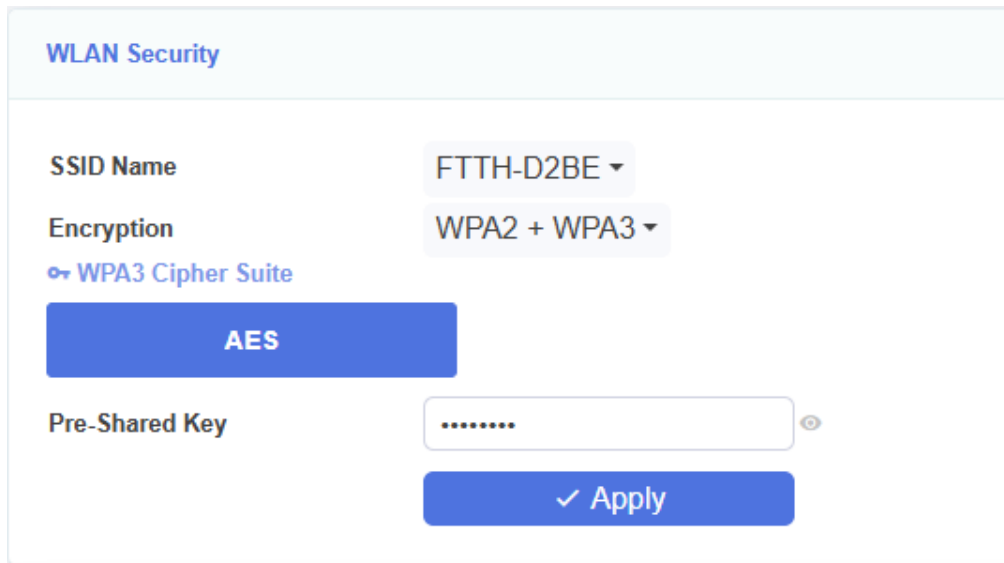
✓ Apply

Figure 3-3-10: 2.4G Basic Settings

Parameter	Illustration
Disable WLAN Interface	Enable or Disable WLAN.
Band Steering	Combine 2.4G Wi-Fi and 5G Wi-Fi for use.
Band	Choose 2.4G Wi-Fi band. This device supports IEEE802.11ax.
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	Wi-Fi 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 Wi-Fi 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.

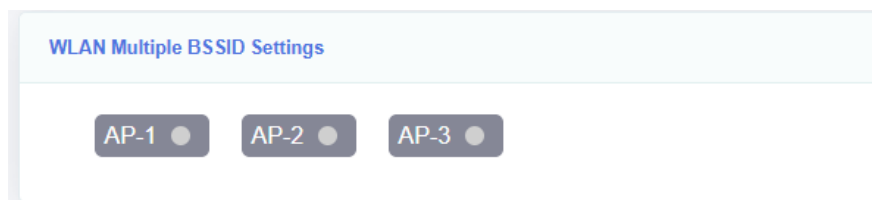


The 'WLAN Security' configuration page features a light blue header with the title 'WLAN Security'. Below the header, the 'SSID Name' is set to 'FTTH-D2BE' with a dropdown arrow. The 'Encryption' is set to 'WPA2 + WPA3' with a dropdown arrow. A link 'WPA3 Cipher Suite' is visible. A large blue button labeled 'AES' is present. The 'Pre-Shared Key' field is masked with dots and has a toggle icon. A blue 'Apply' button with a checkmark is at the bottom.

Figure 3-3-11: WLAN Security

### 3.3.4.3 WLAN Multiple BSSID Settings

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

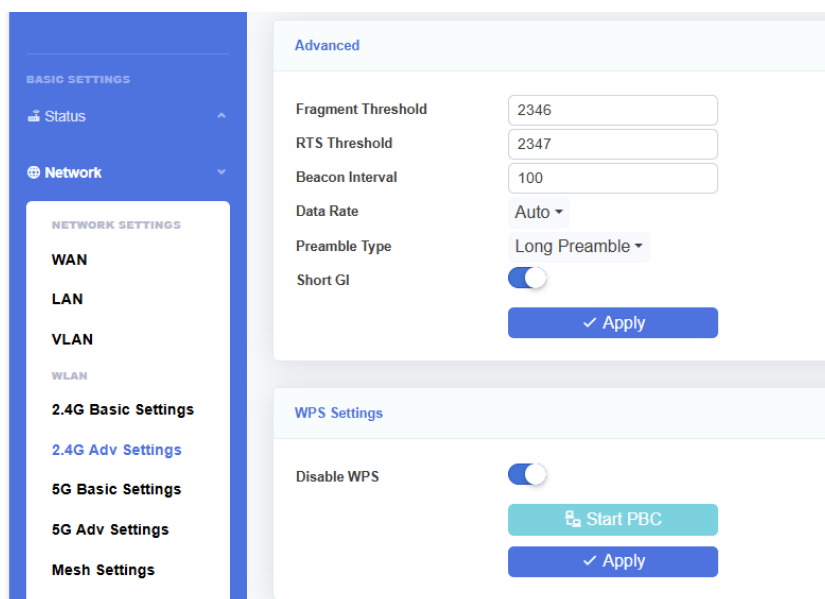


The 'WLAN Multiple BSSID Settings' page has a light blue header with the title 'WLAN Multiple BSSID Settings'. Below the header, there are three toggle switches labeled 'AP-1', 'AP-2', and 'AP-3', all of which are currently turned off.

Figure 3-3-12: WLAN Multiple BSSID Settings

### 3.3.5 2.4G Adv Settings

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.



The '2.4G Adv Settings' page is part of a larger settings interface. On the left is a sidebar with 'BASIC SETTINGS' (Status, Network) and 'NETWORK SETTINGS' (WAN, LAN, VLAN, WLAN, 2.4G Basic Settings, 2.4G Adv Settings, 5G Basic Settings, 5G Adv Settings, Mesh Settings, OTHERS). The main area has a light blue header 'Advanced'. It contains several settings: 'Fragment Threshold' (2346), 'RTS Threshold' (2347), 'Beacon Interval' (100), 'Data Rate' (Auto), 'Preamble Type' (Long Preamble), and 'Short GI' (toggle on). A blue 'Apply' button is below. Below this is a 'WPS Settings' section with 'Disable WPS' (toggle on), a 'Start PBC' button, and another blue 'Apply' button.

Figure 3-3-13: 2.4G Adv Settings



### 3.3.5.1 Advanced

This page allows you to make settings related to the advanced parameters of the wireless network.

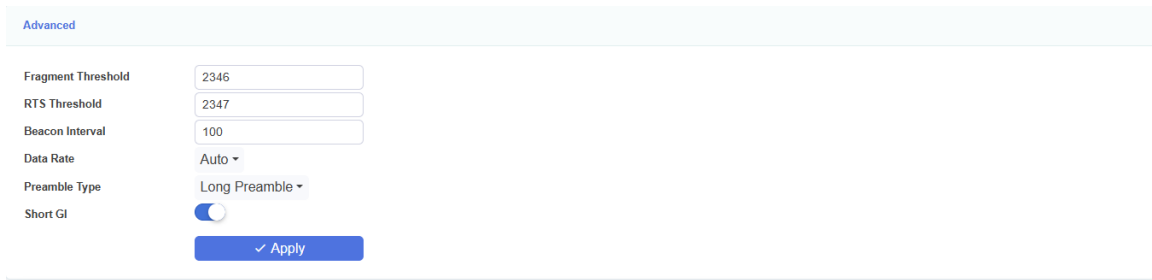


Figure 3-3-14: Advanced

### 3.3.5.2 WPS Settings

These settings allow you to configure WPS setting.



Figure 3-3-15: WPS Settings

## 3.3.6 5G Basic Settings

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).

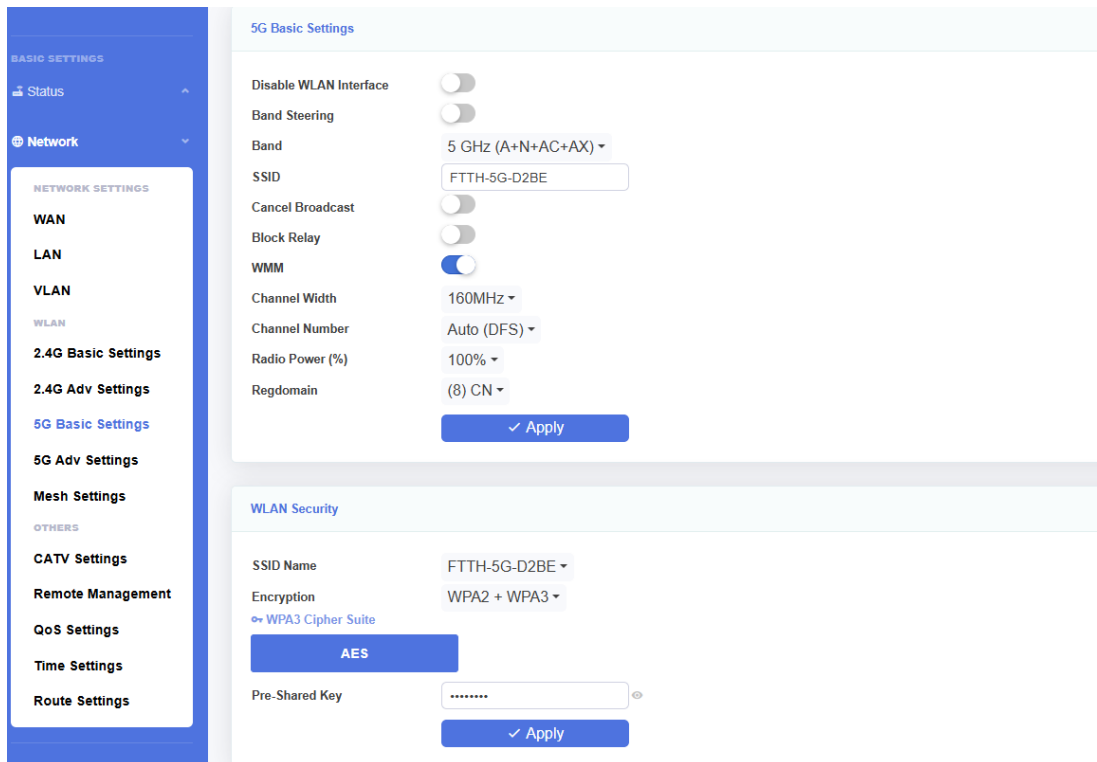


Figure 3-3-16: 5G

### 3.3.6.1 5G 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 Basic Settings

Disable WLAN Interface

Band Steering

Band

SSID

Cancel Broadcast

Block Relay

WMM

Channel Width

Channel Number

Radio Power (%)

Regdomain


✓ Apply

Figure 3-3-17: 5G Basic Settings

Parameter	Illustration
Disable WLAN Interface	Enable or Disable WLAN.
Band Steering	Combine 2.4G WiFi and 5G WiFi for use.
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.

### 3.3.6.2 WLAN security

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



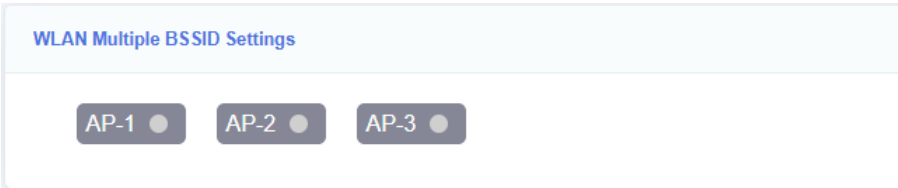
The **WLAN Security** page contains the following fields and controls:

- SSID Name:** A dropdown menu showing "FTTH-5G-D2BE".
- Encryption:** A dropdown menu showing "WPA2 + WPA3".
- WPA3 Cipher Suite:** A link to expand the cipher suite options.
- AES:** A blue button to select the AES cipher suite.
- Pre-Shared Key:** A text input field with masked characters (dots) and a toggle icon to show/hide the key.
- Apply:** A blue button with a checkmark to save the settings.

Figure 3-3-18:5G WLAN Security

### 3.3.6.3 WLAN Multiple BSSID Settings

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



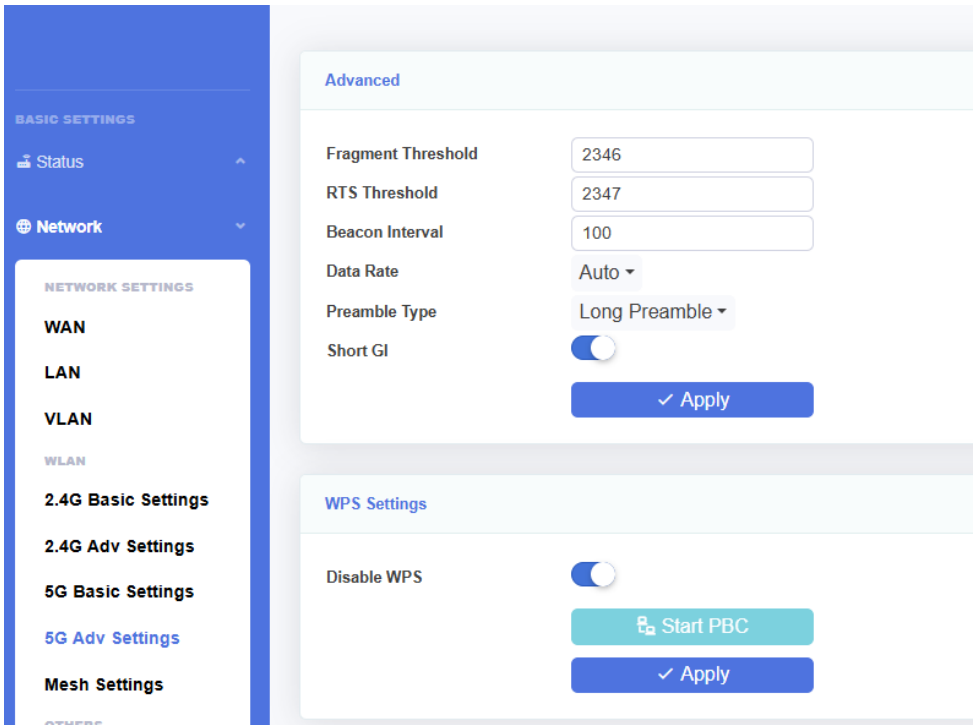
The **WLAN Multiple BSSID Settings** page features three toggle switches for configuring multiple AP parameters:

- AP-1:** A grey toggle switch.
- AP-2:** A grey toggle switch.
- AP-3:** A grey toggle switch.

Figure 3-3-19: WLAN Multiple BSSID Settings

### 3.3.7 5G Adv Settings

This page allows you to make settings related to the advanced parameters of the wireless network



The **5G Adv Settings** page is divided into two main sections:

- Advanced:** Contains several configuration fields:
  - Fragment Threshold:** Input field with value 2346.
  - RTS Threshold:** Input field with value 2347.
  - Beacon Interval:** Input field with value 100.
  - Data Rate:** Dropdown menu set to "Auto".
  - Preamble Type:** Dropdown menu set to "Long Preamble".
  - Short GI:** A toggle switch that is currently turned on.
  - Apply:** A blue button with a checkmark.
- WPS Settings:**
  - Disable WPS:** A toggle switch that is currently turned on.
  - Start PBC:** A light blue button with a PBC icon.
  - Apply:** A blue button with a checkmark.

A sidebar on the left shows the navigation menu with options: BASIC SETTINGS, Status, Network, NETWORK SETTINGS, WAN, LAN, VLAN, WLAN, 2.4G Basic Settings, 2.4G Adv Settings, 5G Basic Settings, 5G Adv Settings (highlighted), and Mesh Settings.

Figure 3-3-20:5G Adv Settings

### 3.3.7.1 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.

Figure 3-3-21: Advanced

### 3.3.7.2 WPS Settings

These settings allow you to configure WPS setting.

Figure 3-3-22: WPS Settings

### 3.3.8 Mesh Settings

This page allows you to enable or disable the HGU as a Mesh controller.

Figure 3-3-23: Mesh Settings

3.3.9 Remote Management

This page allows you to configure Tr069-related parameters or the parameters when registering the OLT.

BASIC SETTINGS

Status

Network

NETWORK SETTINGS

WAN

LAN

VLAN

WLAN

2.4G Basic Settings

2.4G Adv Settings

5G Basic Settings

5G Adv Settings

Mesh Settings

OTHERS

CATV Settings

Remote Management

QoS Settings

Time Settings

Route Settings

ADVANCED SETTINGS

Security

Application

TR069 Client Configuration

EnableRemote Management

✓ Apply

LOID Config

LOID

123456789

Password

.....

✓ Apply

PonPwd Config

GPON SN

GPON00F6D2BE

Password

.....

✓ Apply

STUN Configuration

Enable

STUN Server

stun1.l.google.com

STUN Server Port

19302

STUN Username

STUN Password

UDPConReqAddress

✓ Apply

Figure 3-3-25: Remote Management

3.3.9.1 TR069 Client Configuration

This page allows you to configure TR069 connection parameters.

Figure 3-3-26: TR069 Client Configuration

Parameter	Illustration
Server URL	Server provider's ACS server.
Username	Authentication username for HGU connects to ACS server.
Password	Authentication password for HGU connects to ACS server.
Periodic Report	Switch of inform interval.
Periodic Report Interval	Reconnection interval. HGU will verify connection with ACS server when inform interval times up.
Connect Request Username	Authentication username for ACS connects to HGU.
Connect Request Password	Authentication password for ACS connects to HGU.

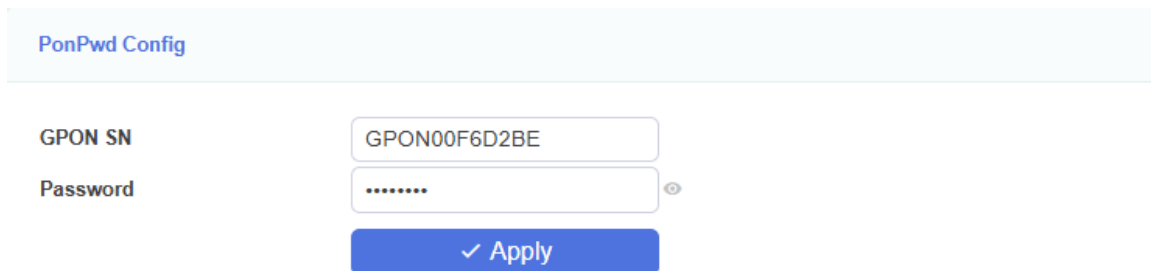
### 3.3.9.2 LOID Config

LOID is used for PON authentication.

Figure 3-3-27: LOID Config

### 3.3.9.3 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.

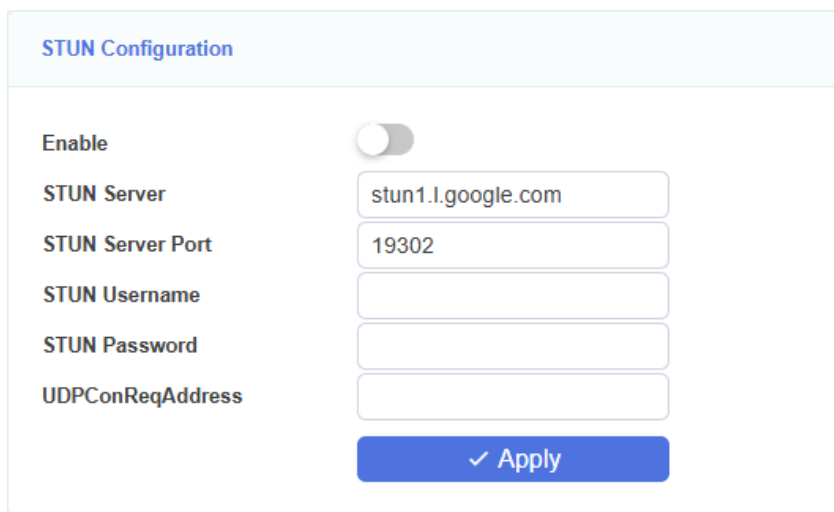


The PonPwd Config interface shows a form with two input fields: "GPON SN" with the value "GPON00F6D2BE" and "Password" with masked characters "\*\*\*\*\*". Below the fields is a blue button labeled "✓ Apply".

Figure 3-3-28: PonPwd Config

### 3.3.9.4 STUN Configuration

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

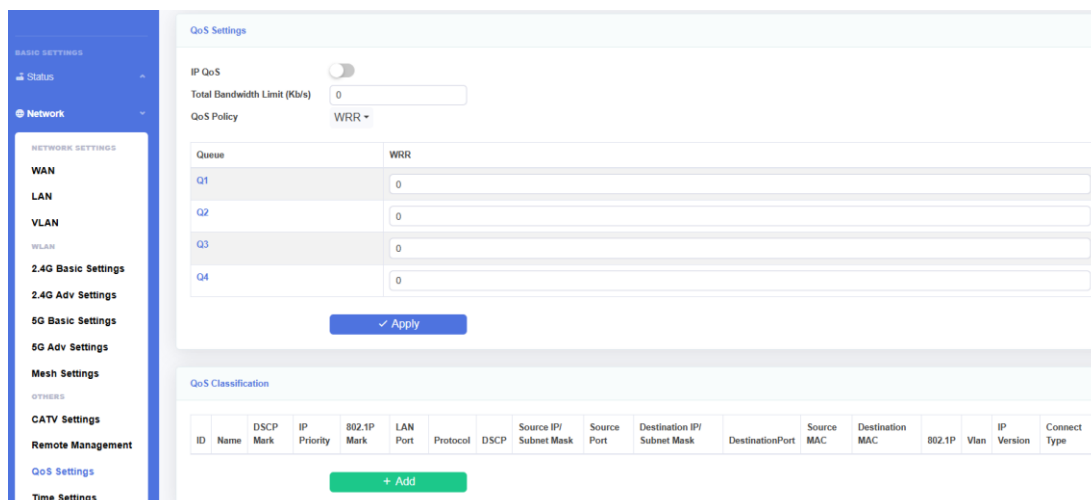


The STUN Configuration interface includes a toggle switch for "Enable" (currently off). Below it are input fields for "STUN Server" (stun1.l.google.com), "STUN Server Port" (19302), "STUN Username", "STUN Password", and "UDPConReqAddress". A blue button labeled "✓ Apply" is at the bottom.

Figure 3-3-29: STUN Configuration

### 3.3.10 QoS Settings

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



The QoS Settings interface is divided into two main sections. The top section, "QoS Settings", includes a toggle for "IP QoS" (off), a "Total Bandwidth Limit (Kb/s)" field (0), and a "QoS Policy" dropdown (WRR). Below this is a table for queue configuration with columns "Queue" and "WRR". The bottom section, "QoS Classification", features a table with columns: ID, Name, DSCP Mark, IP Priority, 802.1P Mark, LAN Port, Protocol, DSCP, Source IP/Subnet Mask, Source Port, Destination IP/Subnet Mask, Destination Port, Source MAC, Destination MAC, 802.1P, Vlan, IP Version, and Connect Type. A green "+ Add" button is at the bottom of the classification table.

Figure 3-3-30: QoS Settings

### 3.3.10.1 QoS Settings

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 Settings

IP QoS ☐

Total Bandwidth Limit (Kb/s)

QoS Policy WRR ▾

Queue	WRR
Q1	<input type="text" value="0"/>
Q2	<input type="text" value="0"/>
Q3	<input type="text" value="0"/>
Q4	<input type="text" value="0"/>

✓ Apply

Figure 3-3-31: QoS Settings

### 3.3.10.2 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	Destination Port	Source MAC	Destination MAC	802.1P	Vlan	IP Version	Connect Type
<span>+ Add</span>																	

Figure 3-3-32: QoS Classification

Add IP QoS Traffic Shaping Rule

IP protocol version IPv4 ▾

Flow control type name

Specify IP Priority Tags Queue 1 ▾

DSCP/TC Remark Default(000000) ▾

802.1p Remark NONE ▾

Mode Selection General mode ▾

Physical LAN Port None ▾

Protocol None ▾

DSCP Check Default(000000) ▾

Vlan

802.1p Priority NONE ▾

Source IP Address

Source subnet mask

Destination IP Address

Destination subnet mask

Physical LAN Port None ▾

Protocol None ▾

DSCP Check Default(000000) ▾

Vlan

802.1p Priority NONE ▾

Source IP Address

Source subnet mask

Destination IP Address

Destination subnet mask

Source start port

Source end port

Destination start port

Destination end port

Source MAC

Destination MAC

✓ Apply

Figure 3-3-33: Add IP QoS Traffic Shaping Rule



Parameter	Illustration
IP protocol version	Select IPv4 or IPv6.
Flow control type name	Input this rule name.
Specify IP Priority Tags	Select queue.
DSCP/TC Remark	Select DSCP tag.
802.1p Remark	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.
Vlan	Select VLAN.
802.1p Priority	Input 802.1p Priority.
Source IP Address	Input source IP address.
Source subnet mask	Input the source subnet mask.
Destination IP Address	Input destination IP address.
Destination subnet mask	Input the destination subnet mask.
Source start port	Input source start port.
Source end port	Input source end port
Destination start port	Input destination start port.
Destination end port	Input destination end port
Source MAC	Input source MAC (xx:xx:xx:xx:xx:xx).
Destination MAC	Input destination MAC (xx:xx:xx:xx:xx:xx).

### 3.3.11 Time Settings

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.

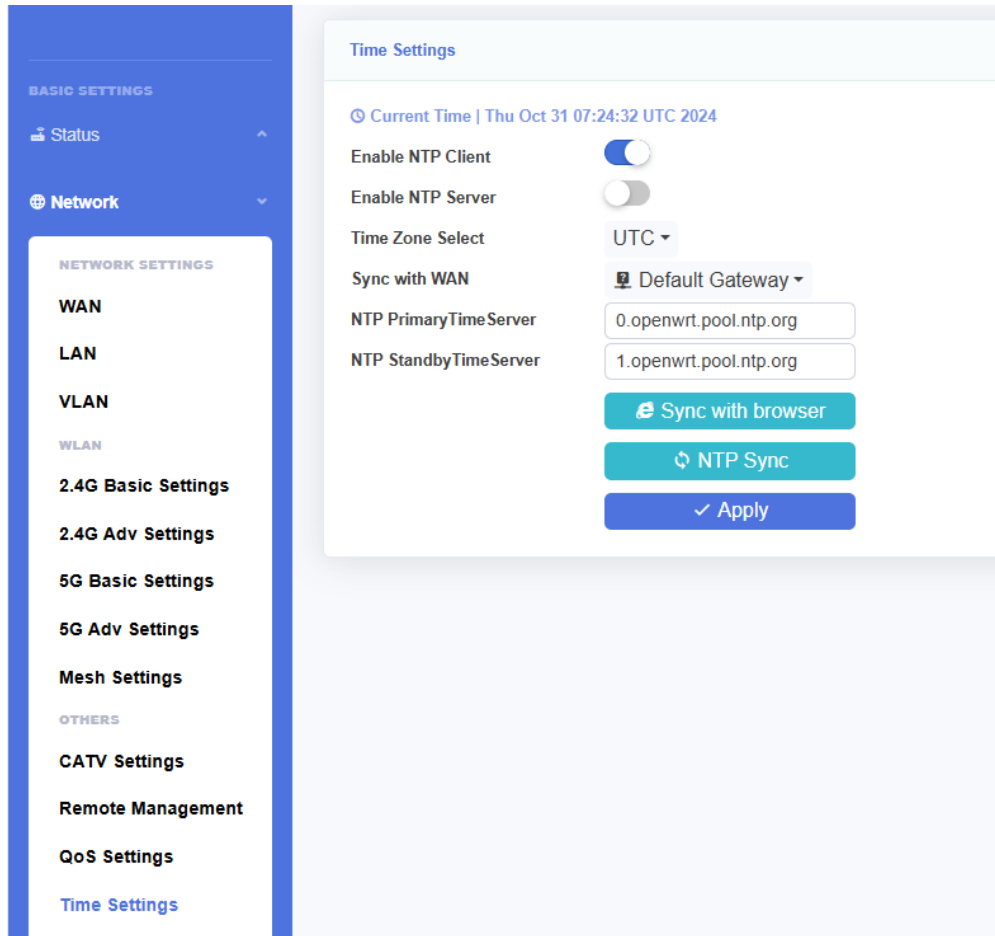


Figure 3-3-34: Time Settings

### 3.3.12 Route Settings

This page allows you to configure static route-related configurations, click “Add” to configure routing rules.

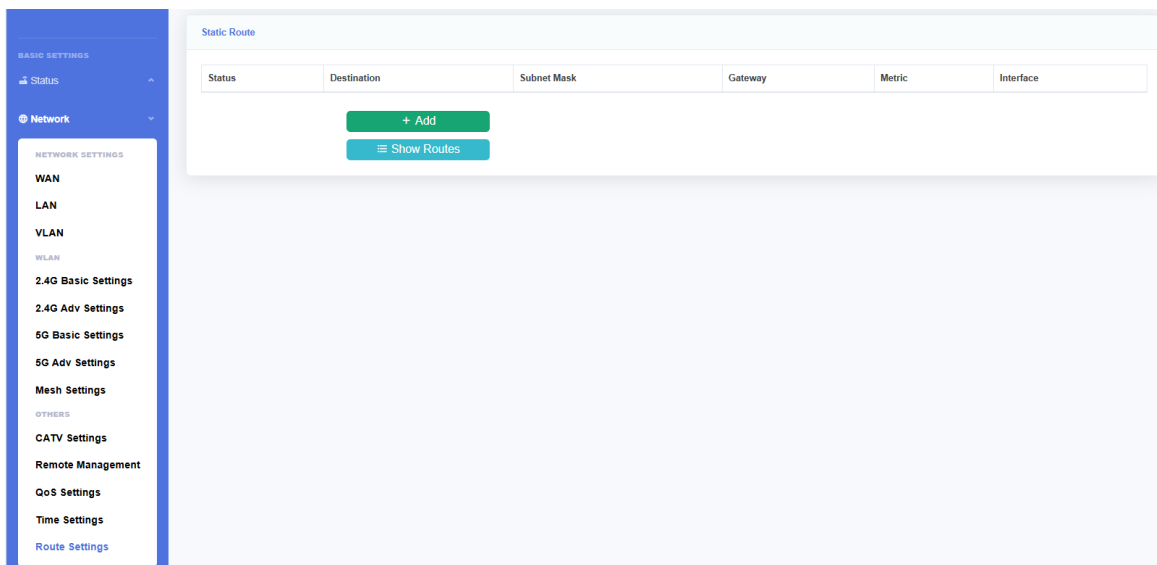


Figure 3-3-35: Route Settings

#### 3.3.12.1 Static Route

This page allows you to configure static routing by clicking "Add" to configure routing rules.

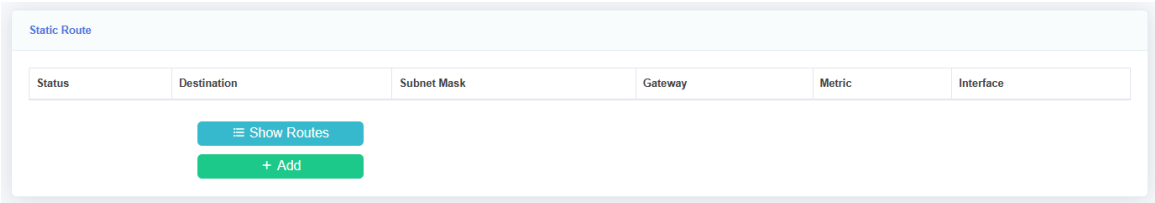


Figure 3-3-36: Static Route

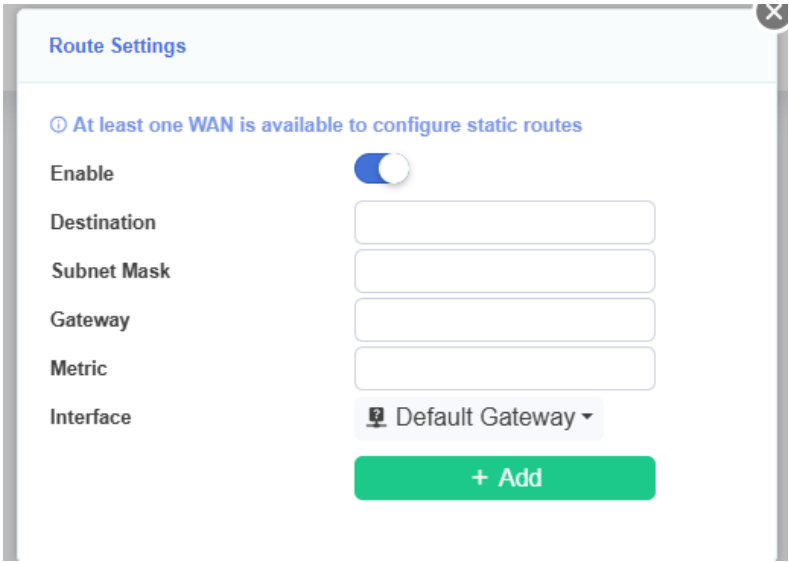


Figure 3-3-37: Route Settings

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 Firewall

This page allows you to configure the firewall level and login privilege.

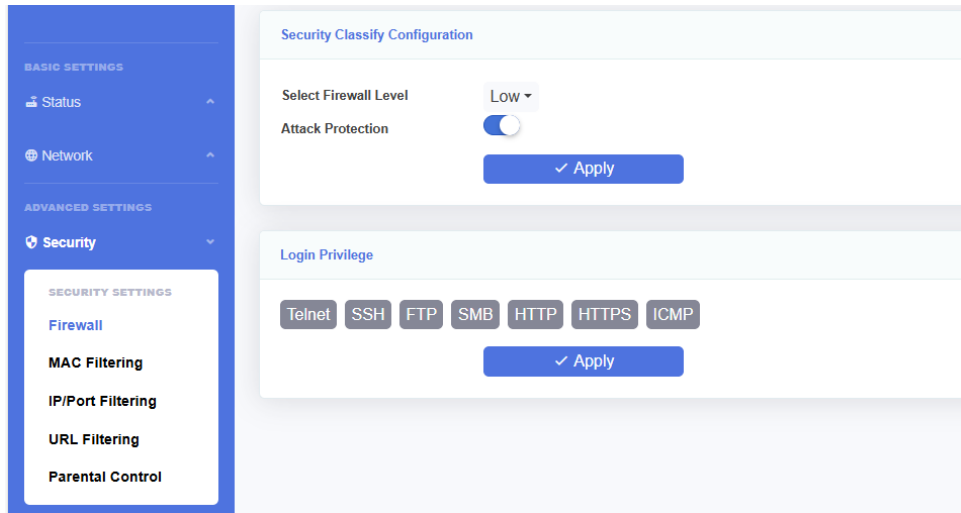


Figure 3-4-1: Firewall

#### 3.4.1.1 Security Classify Configuration

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

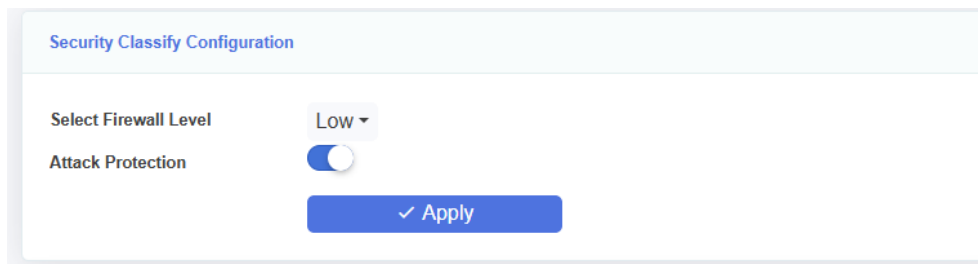


Figure 3-4-2: Security Classify Configuration

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

#### 3.4.1.2 Login Privilege

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

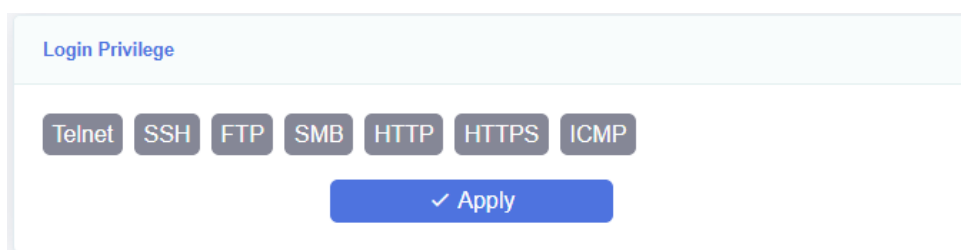


Figure 3-4-3: Login Privilege

### 3.4.2 MAC Filtering

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

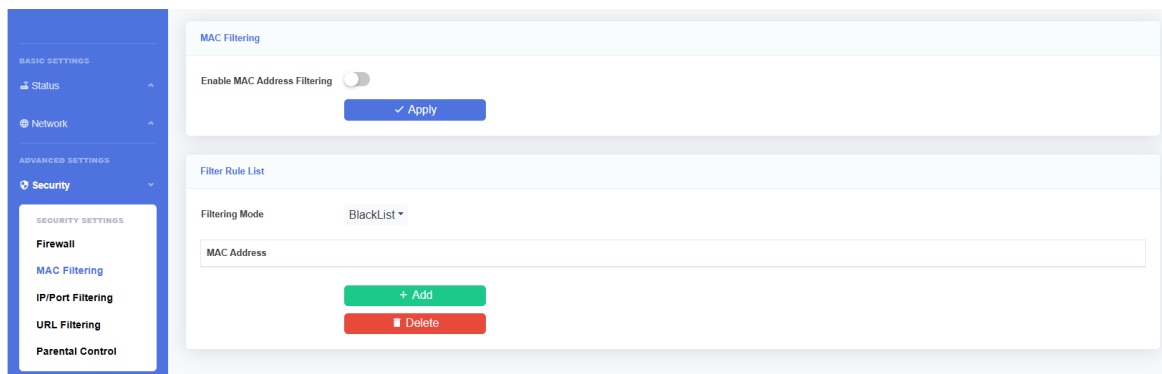


Figure 3-4-4: MAC Filtering

Parameter	Illustration
Enable Mac Address Filtering	unchecked: Disable Mac Filter. checked: Enable Mac Filter.
Filtering Mode	Blacklist: MAC Address in the list will be forbidden, and others will be accessed. Whitelist: 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.

### 3.4.3 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. Blacklist and whitelist take effect simultaneously.

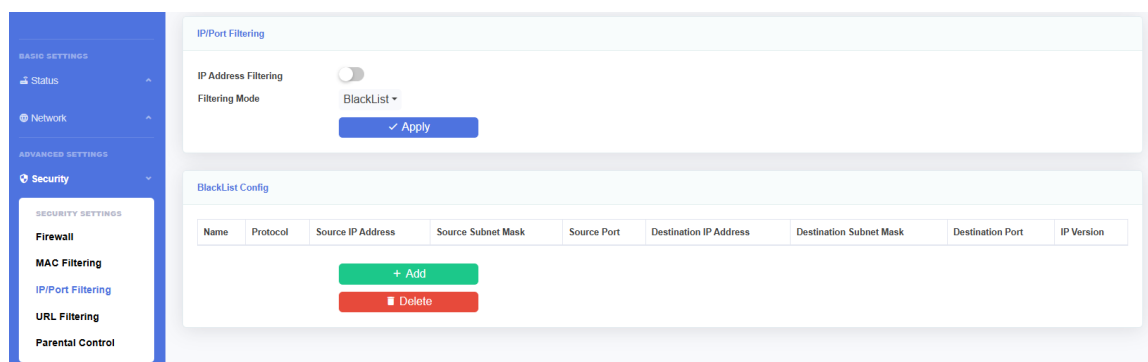


Figure 3-4-5: Ip/Port Filtering

The screenshot shows a configuration window titled "Add IP/Port Filter - Out". It contains the following fields and controls:

- Filter Name: Text input field.
- IP Version: Dropdown menu showing "IPv4".
- Protocol: Dropdown menu showing "TCP/UDP".
- Source Start Address: Text input field.
- Source End Address: Text input field.
- Source subnet mask: Text input field.
- Destination Start Address: Text input field.
- Destination End Address: Text input field.
- Destination subnet mask: Text input field.
- Source start port: Text input field.
- Source end port: Text input field.
- Destination start port: Text input field.
- Destination end port: Text input field.
- Apply: Blue button with a checkmark icon.

Figure 3-4-6: Add IP/Port Filter - Out

Parameter	Illustration
IP Address Filtering	Switch of IP/port filtering.
Filter Mode	<b>Blacklist:</b> Rule in the list will be forbidden, and others will be accessed. <b>Whitelist:</b> 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 Start Address	Input the source start IP address you want to configure in the rule.
Source End Address	Input the source end 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 Start Address	Input the destination start IP address you want to configure in the rule.
Destination Start Address	Input the destination start 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 start Port	Input the source start port you want to configure in the rule.
Source end Port	Input the source end port you want to configure in the rule.
Destination start Port	Input the destination start port you want to configure in the rule.
Destination end Port	Input the destination end port you want to configure in the rule.

3.4.4
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.

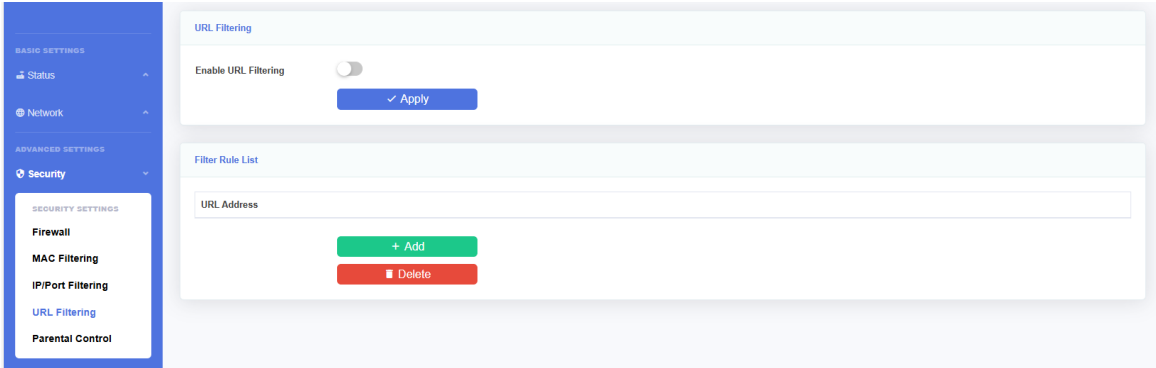


Figure 3-4-7: URL Filtering

Parameter	Illustration
Enable URL Filtering	Enable or Disable URL Filter.
Filtering Mode	Blacklist: URL in the list will be forbidden, and others will be accessed. Whitelist: 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.

3.4.5
Parental Control

This page allows you to configure Parental control. After configure finish on each page, please click “Apply” button to take effect and save it.

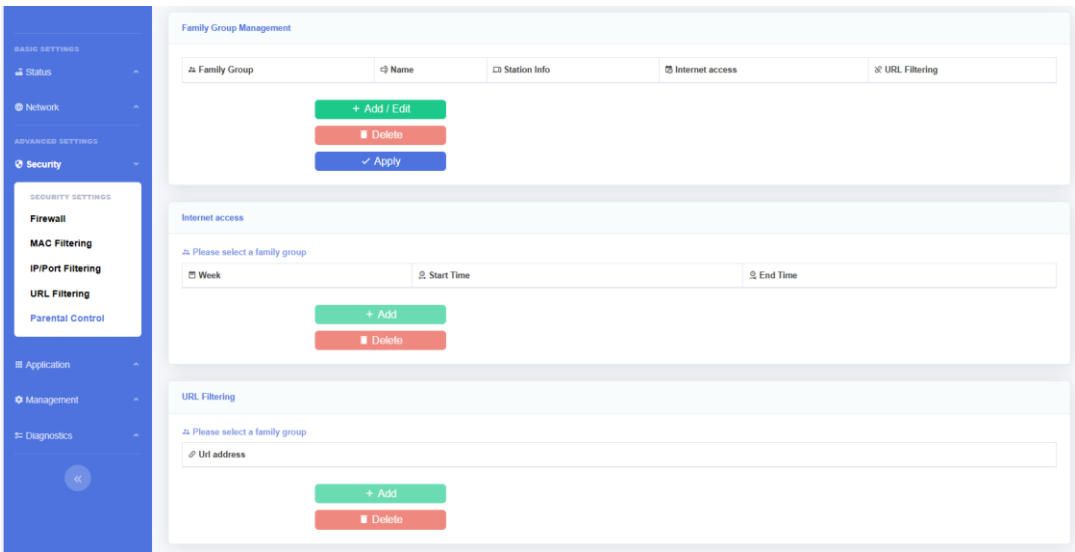


Figure 3-4-8: Parental Control

### 3.4.5.1 Family Group Management

This page allows you to configure the family group member. When clicking "+Add/Edit", a list of family group members will pop up, the HGU will automatically identify all devices currently connected to the HGU also. You can select family members to create family group.

The screenshot shows the 'Family Group Management' interface. At the top, there's a header 'Family Group Management'. Below it, there's a table with columns: 'Family Group', 'Name', 'Station Info', 'Internet access', and 'URL Filtering'. Below the table, there are three buttons: '+ Add / Edit' (green), 'Delete' (red), and 'Apply' (blue). A modal window titled 'Add Family Group' is open. It contains a 'Family Group' dropdown set to '1', a 'Name' text input, and a message: 'Please select devices you want to join the family group from the device list'. Below this is a table with columns: 'Device Name', 'IP Address', and 'MAC Address'. The table has one row with values: '00:0E:C6:39:6D:59', '192.168.1.33', and '000ec6396d59'. At the bottom of the modal is an 'Apply' button.

Figure 3-4-9: Family Group Management

### 3.4.5.2 Internet access

This page allows you to configure the internet access rule for the family groups. Firstly, you need to select the family group that needs to configure rules in "Family Group Management", and then you can configure the time when the family group can access the internet.

The screenshot shows the 'Internet access' configuration page. At the top, there's a header 'Internet access'. Below it, there's a section 'Family group selected | 1'. Below this, there's a table with columns: 'Week', 'Start Time', and 'End Time'. Below the table, there are two buttons: '+ Add' (green) and 'Delete' (red). A modal window titled 'Add Internet access' is open. It contains a message: 'Allow the family group to access the network for the selected time period'. Below this is a 'Week' dropdown, and two time selection fields: 'Start Time' and 'End Time', each with a clock icon. At the bottom of the modal is an 'Apply' button.

Figure 3-4-10: Add Internet access



### 3.4.5.3 URL Filtering

This page allows you to configure the URL filter for the family groups. Firstly, you need to select the family group that needs to configure rules in “Family Group Management”, and then you can configure the URL which the family group cannot access.

The screenshot displays two main configuration panels. The top panel, titled "URL Filtering", indicates that one family group is selected. It features a text input field labeled "Url address" with a link icon, and two buttons: a green "+ Add" button and a red "Delete" button. The bottom panel, titled "Add URL Filtering", provides a helpful note: "Do not add HTTP and WWW before URL eg. if you need to block http://www.example.com just input example.com". It includes another "Url address" input field and a blue "Apply" button with a checkmark icon.

Figure 3-4-11: URL Filtering

## 3.5 Application

### 3.5.1 VoIP Basic Settings

This page allows you to do VoIP basic configurations.

BASIC SETTINGS

Status

Network

ADVANCED SETTINGS

Security

Application

APPLICATION SETTINGS

VoIP Basic Settings

VoIP Adv Settings

Multicast Settings

NAT Settings

MQTT Settings

USB Storage

Management

Diagnostics

<<

VoIP Basic Settings

Server Type

Server Type

Soft Switch SIP

Primary SIP Register

Primary SIP Register Address

0.0.0.0

Port

5060

Standby SIP Register

Standby SIP Register Address

0.0.0.0

Port

5060

Primary SIP Proxy

Proxy Address

0.0.0.0

Enable Subscribe

5060

Enable Outbound Proxy

Outbound Proxy Address

0.0.0.0

Outbound Proxy Port

5060

SIP Domain

Register Expire (sec)

1800

Standby SIP Proxy

Standby SIP Enable

Enable Subscribe

Proxy Address

0.0.0.0

Port

5060

Enable Outbound Proxy

Outbound Proxy Address

0.0.0.0

Outbound Proxy Port

5060

SIP Domain

Register Expire (sec)

1800

Line 1 User Account

Enable

User Number

User Account

User Password

✓ Apply

Figure 3-5-1: VoIP Basic Settings

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 expires 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 SIP user.
User Password	Enter the password used for authentication with the registrar.

For VOIP WAN connection, service mode must contain VOIP.

### 3.5.2 VoIP Adv Settings

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

BASIC SETTINGS

Status ^

Network ^

ADVANCED SETTINGS

Security ^

Application v

APPLICATION SETTINGS

VoIP Basic Settings

VoIP Adv Settings

Multicast Settings

NAT Settings

MQTT Settings

USB Storage

Management ^

Diagnostics ^

<<

VoIP Adv Settings

SIP

SIP Local Port 5060

RTP Start Port 41000

Packet Time 20

DTMF Mode DTMF\_delete v

RFC2833 payload 97

VoIP Adv Settings

Echo Suppression Settings ☐

VAD ☐

T.38 ☐

Sync Phone time ☒

Caller ID Mode DTMF v

Region CHN-CHINA v

Session Expire (sec) 0

Flash Time min(80ms) 90

Flash Time max(2000ms) 800

Dial Tone Duration (sec) 15

Short digit timer (sec) 3

Long digit timer (sec) 10

Busy tone Duration (sec) 40

Howler tone Duration (sec) 60

Register retry interval 60

Heart beat Mode Disable v

Heart beat cycle[0:Disable] 0

No Answer Timer[0:Disable] 60

**Codec Priority**

Priority 1: G711-ulaw ▼

Priority 2: G711-alaw ▼

Priority 3: G729 ▼

Priority 4: G722 ▼

**Dial Plan**

Dial plan enable: ☒

Dial Plan: 00x.|0[1-9]x.|x.|[1-9]x.|ExxFx.F|FxxF|E54Ex

**Line 1**

Send gain(dB): 0

Recv gain(dB): 0

Call Waiting: ☒

3PTY Conference: ☒

HotLine Enable: ☐

HotLine Timeout: 5

Hot Line Number: \*53#

Uncondition Forward: ☐

Uncondition Forward Num:

Busy Forward: ☐

Busy Forward Num:

No Answer Forward: ☐

No Answer Forward Num:

No Answer Forward Time: 60

Call Transfer: ☒

Figure 3-5-2: VoIP Adv 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 dialling 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.
Heartbeat mode	Set heartbeat mode.
Heartbeat 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 modes, 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	Set 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 Timeout	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.

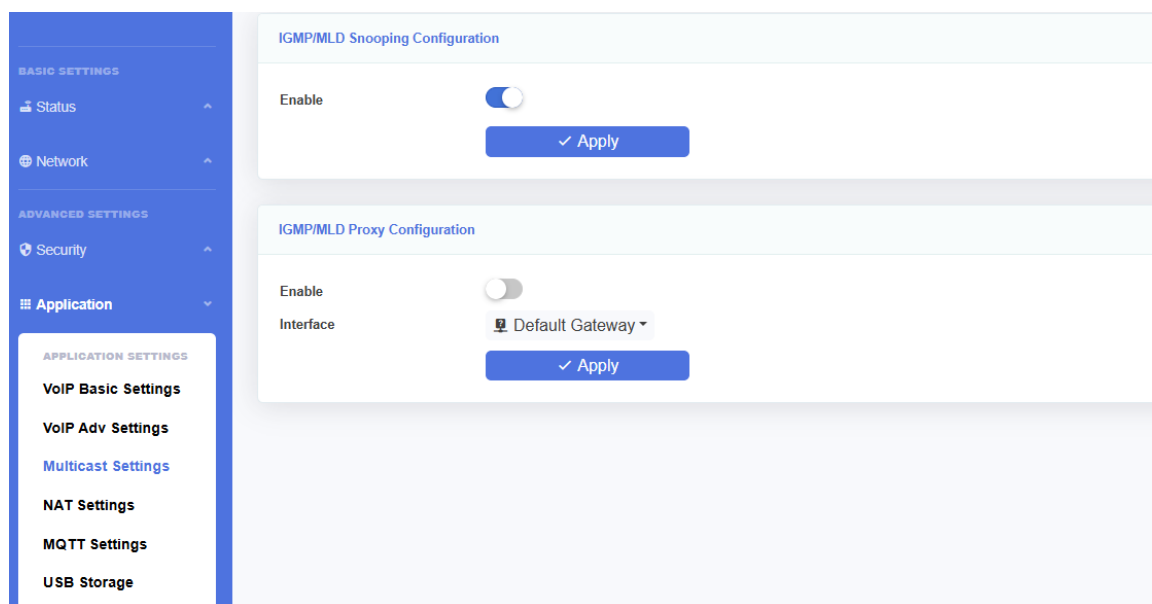


Figure 3-5-3: Multicast Settings

#### 3.5.3.1 IGMP/MLD Snooping Configuration

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

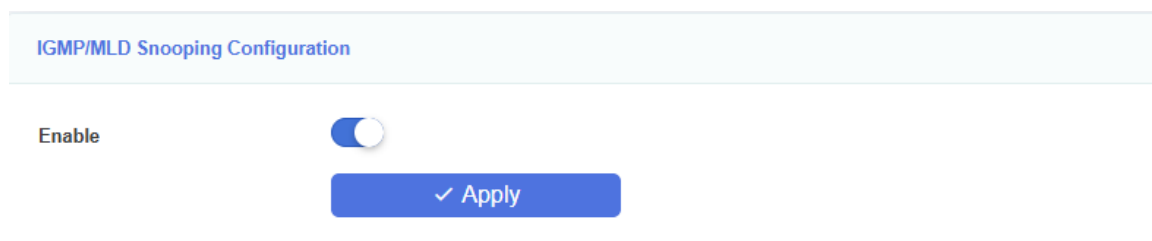
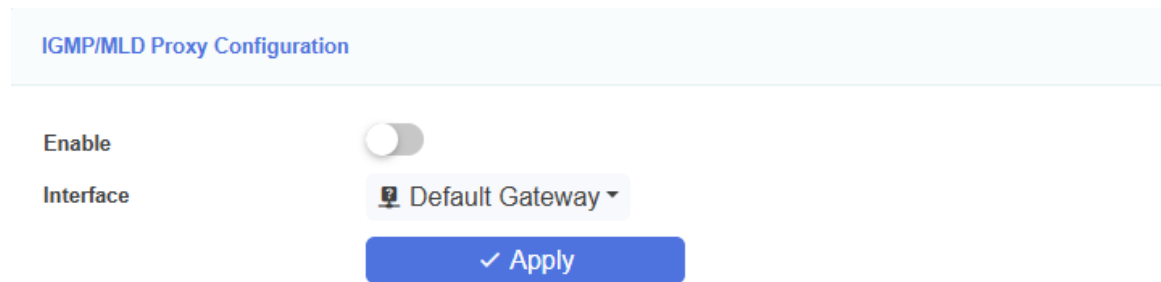


Figure 3-5-4: IGMP/MLD Snooping Configuration

### 3.5.3.2 IGMP/MLD Proxy Configuration

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

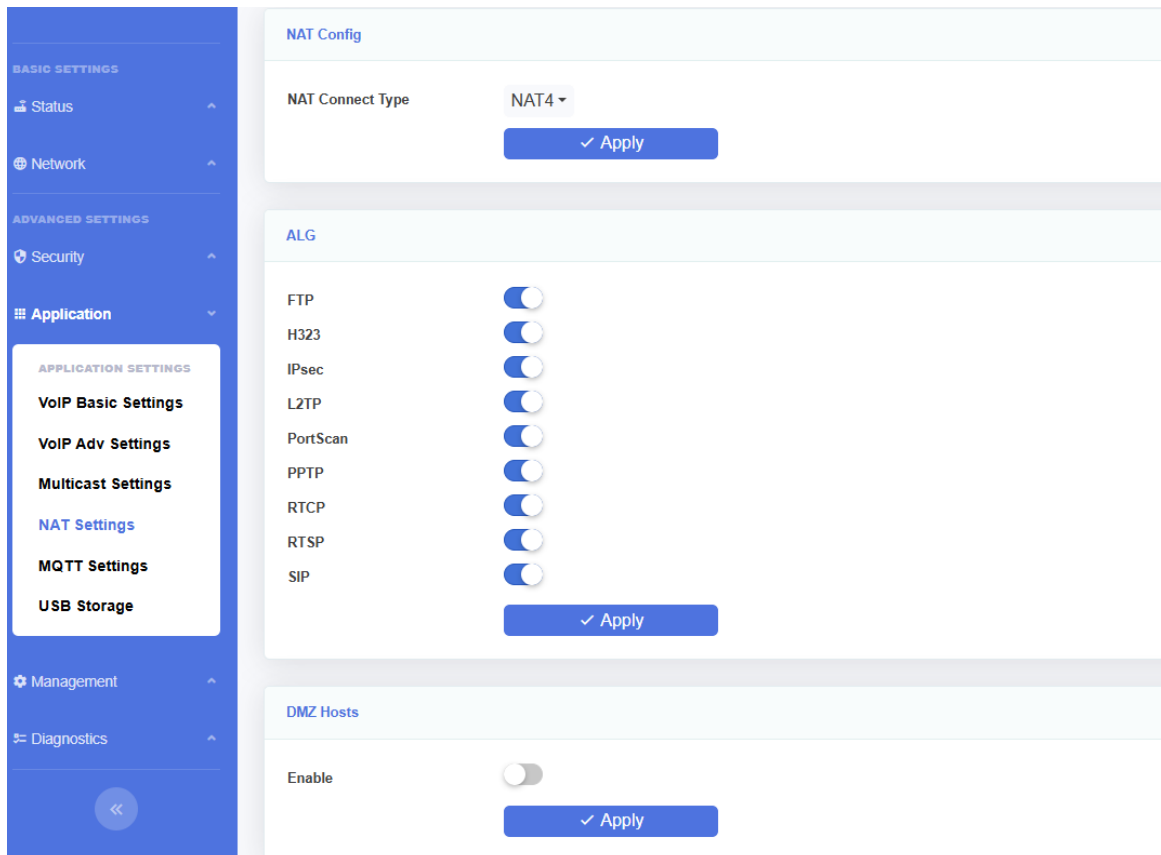


The screenshot shows the 'IGMP/MLD Proxy Configuration' page. It features a toggle switch for 'Enable' which is currently turned off. Below it, the 'Interface' is set to 'Default Gateway' with a dropdown arrow. At the bottom, there is a blue button with a checkmark and the text 'Apply'.

Figure 3-5-5: IGMPMLD Proxy Configuration

### 3.5.4 NAT Settings

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



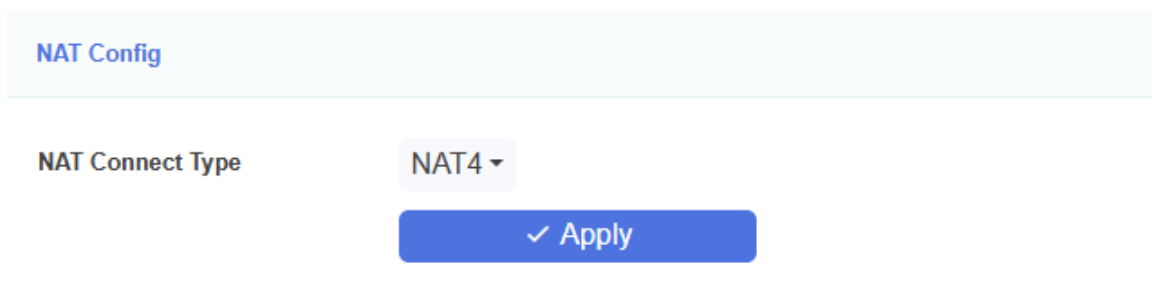
The screenshot shows the 'NAT Settings' page. On the left is a blue sidebar with a menu. The main content area is divided into three sections: 'NAT Config', 'ALG', and 'DMZ Hosts'.  
1. 'NAT Config': Contains a 'NAT Connect Type' dropdown set to 'NAT4' and a blue 'Apply' button.  
2. 'ALG': A list of application layer gateways with toggle switches: FTP, H323, IPsec, L2TP, PortScan, PPTP, RTCP, RTSP, and SIP. All are currently turned on. A blue 'Apply' button is at the bottom.  
3. 'DMZ Hosts': Contains an 'Enable' toggle switch which is turned off, and a blue 'Apply' button at the bottom.  
The sidebar menu includes: BASIC SETTINGS (Status, Network), ADVANCED SETTINGS (Security, Application), APPLICATION SETTINGS (VoIP Basic Settings, VoIP Adv Settings, Multicast Settings, NAT Settings, MQTT Settings, USB Storage), Management, and Diagnostics.

Figure 3-5-6: NAT Settings

#### 3.5.4.1 NAT Config

This page can select the type of NAT to be used.



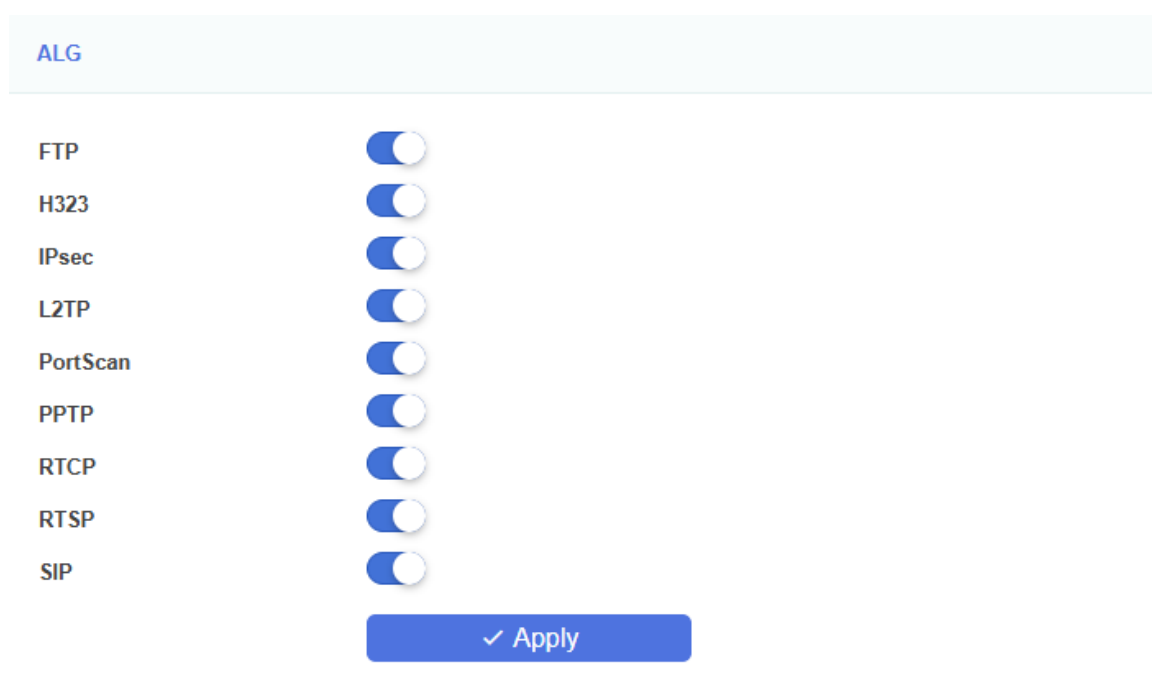


The NAT Config interface features a light blue header with the title "NAT Config". Below the header, the "NAT Connect Type" is set to "NAT4" in a dropdown menu. A blue button with a checkmark and the text "Apply" is positioned below the dropdown.

Figure 3-5-7: NAT Config

#### 3.5.4.2 ALG

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

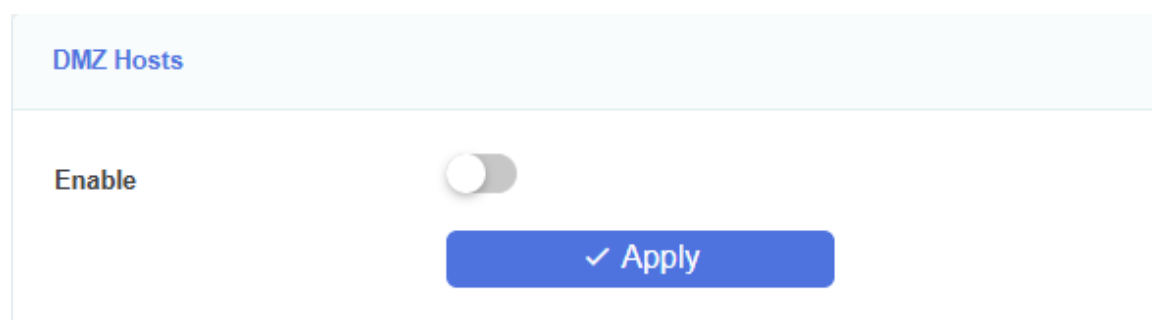


The ALG interface has a light blue header titled "ALG". It contains a list of protocols with corresponding toggle switches: FTP, H323, IPsec, L2TP, PortScan, PPTP, RTCP, RTSP, and SIP. All switches are currently turned on. A blue button with a checkmark and the text "Apply" is located at the bottom right of the list.

Figure 3-5-8: ALG

#### 3.5.4.3 DMZ Hosts

This page allows you to configure DMZ server.



The DMZ Hosts interface has a light blue header titled "DMZ Hosts". Below the header, there is a label "Enable" next to a toggle switch that is currently turned off. A blue button with a checkmark and the text "Apply" is positioned below the toggle switch.

Figure 3-5-9: DMZ Hosts

#### 3.5.4.4 UPnP Configuration

This page allows you to configure UPnP server.

UPnP Configuration

ⓘ UPnP is only available if the selected WAN connection has a public IP

Enable MiniUPnP Service

☒

Enable UPnP

☒

Enable NAT-PMP

☒

IGDv1 Compatible Mode

☐

Interface

📍 Default Gateway ▾

✓ Apply

Figure 3-5-10: UPnP Configuration

3.5.4.5 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
<div>+ Add</div> <div>■ Delete</div>						

Figure 3-5-11: Add Virtual Server

Virtual Server Configuration

Server Name

External IP Address

External Start Port

External End Port

Protocol

TCP ▾

Server IP Address

Source Port

+ Add

Figure 3-5-12: Virtual Server configuration

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

3.5.4.6 Dynamic DNS Configuration

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

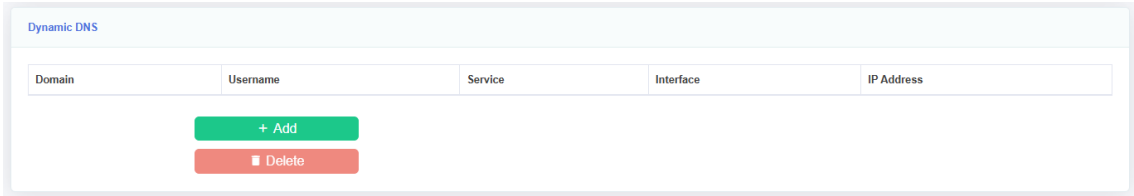


Figure 3-5-13: Dynamic DNS

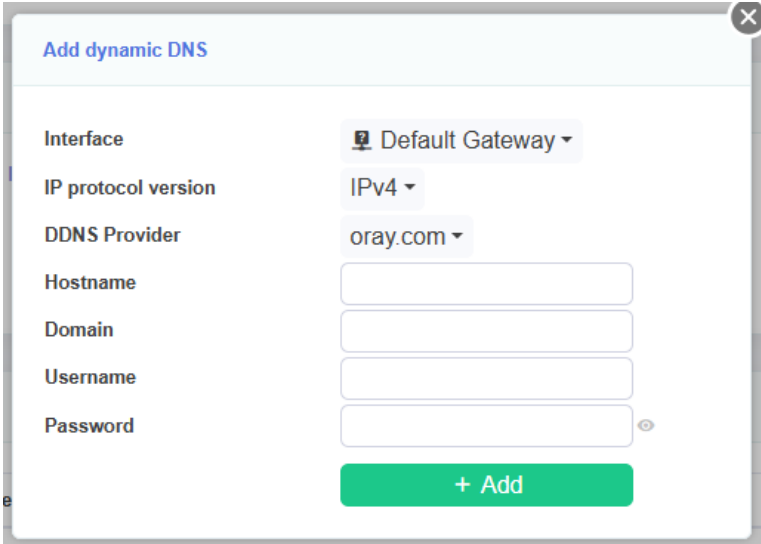


Figure 3-5-14: Add dynamic DNS

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

Parameter	Illustration
Interface	The interface of accessing by DDNS.
IP protocol version	Optional IPV4/IPV6.
DDNS Provider	Choose DDNS service provider.
Hostname	Set host name of the device.
Domain	Set the domain of the DDNS.
Username	The username which is used to access DDNS server.
Password	The password which is used to access DDNS server.

3.5.5 MQTT Settings

This page allows you to configure the ONU's MQTT protocol settings.

**BASIC SETTINGS**

- Status
- Network

**ADVANCED SETTINGS**

- Security
- Application**
  - APPLICATION SETTINGS**
    - Multicast Settings
    - NAT Settings
    - MQTT Settings**
    - USB Storage
  - Management
  - Diagnostics

**MQTT Settings**

MQTT Status | Not Connected

Enable ☒

LOG Info ☐

Server Address

Username

Password

✓ Apply

Figure 3-5-15: MQTT Settings

### 3.5.6 USB Storage

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

**BASIC SETTINGS**

- Status
- Network

**ADVANCED SETTINGS**

- Security
- Application**
  - APPLICATION SETTINGS**
    - Multicast Settings
    - NAT Settings
    - MQTT Settings
    - USB Storage**
  - Management
  - Diagnostics

**FTP**

Enable ☐

✓ Apply

**Samba**

Enable ☐

✓ Apply

**USB Printer**

Enable ☐

✓ Apply

**USB Partition Selection**

Device Name	USB Directory	Resource Info
<div>▲ USB Unload</div>		

Figure 3-5-16: USB Storage

3.5.6.1
FTP

This page is used to configure FTP.

FTP

Enable

☒

Username

ftp

Password

Keep Unchanged

✓
Apply

Figure 3-5-17: FTP

3.5.6.2
Samba

This page is used to configure the Samba.

Samba

Enable

☒

SMBv1 Compatible Mode

☐

Hostname

USB

Username

admin

Password

Keep Unchanged

✓
Apply

Figure 3-5-18: Samba

3.5.6.3
USB Printer

This page is used to configure the USB Printer

USB Printer

Enable

☒

Port

9100

Device Type

/dev/usb/lp0

Device Name

V2804AX30T

Device Maker

USB Printer

✓
Apply

Figure 3-5-19: USB Printer

3.5.6.4
USB Partition Selection

This page is used to configure the USB partition.

USB Partition Selection

Device Name

USB Directory

Resource Info

⬆
USB Unload

Figure 3-5-20: USB Partition Selection

## 3.6 Management

### 3.6.1 User Manage

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

The screenshot shows the 'User Manage' page. On the left is a blue sidebar with a menu. Under 'BASIC SETTINGS', there are 'Status' and 'Network'. Under 'ADVANCED SETTINGS', there are 'Security', 'Application', and 'Management'. The 'Management' menu is expanded, showing 'User Manage' (highlighted), 'Device Manage', 'Log Manage', and 'Mode Manage'. The main content area has a title 'User Manage' and four password requirements: '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:', and '0-9, a-z, A-Z, Special characters (. \_ / @ ! ~ # \$ % ^ \* ( ) + : ? =)'. Below these are four input fields: 'Username' (containing 'admin'), 'Old Password', 'New Password', and 'Confirm Password'. Each password field has an eye icon to toggle visibility. At the bottom is a blue 'Apply' button with a checkmark icon.

Figure 3-6-1: User Manage

### 3.6.2 Device Manage

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

The screenshot shows the 'Device Manage' page. The left sidebar is identical to the previous screenshot. The main content area has three sections: 'Upgrade Image', 'Commit/Reboot', and 'Timely Reboot'. The 'Upgrade Image' section has a note: '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.' Below the note is a 'Choose File' button and a 'No file chosen' status. There is an 'Upgrade' button with a circular arrow icon. The 'Commit/Reboot' section has a 'Reboot' button with a circular arrow icon. The 'Timely Reboot' section shows the current time 'Thu Oct 31 09:24:44 UTC 2024' and a 'Week Day' section with toggle switches for Mon, Tue, Wed, Thu, Fri, Sat, and Sun. Below this is a 'Time' section with 'Hour' and 'Min' dropdowns, both set to '00'. At the bottom is a blue 'Apply' button with a checkmark icon.

Figure 3-6-2: Device Manage

### 3.6.2.1 Upgrade Image

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

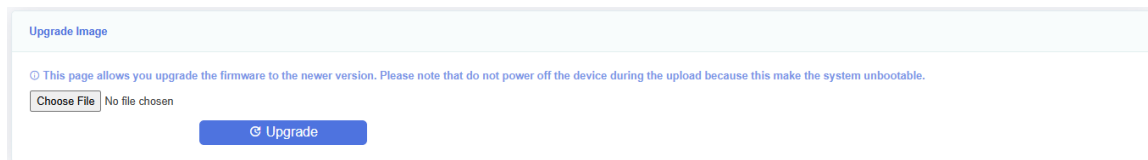


Figure 3-6-3: Upgrade Image

### 3.6.2.2 Commit/Reboot

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

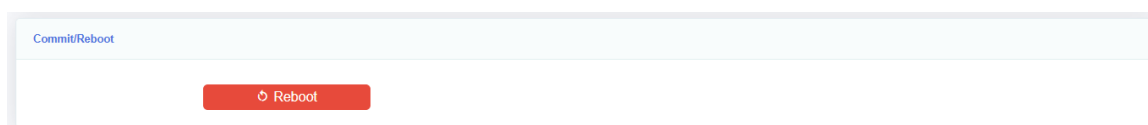


Figure 3-6-4: Commit/Reboot

### 3.6.2.3 Timely Reboot

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

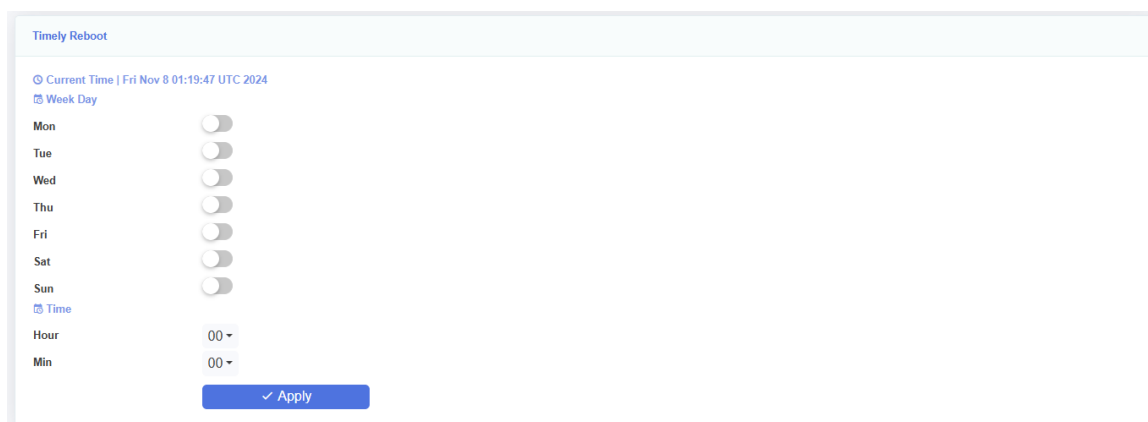


Figure 3-6-5: Timely Reboot

### 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 HGU configurations. After restored, it will restart automatically.

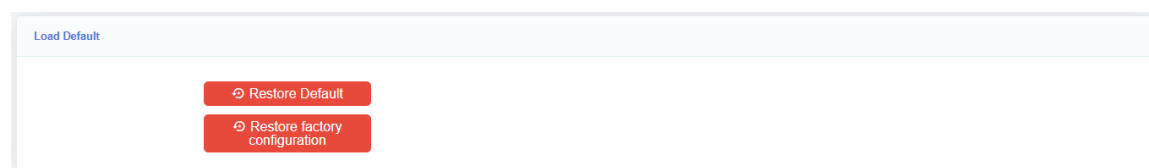


Figure 3-6-6: Load Default

### 3.6.2.5 Current Configuration Management

This page allows you to back up the configurations of HGU. "Download" button can download the current configuration file to your PC. "

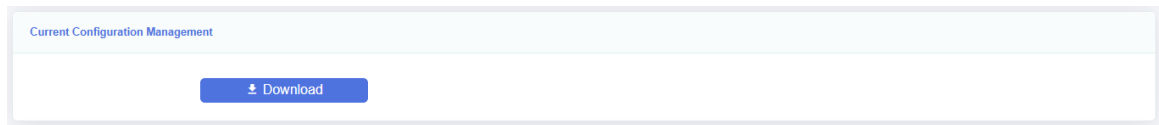


Figure 3-6-7: Current Configuration Management

### 3.6.2.6 Upload Configuration Management

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

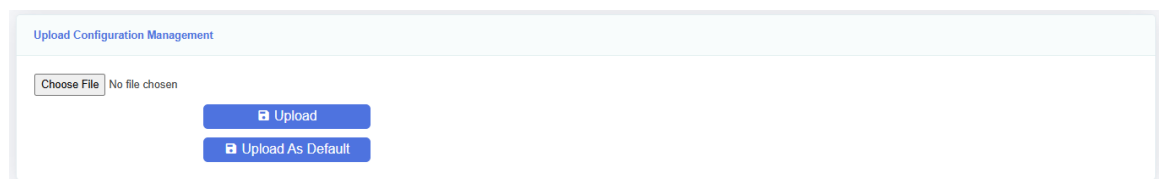


Figure 3-6-8: Upload Configuration Management

## 3.6.3 Log Manage

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

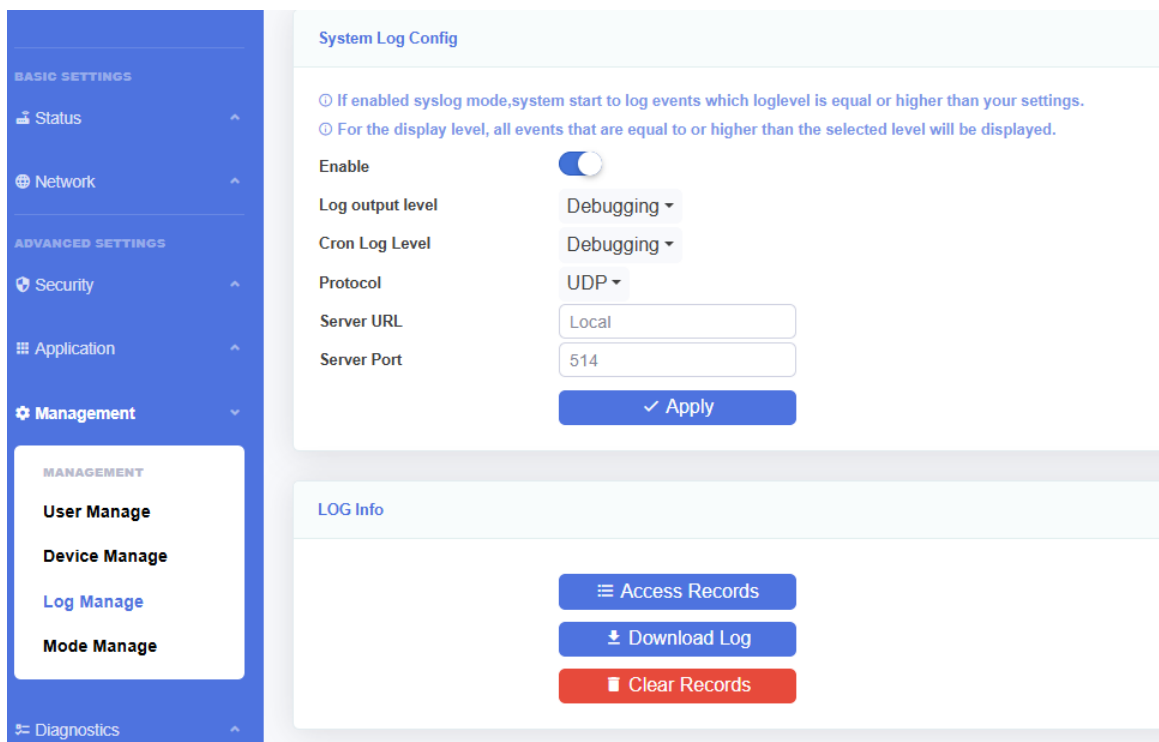


Figure 3-6-9: Log Manage



3.6.3.1
System Log Config

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

System Log Config

If enabled syslog mode,system start to log events which loglevel is equal or higher than your settings.

For the display level, all events that are equal to or higher than the selected level will be displayed.

Enable

Log output level

Cron Log Level

Protocol

Server URL

Server Port

Submit

Figure 3-6-10: System Log Config

Parameters	Illustration
Log output level	Log output level, include Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debugging.
Cron Log Level	Cron log level, include Debugging, Normal, Debugging.
Protocol	Enter the type of protocol used by the server, optional UDP/TCP
Server URL	Enter the server URL
Server Port	Enter the server port

3.6.3.2
LOG Info

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

LOG Info

Access Records

Download Log

Clear Records

Figure 3-6-11: LOG Info

3.6.4
Mode Manage

This page allows you to configure the PON mode. By default, it enables automatic switching of PON mode.

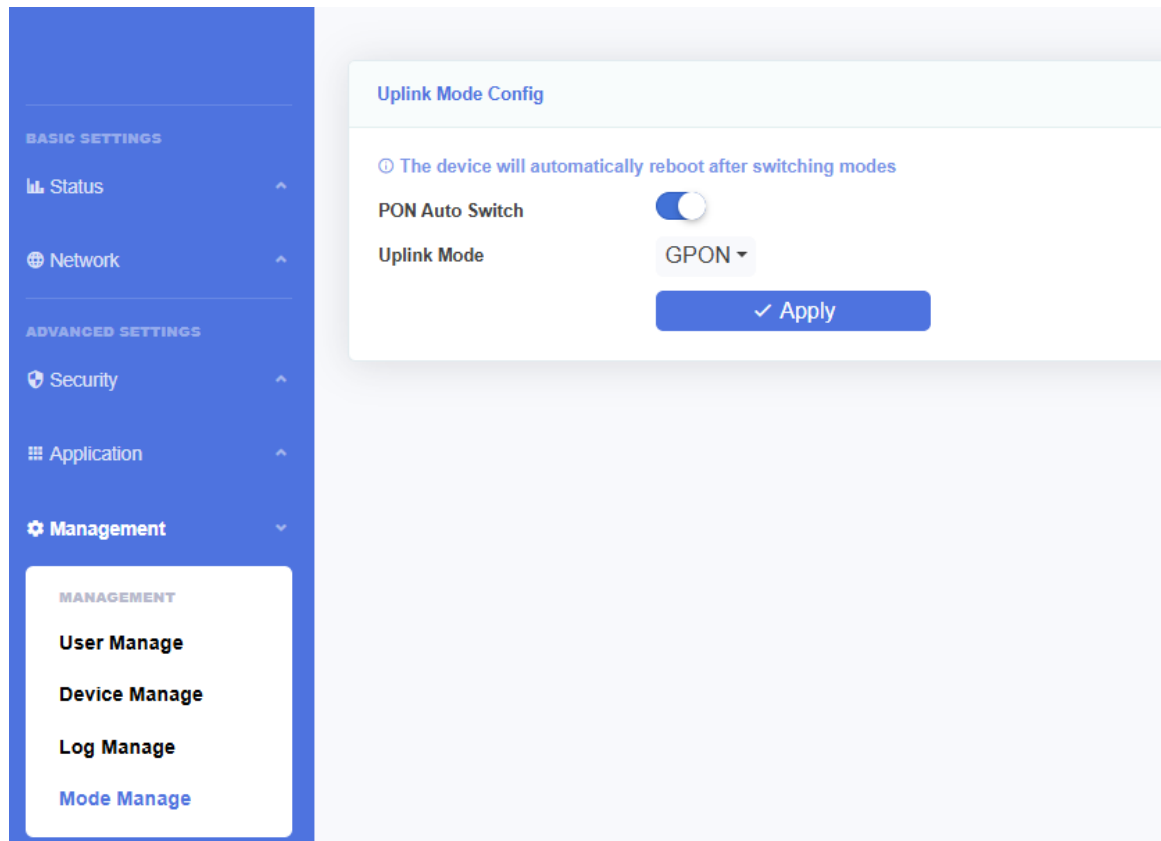


Figure 3-6-12: Mode Manage

## 3.7 Diagnostics

### 3.7.1 Network diagnostics

#### 3.7.1.1 Network diagnostics

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

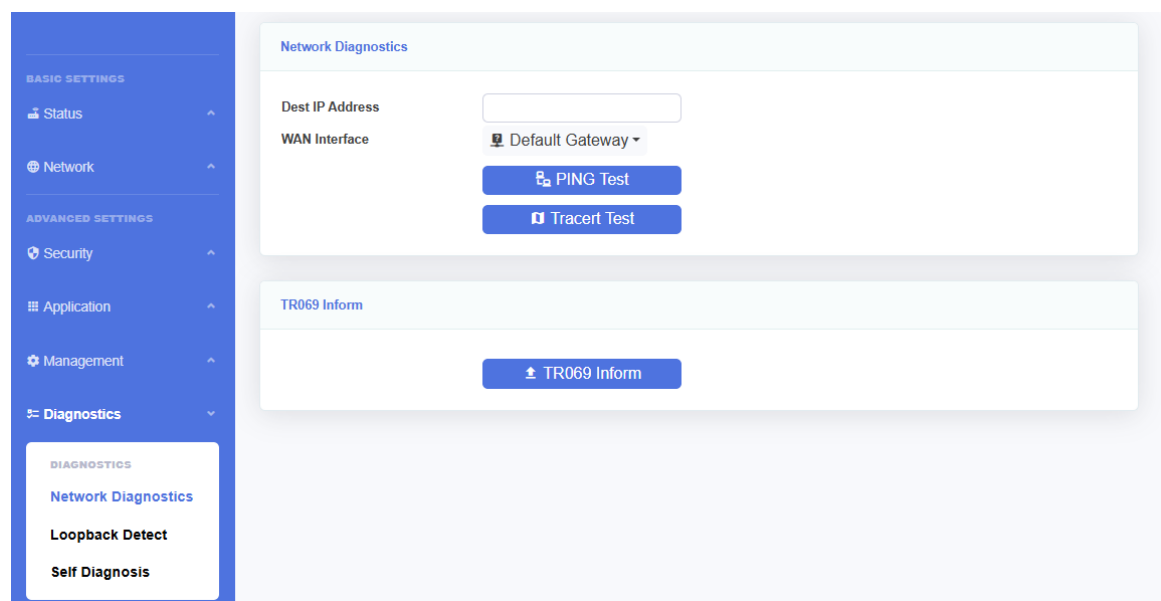


Figure 3-7-1: Network Diagnostics

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

### 3.7.1.2 TR069 Inform

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

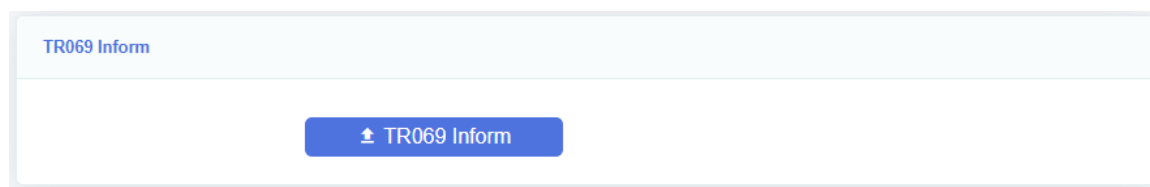


Figure :3-7-2 TR069 Inform

## 3.7.2 Loopback Detect

### 3.7.2.1 Loopback Test

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

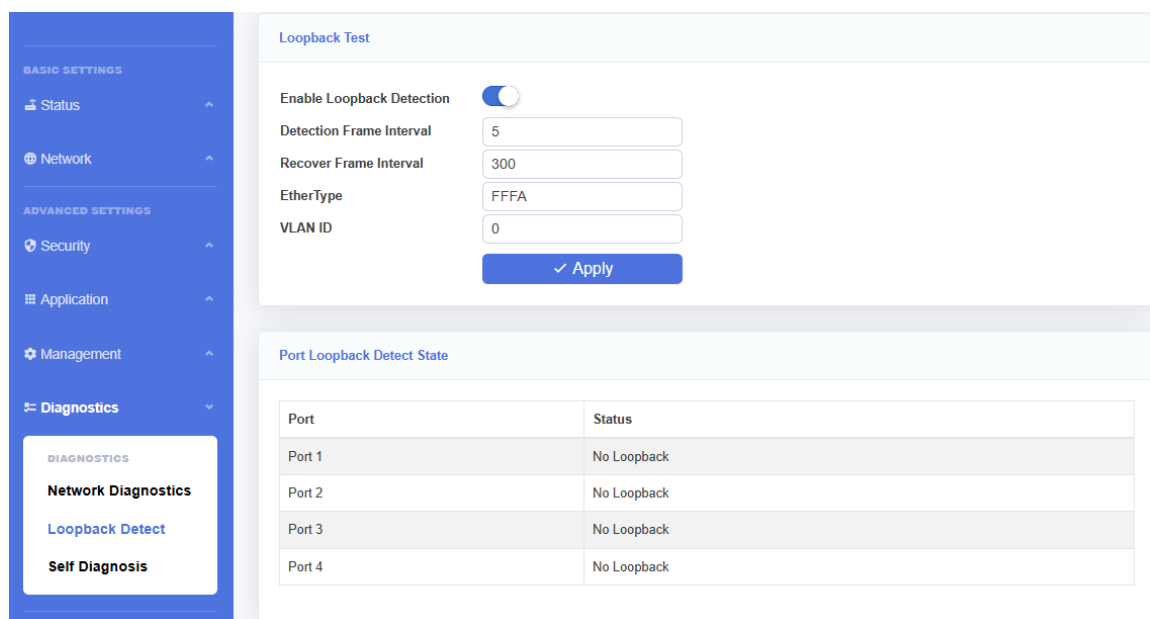


Figure 3-7-3: Loopback Test

### 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
Port 1	No Loopback
Port 2	No Loopback
Port 3	No Loopback
Port 4	No Loopback

Figure 3-7-4: Port Loopback Detect State

### 3.7.3 Self-Diagnosis

#### 3.7.3.1 Self-Diagnosis

This page is use for checking the onu working state.

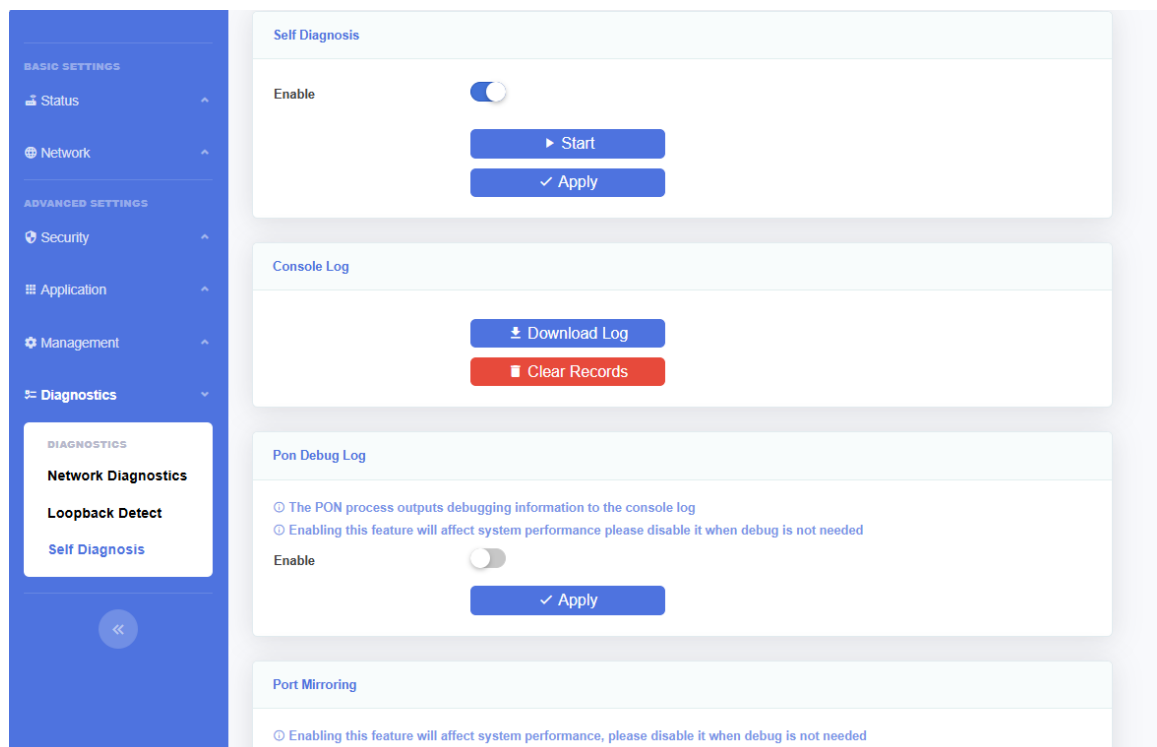


Figure 3-7-5: Self Diagnosis

#### 3.7.3.2 Console Log

This page is use for download and clear the console log.

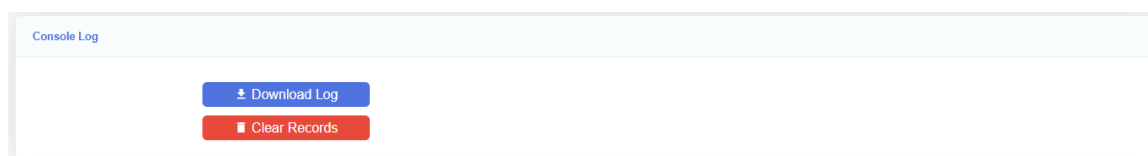


Figure 3-7-6: Console Log

#### 3.7.3.3 Pon Debug Log

This page is use for enable/disable the onu pon debugging information to the console log, if you no need to enable it, please disable

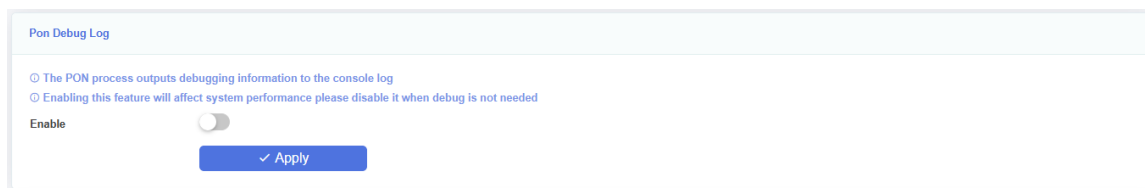


Figure 3-7-7: Pon Debug Log

### 3.7.3.4 Port Mirroring

This page is used to enable the port mirroring function of HGU.

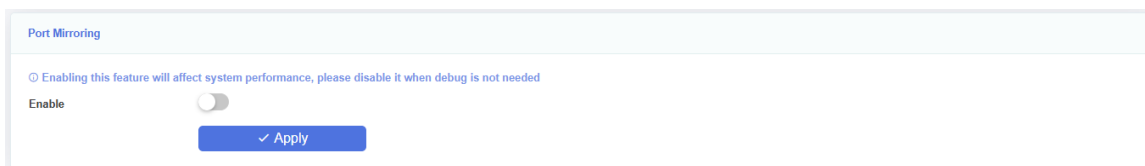


Figure 3-7-8: Port Mirroring

### 3.7.3.5 Capture Packets

This page is used to enable ONU to capture packets for checking whether the message exchange is normal or not and click Download Capture Packets to view the network messages after the capture is completed.

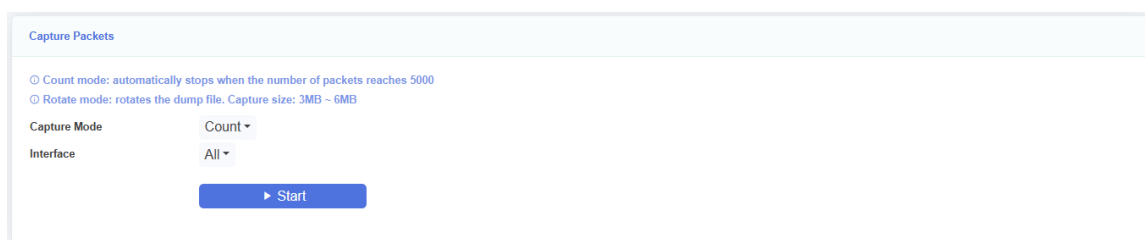


Figure 3-7-9: Capture Packets

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

#### 4.1.2 Steps

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

##### 4.1.2.1 Bridge mode for Internet service

- 1) Add a WAN connection

Choose “Network > WAN > WAN Configuration” 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 (IPTV).
- ✧ Bind port 1.
- ✧ Other parameters keep default.

The screenshot displays the 'WAN Configuration' page. The 'Connectin Name' is set to '1\_OTHER\_B\_VID\_9'. The 'Mode' is 'Bridge', 'Application type' is 'OTHER (IPTV)', and 'IP Version' is 'IPv4'. The 'Enable VLAN' toggle is turned on, with 'VLAN ID' set to '9'. '802.1p Priority' is '0' and 'MTU' is '1500'. The 'Disable LAN DHCP' toggle is turned on. A 'Bind Port' checkbox is checked. Below these settings is a grid of port selection buttons: 'Port 1' (highlighted in blue), 'Port 2', 'Port 3', and 'Port 4'. Under each port button are two WLAN options: 'WLAN AP1-2.4G', 'WLAN AP2-2.4G', 'WLAN AP3-2.4G', 'WLAN AP4-2.4G' for the top row, and 'WLAN AP1-5G', 'WLAN AP2-5G', 'WLAN AP3-5G', 'WLAN AP4-5G' for the bottom row. At the bottom of the form are three buttons: 'Apply' (blue), 'Reboot' (red), and 'Delete' (red).

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 Configuration” in navigation menu. Add a route mode WAN connection as the following parameters.

- ✧ Mode is Route
- ✧ 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.

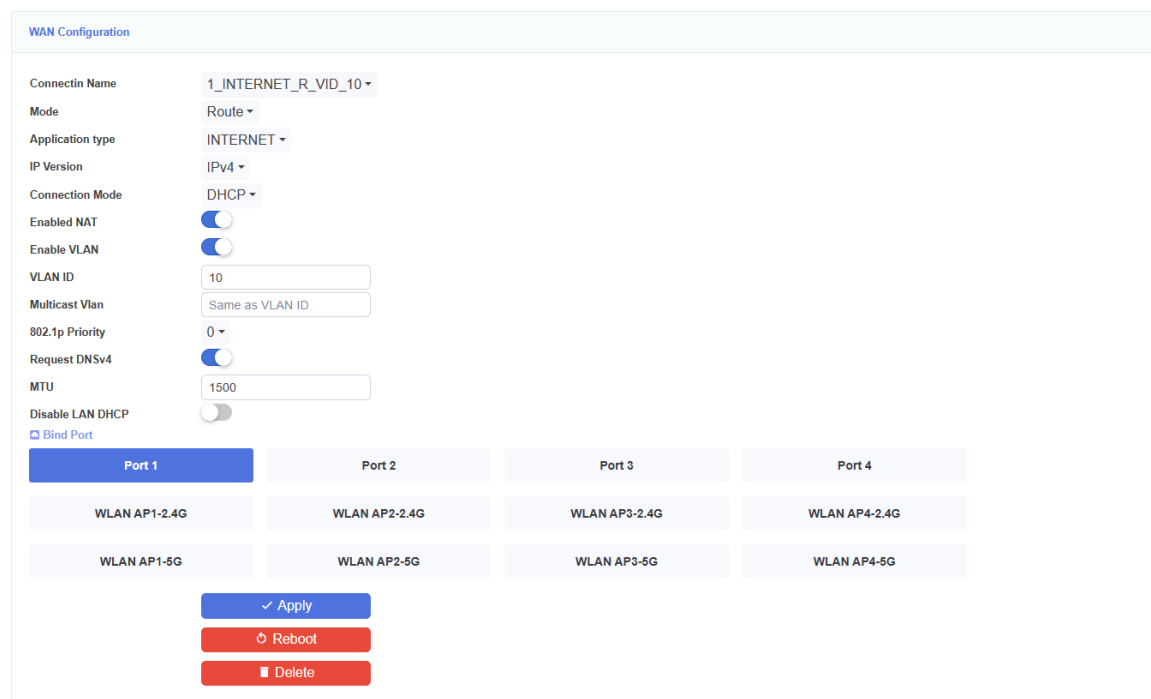


Figure 4-1-2: Add a route WAN connection

##### 2) Surf the Internet

Connect PC to LAN port 1. The PC gets IP address from HGU and HGU 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 HGU works on route mode.

### 4.2.1 Requirement

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

## 4.2.2 Steps

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

### 4.2.2.1 Bridge mode for IGMP

#### 1) Add a WAN connection

Choose “Network > WAN > WAN Configuration” 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 (IPTV).
- ✧ Bind port 2.
- ✧ Other parameters keep default.

The screenshot shows the 'WAN Configuration' page. The 'Connectin Name' is '1\_OTHER\_B\_VID\_20'. The 'Mode' is 'Bridge'. The 'Application type' is 'OTHER (IPTV)'. The 'IP Version' is 'IPv4'. The 'Enable VLAN' toggle is turned on. The 'VLAN ID' is '20'. The '802.1p Priority' is '0'. The 'MTU' is '1500'. The 'Disable LAN DHCP' toggle is turned on. There is a 'Bind Port' checkbox which is checked. Below these settings is a table of ports:

Port 1	Port 2	Port 3	Port 4
WLAN AP1-2.4G	WLAN AP2-2.4G	WLAN AP3-2.4G	WLAN AP4-2.4G
WLAN AP1-5G	WLAN AP2-5G	WLAN AP3-5G	WLAN AP4-5G

At the bottom of the form are three buttons: 'Apply' (blue), 'Reboot' (red), and 'Delete' (red).

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

#### 2) Enable IGMP snooping

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

The screenshot shows the 'IGMP/MLD Snooping Configuration' page. There is an 'Enable' toggle switch which is turned on. Below the toggle is an 'Apply' button (blue).

Figure 4-2-2: Enable IGMP snooping

#### 3) Join multicast group

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

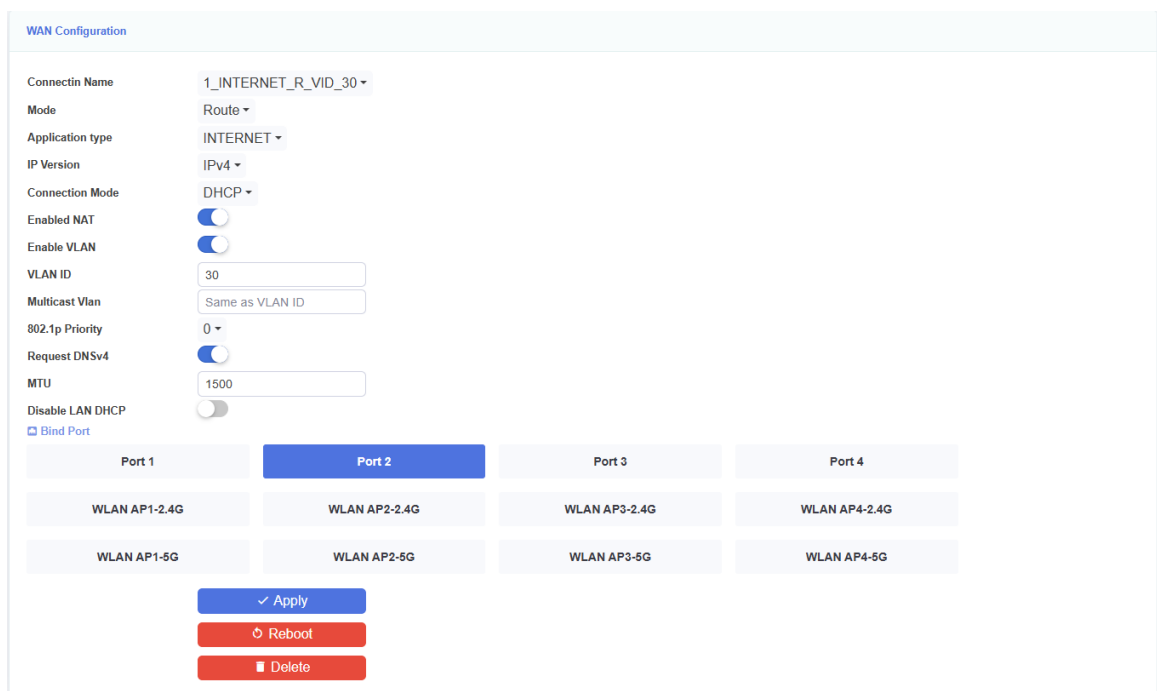
### 4.2.2.2 Route mode for IGMP

#### 1) Add a WAN connection



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

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

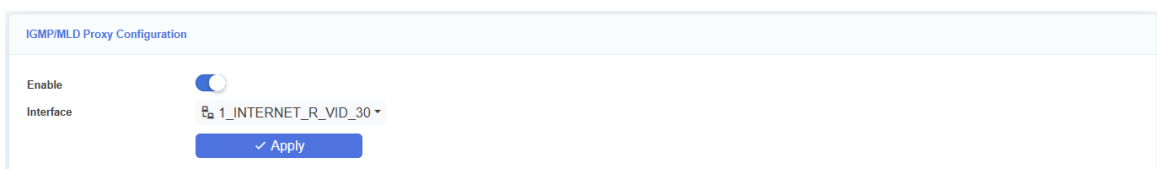


The screenshot shows the 'WAN Configuration' page. The 'Connectin Name' is '1\_INTERNET\_R\_VID\_30'. The 'Mode' is 'Route'. The 'Application type' is 'INTERNET'. The 'IP Version' is 'IPv4'. The 'Connection Mode' is 'DHCP'. The 'Enabled NAT' toggle is turned on. The 'Enable VLAN' toggle is turned on. The 'VLAN ID' is '30'. The 'Multicast Vlan' is 'Same as VLAN ID'. The '802.1p Priority' is '0'. The 'Request DNSv4' toggle is turned on. The 'MTU' is '1500'. The 'Disable LAN DHCP' toggle is turned off. The 'Bind Port' checkbox is checked. Below these settings, there are four port selection buttons: 'Port 1', 'Port 2' (highlighted in blue), 'Port 3', and 'Port 4'. Below the port selection, there are four WLAN AP selection buttons: 'WLAN AP1-2.4G', 'WLAN AP2-2.4G', 'WLAN AP3-2.4G', and 'WLAN AP4-2.4G'. Below these, there are four WLAN AP selection buttons: 'WLAN AP1-5G', 'WLAN AP2-5G', 'WLAN AP3-5G', and 'WLAN AP4-5G'. At the bottom, there are three buttons: 'Apply' (blue), 'Reboot' (red), and 'Delete' (red).

Figure 4-2-3: Add a route WAN connection

## 2) Enable IGMP proxy

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



The screenshot shows the 'IGMP/MLD Proxy Configuration' page. The 'Enable' toggle is turned on. The 'Interface' dropdown menu is set to '1\_INTERNET\_R\_VID\_30'. At the bottom, there is an 'Apply' button (blue).

Figure 4-2-4: Enable IGMP proxy

## 3) Join multicast group

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

### 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 Configuration” 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.

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

- Connectin Name: 1\_VOIP\_R\_VID\_3000
- Mode: Route
- Application type: VOIP
- IP Version: IPv4
- Connection Mode: Static
- Enable VLAN: ☒
- VLAN ID: 3000
- Multicast Vlan: Same as VLAN ID
- 802.1p Priority: 0
- 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
- MTU: 1500

At the bottom, there are three buttons: 'Apply' (blue), 'Reboot' (red), and 'Delete' (red).

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 phone number, username and password.

**VoIP Basic Settings**

**☎ Server Type**

Server Type Soft Switch SIP ▾

**☎ Primary SIP Register**

Primary SIP Register Address 192.168.6.6

Port 5060

**☎ Standby SIP Register**

Standby SIP Register Address 0.0.0.0

Port 5060

**☎ Primary SIP Proxy**

Proxy Address 192.168.6.6

Enable Subscribe ☒

Port 5060

Enable Outbound Proxy ☒

Outbound Proxy Address 0.0.0.0

Outbound Proxy Port 5060

SIP Domain

Register Expire (sec) 1800

**☎ Standby SIP Proxy**

Standby SIP Enable ☐

Enable Subscribe ☒

Proxy Address 0.0.0.0

Port 5060

Enable Outbound Proxy ☒

Outbound Proxy Address 0.0.0.0

Outbound Proxy Port 5060

SIP Domain

Register Expire (sec) 1800

**☎ Line 1 User Account**

Enable ☒

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
Register Fail Reason	

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) HGU 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) HGU 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

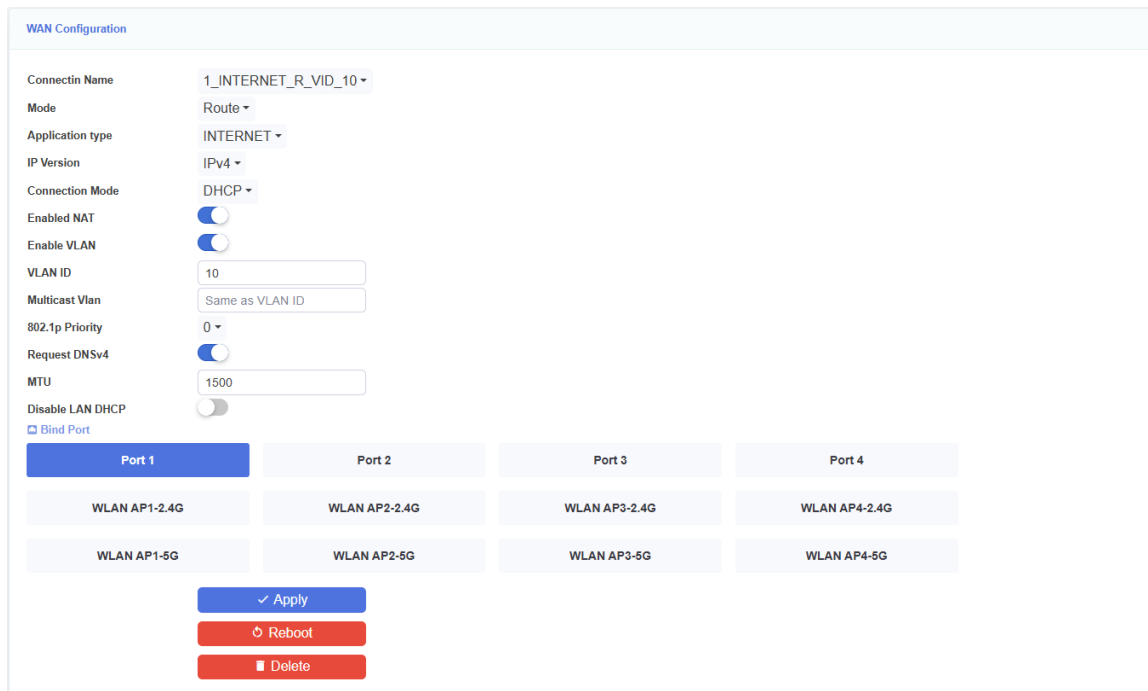
Before configuring, make sure HGU has registered and been authorized successfully. Connect PC to one LAN port of HGU directly with twisted cable.

#### 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.

- ✧ Choose the route mode
- ✧ 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.



The screenshot shows the 'WAN Configuration' page for a route mode WAN connection. The configuration parameters are as follows:

- Connectin Name: 1\_INTERNET\_R\_VID\_10
- Mode: Route
- Application type: INTERNET
- IP Version: IPv4
- Connection Mode: DHCP
- Enabled NAT: ☒
- Enable VLAN: ☒
- VLAN ID: 10
- Multicast Vlan: Same as VLAN ID
- 802.1p Priority: 0
- Request DNSv4: ☒
- MTU: 1500
- Disable LAN DHCP: ☐
- Bind Port: ☒

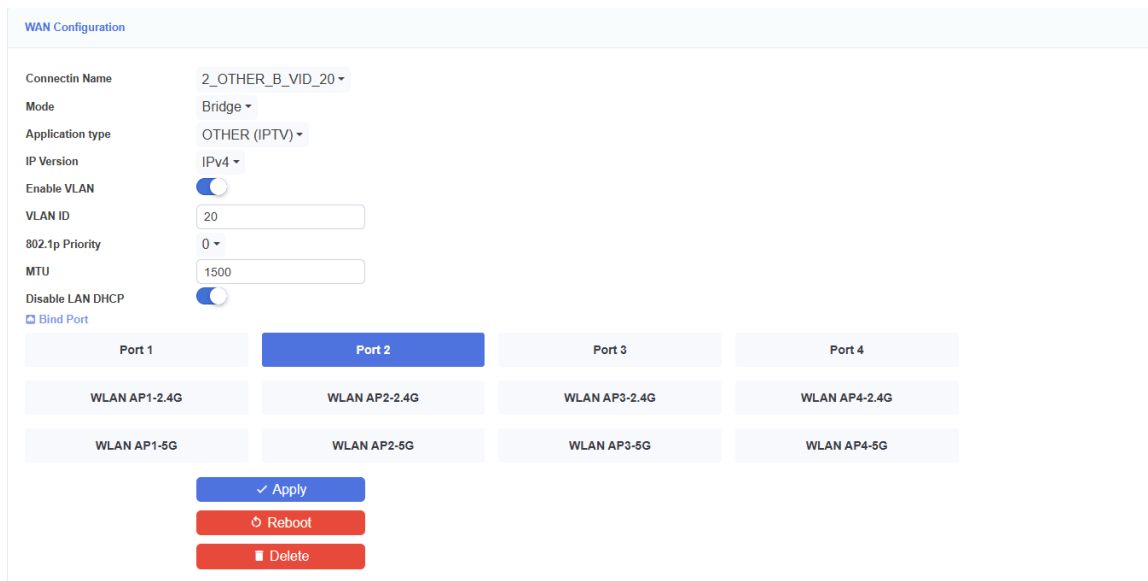
Below the configuration fields, there is a table of ports and their associated WLANs:

Port 1	Port 2	Port 3	Port 4
WLAN AP1-2.4G	WLAN AP2-2.4G	WLAN AP3-2.4G	WLAN AP4-2.4G
WLAN AP1-5G	WLAN AP2-5G	WLAN AP3-5G	WLAN AP4-5G

At the bottom, there are three buttons: 'Apply' (blue), 'Reboot' (red), and 'Delete' (red).

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 (IPTV) and bind port 2.



The screenshot shows the 'WAN Configuration' page for a bridge mode WAN connection. The configuration parameters are as follows:

- Connectin Name: 2\_OTHER\_B\_VID\_20
- Mode: Bridge
- Application type: OTHER (IPTV)
- IP Version: IPv4
- Enable VLAN: ☒
- VLAN ID: 20
- 802.1p Priority: 0
- MTU: 1500
- Disable LAN DHCP: ☒
- Bind Port: ☒

Below the configuration fields, there is a table of ports and their associated WLANs:

Port 1	Port 2	Port 3	Port 4
WLAN AP1-2.4G	WLAN AP2-2.4G	WLAN AP3-2.4G	WLAN AP4-2.4G
WLAN AP1-5G	WLAN AP2-5G	WLAN AP3-5G	WLAN AP4-5G

At the bottom, there are three buttons: 'Apply' (blue), 'Reboot' (red), and 'Delete' (red).

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

## 2) 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.

## 3) 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.

The screenshot shows the 'WAN Configuration' page. The 'Connectin Name' is set to '1\_INTERNET\_R\_VID\_11'. The 'Mode' is 'Route'. The 'Application type' is 'INTERNET'. The 'IP Version' is 'IPv4'. The 'Connection Mode' is 'DHCP'. The 'Enabled NAT' toggle is on. The 'Enable VLAN' toggle is on. The 'VLAN ID' is '11'. The 'Multicast Vlan' is 'Same as VLAN ID'. The '802.1p Priority' is '0'. The 'Request DNSv4' toggle is on. The 'MTU' is '1500'. The 'Disable LAN DHCP' toggle is off. There is a 'Bind Port' checkbox which is checked. Below these settings are four columns representing ports: Port 1, Port 2, Port 3, and Port 4. Each column has two rows: 'WLAN AP1-2.4G' and 'WLAN AP1-5G' for Port 1; 'WLAN AP2-2.4G' and 'WLAN AP2-5G' for Port 2; 'WLAN AP3-2.4G' and 'WLAN AP3-5G' for Port 3; and 'WLAN AP4-2.4G' and 'WLAN AP4-5G' for Port 4. At the bottom are three buttons: 'Apply', 'Reboot', and 'Delete'.

Figure 4-4-3: 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.

The screenshot shows the 'IGMP/MLD Proxy Configuration' page. The 'Enable' toggle is on. The 'Interface' is set to '1\_INTERNET\_R\_VID\_11'. There is an 'Apply' button at the bottom.

Figure 4-4-4: Enable IGMP proxy

## 3) 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.

## 4) 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.

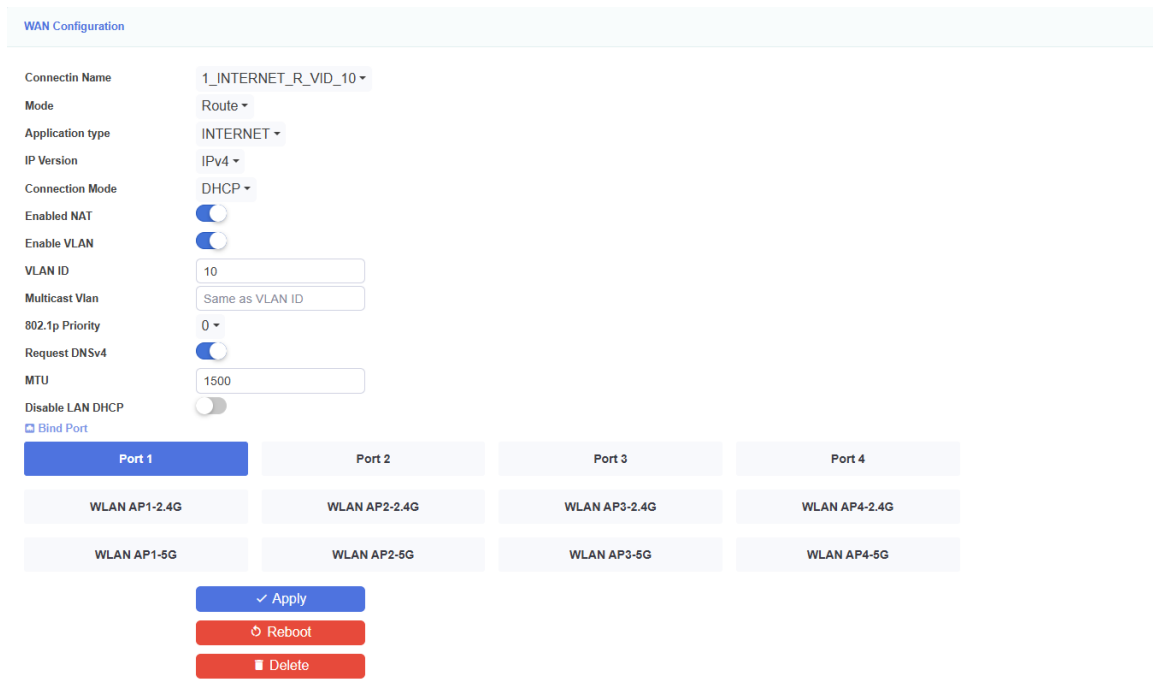
### 4.5.2 Steps

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 Configuration” in navigation menu. Add a route mode WAN connection for Internet service as the following parameters.

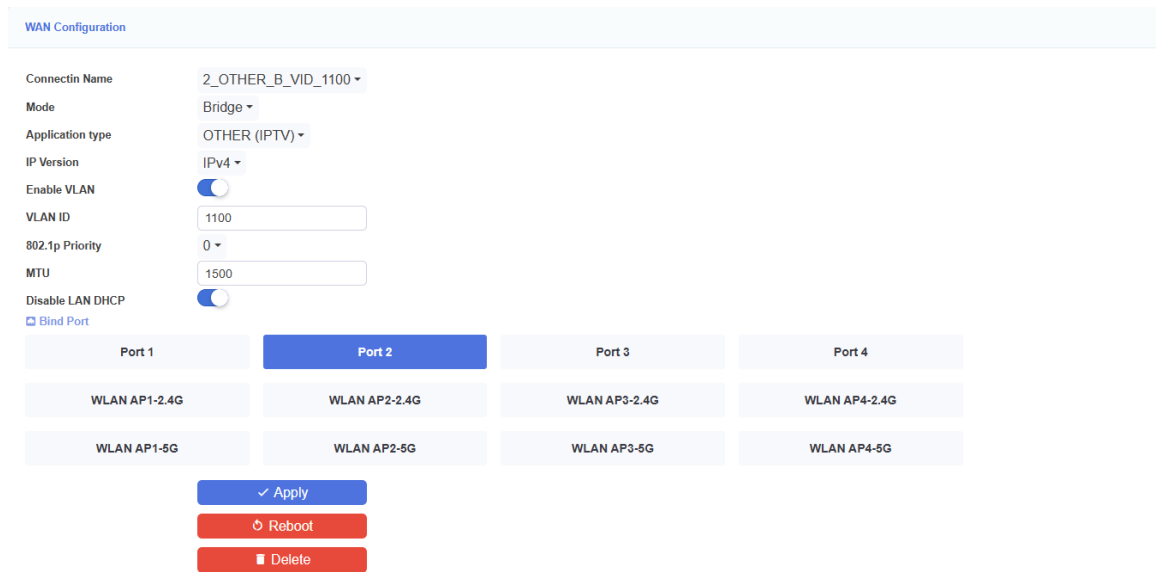
- ✧ Protocol mode is IPv4.
- ✧ Choose DHCP. (Provided by ISP).
- ✧ NAT function is checked.
- ✧ Enable VLAN and VLAN ID is 10.
- ✧ Service mode is INTERNET.
- ✧ Bind port 1.
- ✧ Other parameters keep default.



The screenshot shows the 'WAN Configuration' page. The 'Connectin Name' is '1\_INTERNET\_R\_VID\_10'. The 'Mode' is 'Route'. The 'Application type' is 'INTERNET'. The 'IP Version' is 'IPv4'. The 'Connection Mode' is 'DHCP'. The 'Enabled NAT' toggle is turned on. The 'Enable VLAN' toggle is turned on. The 'VLAN ID' is '10'. The 'Multicast Vlan' is 'Same as VLAN ID'. The '802.1p Priority' is '0'. The 'Request DNSv4' toggle is turned on. The 'MTU' is '1500'. The 'Disable LAN DHCP' toggle is turned off. The 'Bind Port' section shows 'Port 1' selected. Below the 'Bind Port' section, there are buttons for 'Apply', 'Reboot', and 'Delete'.

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 Configuration

Connectin Name: 2\_OTHER\_B\_VID\_1100

Mode: Bridge

Application type: OTHER (IPTV)

IP Version: IPv4

Enable VLAN: ☒

VLAN ID: 1100

802.1p Priority: 0

MTU: 1500

Disable LAN DHCP: ☒

☒ Bind Port

Port 1	Port 2	Port 3	Port 4
WLAN AP1-2.4G	WLAN AP2-2.4G	WLAN AP3-2.4G	WLAN AP4-2.4G
WLAN AP1-5G	WLAN AP2-5G	WLAN AP3-5G	WLAN AP4-5G

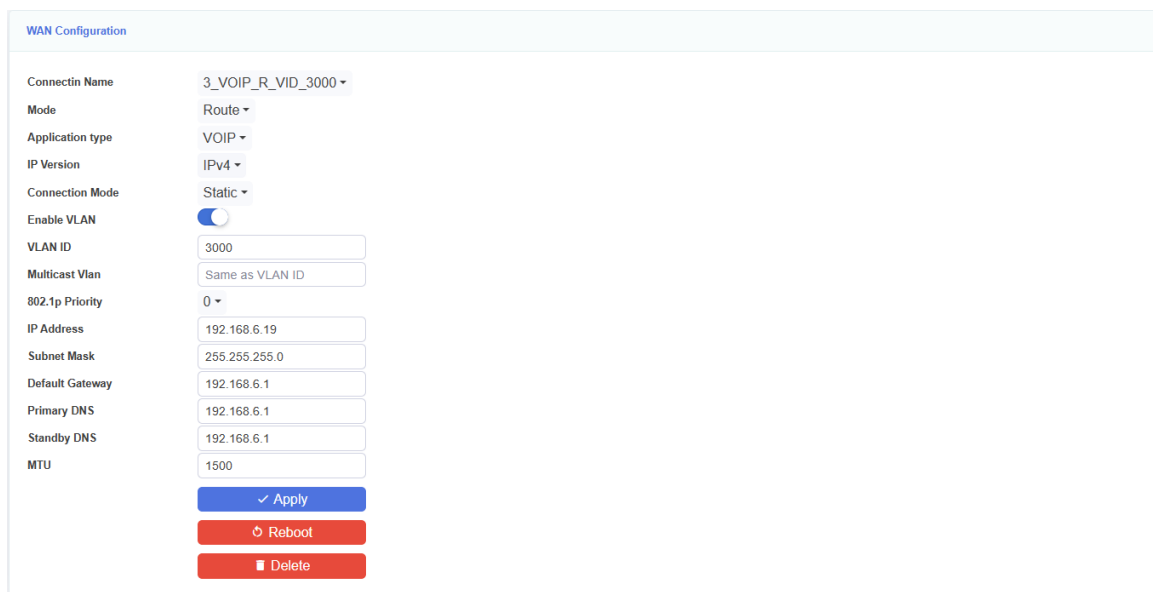
✓ Apply

↻ Reboot

🗑 Delete

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 Configuration

Connectin Name: 3\_VOIP\_R\_VID\_3000

Mode: Route

Application type: VOIP

IP Version: IPv4

Connection Mode: Static

Enable VLAN: ☒

VLAN ID: 3000

Multicast Vlan: Same as VLAN ID

802.1p Priority: 0

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

MTU: 1500

✓ Apply

↻ Reboot

🗑 Delete

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
Soft Switch SIP

Primary SIP Register

Primary SIP Register Address
192.168.6.33

Port
5060

Standby SIP Register

Standby SIP Register Address
0.0.0.0

Port
5060

Primary SIP Proxy

Proxy Address
192.168.6.33

Enable Subscribe
☒

Port
5060

Enable Outbound Proxy
☒

Outbound Proxy Address
0.0.0.0

Outbound Proxy Port
5060

SIP Domain

Register Expire (sec)
1800

Standby SIP Proxy

Standby SIP Enable
☐

Enable Subscribe
☒

Proxy Address
0.0.0.0

Port
5060

Enable Outbound Proxy
☒

Outbound Proxy Address
0.0.0.0

Outbound Proxy Port
5060

SIP Domain

Register Expire (sec)
1800

Line 1 User Account

Enable
☒

User Number
12345678

User Account
12345678

User Password
\*\*\*\*\*

Submit

Figure 4-5-4: VOIP general settings

### 3) 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.

#### 4) Watch IPTV

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

#### 5) 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
Register Fail Reason	

Figure 4-5-5: 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 “FTTH-D2BE”. Network authentication method is WPA2+WPA3, and encryption method is AES.

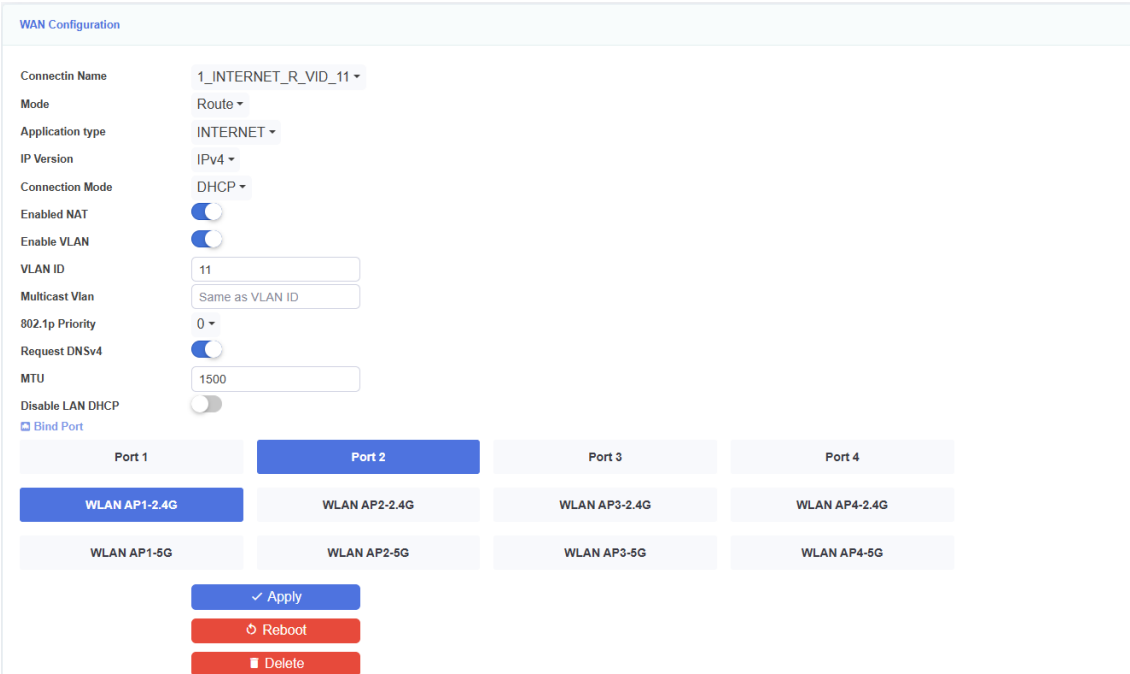
### 4.6.2 Steps

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 Configuration” 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 Configuration**

Connectin Name: 1\_INTERNET\_R\_VID\_11 ▾

Mode: Route ▾

Application type: INTERNET ▾

IP Version: IPv4 ▾

Connection Mode: DHCP ▾

Enabled NAT: ☒

Enable VLAN: ☒

VLAN ID: 11

Multicast Vlan: Same as VLAN ID

802.1p Priority: 0 ▾

Request DNSv4: ☒

MTU: 1500

Disable LAN DHCP: ☐

☒ Bind Port

Port 1	Port 2	Port 3	Port 4
WLAN AP1-2.4G	WLAN AP2-2.4G	WLAN AP3-2.4G	WLAN AP4-2.4G
WLAN AP1-5G	WLAN AP2-5G	WLAN AP3-5G	WLAN AP4-5G

✓ Apply

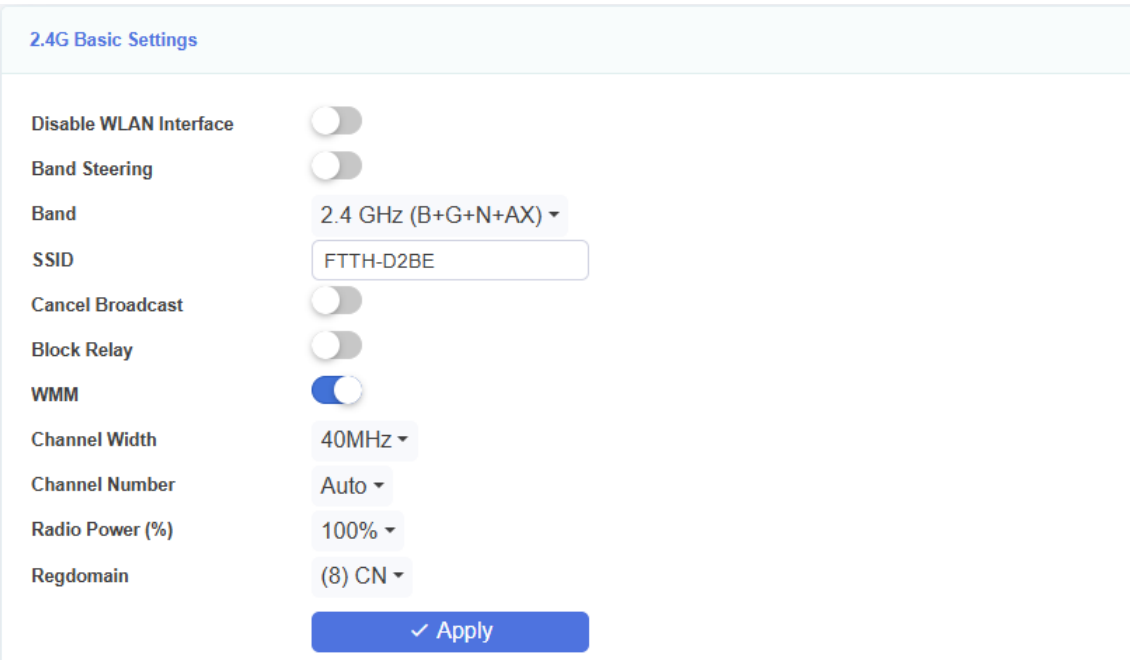
↻ Reboot

■ Delete

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

## 2) Configure WLAN basic parameters

Choose “Network > 2.4G Basic Settings> 2.4G WLAN Basic Settings” in navigation menu. Enable wireless and modify SSID1’s name to FTTH-D2BE. For other parameters, just configure the suitable ones if necessary.



**2.4G Basic Settings**

Disable WLAN Interface: ☐

Band Steering: ☐

Band: 2.4 GHz (B+G+N+AX) ▾

SSID: FTTH-D2BE

Cancel Broadcast: ☐

Block Relay: ☐

WMM: ☒

Channel Width: 40MHz ▾

Channel Number: Auto ▾

Radio Power (%): 100% ▾

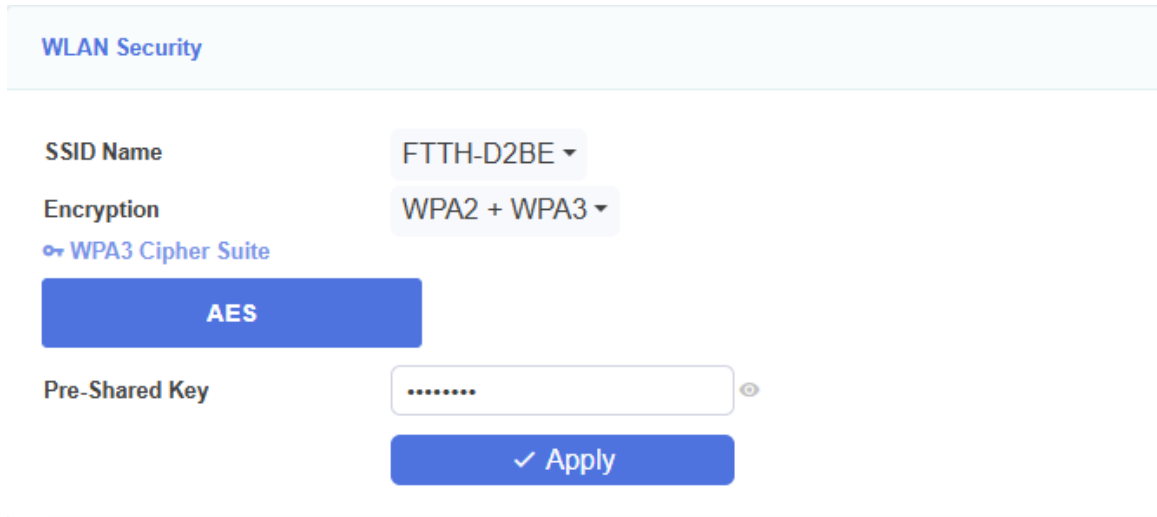
Regdomain: (8) CN ▾

✓ Apply

Figure 4-6-2: WLAN basic settings

## 3) Configure network authentication

Choose “Network > 2.4G Basic Settings> WLAN Security” in navigation menu. Select the SSID and set up WPA2+WPA3 for its network authentication method and AES for its encryption method. Fill a password in passphrase textbox.



The image shows the 'WLAN Security' configuration page. It includes a title bar 'WLAN Security'. Below it, there are two dropdown menus: 'SSID Name' set to 'FTTH-D2BE' and 'Encryption' set to 'WPA2 + WPA3'. Under 'Encryption', there is a link 'WPA3 Cipher Suite' with a plus icon. Below this link is a blue button labeled 'AES'. Further down is a 'Pre-Shared Key' field with a masked password '.....' and a toggle icon. At the bottom is a blue button with a checkmark and the text 'Apply'.

Figure 4-6-3: WLAN security settings

#### 4) Surf the Internet

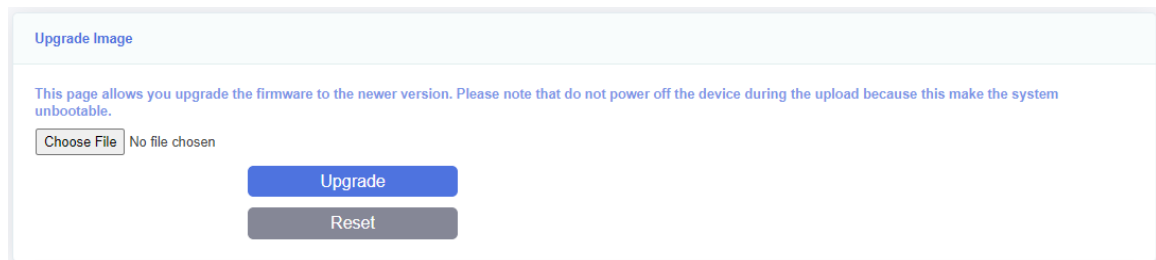
Search SSID named FTTH-D2BE with a laptop, double-click to connect and enter the correct password.

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.



The image shows the 'Upgrade Image' page. It has a title bar 'Upgrade Image'. Below the title bar is a warning message: '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.' Below the warning is a file selection area with a button 'Choose File' and the text 'No file chosen'. At the bottom are two buttons: 'Upgrade' (blue) and 'Reset' (grey).

Figure 4-7-1: Update software

## 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 fibre is broken down or connection loosened.  
(2) Optical power is too low.  
(3) The fibre 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.

## 6 Technical Specifications

Item Name	TONT-4600A
Art. Number	308704
<b>Interface</b>	
PON	1XPON port (EPON PX20+ and GPON Class B+)
	SC single mode, SC/UPC connector
	TX optical power: 0~+4dBm
	RX sensitivity: -27dBm
	Overload optical power: -3dBm (EPON) or - 8dBm (GPON)
	Transmission distance: 20KM
	Wavelength: TX 1310nm, RX1490nm
User interface	4 x GE, Auto-negotiation, RJ45 ports
Antenna	4 x external antennas + 1 x internal antenna
USB	1 x USB3.0 for shared storage/printer
<b>Function data</b>	
O&M	WEB/TELNET/OAM/OMCI/TR069
	Support private OAM/OMCI protocol
Internet connection	Support Routing Mode
Multicast	IGMP v1/v2/v3, IGMP snooping, MLD v1/v2 snooping
Wi-Fi	Wi-Fi 6: 802.11a/n/ac/ax 5GHz & 802.11g/b/n/ax 2.4GHz
	Wi-Fi Encryption: WPA/WPA2/WPA3
	Support OFDMA, MU-MIMO, Dynamic QoS, 1024-QAM
	Smart Connect for one Wi-Fi name
	One SSID for 2.4GHz and 5GHz dual band
L2	802.1 p Cos,802.1Q VLAN
L3	IPv4/IPv6, DHCP Client/Server, PPPoE, NAT, DMZ, DDNS
Firewall	Anti-DDOS, Filtering Based on ACL/MAC/URL
<b>Electrical</b>	
Power adapter	DC 12V, 1.5A, external AC-DC power adaptor, ≤18W
Indicators	PWR, PON, LOS, WAN, LAN1~4, 2.4G, 5.0G, WPS, USB
Interfaces	1*XPON + 4*GE + 1*USB3.0+ Wi-Fi6
<b>General</b>	
Operating condition	Operating temperature: -10 ~ +55°C
	Operating humidity: 5 ~ 95% (non-condensing)
Storage condition	Storage temperature: -40 ~ +70°C
	Storage humidity: 5~ 95% (non-condensing)
Packaging size (L x W x H) / Net weight	260.4 x 157.4 x 45.8mm / 0.55Kg

## 7 EU Declaration of Conformity

The product Declaration of Conformity can be downloaded from the product page at [www.triax.com](http://www.triax.com)

## 8 Conditions of warranty

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

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

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

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

### **THE WARRANTY IS NOT APPLIED IF**

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

### **NOTE**

Date of production can be found in the product's serial number code. The format is "YYWW1234567 (YEAR, WEEK, 123456 product unique number), e.g. 25320000020 = year 2025 week 32, product No.20 of this batch.

