

Model: BD-ONT-214GWI-AC

4LAN+1POTS+WiFi(Dual Band)

DUAL MODE HGU USER MANUAL

Version V1.0

Release Date 2020-10-16

Contents

Chapter 1 Product Introduction 1
1.1 Product Description 1
1.2 Special features 1
1.3 Technical parameters 2
1.4 Application chart 2
1.5 Panel description 3
Chapter 2 Quick Installation 5
2.1 Standard Packing Contents 5
2.2 Quick Installation 5
2.3 Set up Connection 6
Chapter 3 Configuration 7
3.1 Login 7
3.2 Status 7
3.2.1 Device Info 7
3.2.2 WAN Connection Info 8
3.2.3 User Information 9
3.2.4 VoIP Information 10
3.2.5 TR069 Status 10
3.3 Network 11
3.3.1 Internet 11
3.3.2 NAT2 Config 12
3.3.3 Binding Settings 12
3.3.4 LAN Settings 13
3.3.5 WLAN (5G) 15
3.3.6 WLAN (2.4G) 19
3.3.7 TR069 22
3.3.8 QoS 24
3.3.9 Time 27

3.3.10 Route 28
3.4 Security 29
3.4.1 WAN Access 29
3.4.2 Firewall 30
3.4.3 MAC Filtering 31
3.4.4 IP/Port Filtering 31
3.5 Application 33
3.5.1 DDNS 33
3.5.2 Advanced NAT 34
3.5.3 UPNP 36
3.5.4 VoIP 36
3.5.5 IGMP 41
3.5.6 MLD 41
3.5.7 Daily Application 42
3.6 Management 42
3.6.1 User Management 42
3.6.2 Device Management 43
3.6.3 Log File 45
3.6.4 Maintain 46
3.7 Diagnose 46
3.7.1 Network diagnostics 46
3.7.2 Loopback detect 47
3.7.3 Port state 48
3.8 Help 48
Chapter 4 Examples 49
4.1 Internet service 49
4.1.1 Requirement 49
4.1.2 Steps 49
4.2 IPTV service 51
4.2.1 Requirement 51

4.2.2 Steps 51
4.3 VoIP service 54
4.3.1 Requirement 54
4.3.2 Steps 54
4.4 Internet and IPTV service mixed 57
4.4.1 Requirement 57
4.4.2 Steps 57
4.5 Internet, IPTV and VOIP service mixed 60
4.5.1 Requirement 60
4.5.2 Steps 60
4.6 WLAN service 64
4.6.1 Requirement 64
4.6.2 Steps 64
4.7 Update image 67
Chapter 5 FAQ 68

Chapter 1 Product Introduction

1.1 Product Description

Thank you for choosing the 4LAN+1POTS+WiFi Home Gateway Unit. The terminal devices are designed for fulfilling FTTH and triple play service demand of fixed network operators or cable operators. The box is based on mature GPON and Gigabit EPON technology, which has high ratio of performance to price, and the technology of 802.11n WiFi(2T2R), 802.11ac WiFi(2T2R), Layer 2/3, and high quality VoIP as well. They are highly reliable and easy to maintain, with guaranteed QoS for different service. And it is fully compliant with GPON and EPON technical regulations such as ITU-T G.984.x, IEEE802.3ah and technical requirement of EPON equipment from China Telecom. Dual mode HGU can detect and exchange PON mode automatically.



Figure 1-1: 4LAN+1POTS+WiFi(Dual band) Dual Mode HGU

1.2 Special 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.
- Fully compatibility with OLT based on Broadcom/PMC/Cortina chipset.
- Support 802.11n WiFi(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.

1.3 Technical parameters

Technical items	Descriptions
PON interface	1GPON/EPON connector, SC single-mode/single-fiber. GPON: uplink 1.25Gbps, downlink 2.5Gbps; EPON: symmetric 1.25Gbps.
Wavelength	Tx1310nm,Rx 1490nm
Optical interface	SC/UPC connector.
Interface	4* 10/100/1000Mbps adaptive Ethernet interfaces, RJ45 connector. 1* POTS, RJ11 connector.
Wireless	Compliant with IEEE802.11b/g/n/ac, up to 1.167Gbps, 4T4R(four external antennas).
LED	9 indicators, for status of POWER, PON, LOS, WAN, LAN, WIFI, POTS.
Operating condition	-5℃～55℃，10%～90%（non-condensed）
Storing condition	-30℃～60℃，10%～90%（non-condensed）
Power supply	DC 12V, 1.5A
Power consumption	≤12W
Dimension	180mm*120mm*35mm(L*W*H)
Net weight	0.36Kg

1.4 Application chart

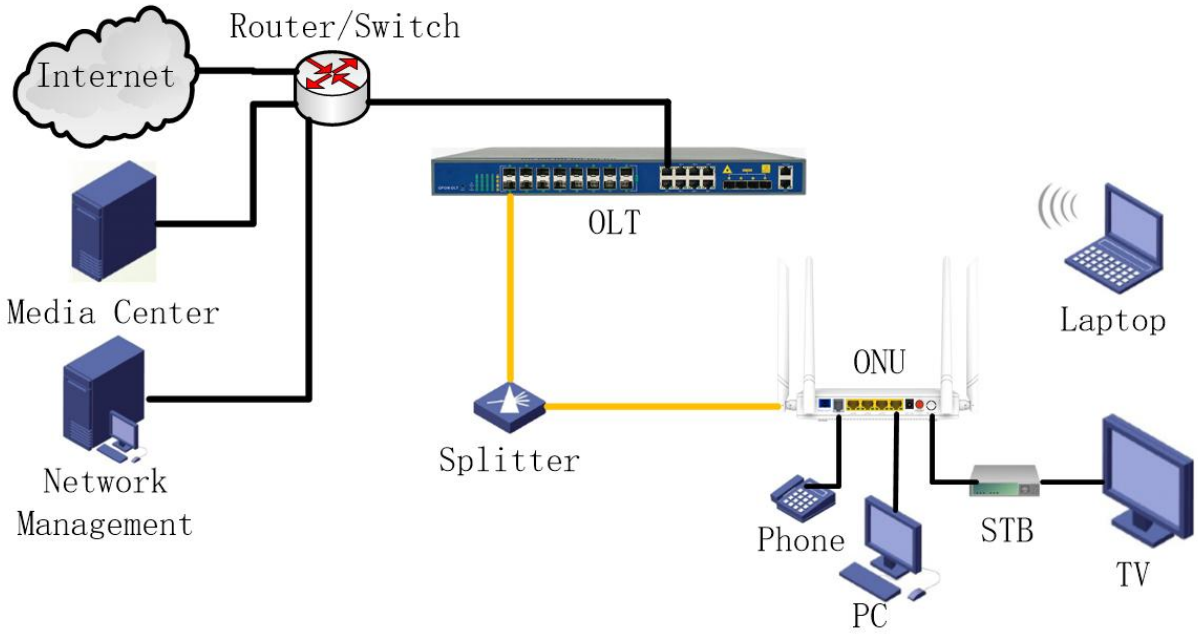


Figure 1-2: Application chart

1.5 Panel description

Interface panel

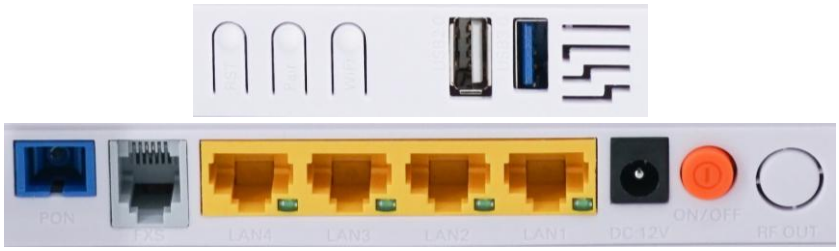


Figure 1-3: Interface panel

Name	Function
PON	Connect GPON or EPON port with internet by SC type, single mode optical fiber cable.
FXS	Connect the telephone with FXS port by telephone wire.
LAN1-LAN4	Connect PC with HGU Ethernet port by RJ-45 CAT5 cable.
DC 12V	Connect with power adapter.
ON/OFF	Power supply switch.
RST	Press down reset button to make the device restart and recover from the factory default settings.

Pair(wireless pair)	Press down Wi-Fi pair button for WPS function.
WiFi	Press down Wi-Fi button to enable/disable Wi-Fi function.

Indication Panel



Figure 1-4: Indication panel

Name	Status	Function
PWR	OFF	Power is not supplied.
	ON	Power is supplied.
PON	OFF	Device is not registered to OLT.
	ON	Device has been registered to OLT.
	Flash	Device registered incorrect.
LOS	OFF	Received optical power is normal.
	Flash	Received optical power is lower than the sensitivity of the optical receiver.
WAN	OFF	Router mode WAN connection status is down.
	ON	Router mode WAN connection status is up.
LAN1/LAN2	OFF	Device is power off or Ethernet link is not established.
	ON	Ethernet link is established but without ongoing data
	Flash	The port is ongoing data transmission.
2.4G/5G	OFF	Device is power off or WiFi is turned off.
	ON	WiFi is turned on.
	Flash	WiFi is turned on and with ongoing data transmission.
PHONE	OFF	Device is power off or not registered to the soft-switch.
	ON	Device has registered to the soft-switch.
	Flash	The port is working.

Chapter 2 Quick Installation

2.1 Standard Packing Contents

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

Contents	Description
4LAN+1POTS+WiFi Home Gateway	1 pc
Power Adapter	1 pc
Installation Guide	1 pc

2.2 Quick Installation

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

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

While connecting, please note:

- Keep the optical connector and the optical fiber clean.
- Make sure there are no tight bends in the fiber and that the bending diameter is greater than 6cm. Otherwise, the optical signal loss may be increased, to the extent that signal may be unavailable.
- Cover all optic ports and connectors with protective cap to guard against dust and moisture when the fiber is not used.

2. Apply power to the unit. Push the power button.
3. After the HGU is power ON, Indicators should light up as for normal operation. Check whether the PON interface status LED (PON) is on continuously. 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

fiber. Please refer to the Layout Description section of this installation manual for normal LED activity.

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

Unit Installation Adjustment

Installing the HGU on a horizontal surface (Bench top)

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

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

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

a) Insert the screws into the wall. The screw positions must be in the same horizontal line and the distance between them must be 165mm. Reserved at least 6mm between the screw caps and the wall.

b) Hang the HGU on the screws through the mounting holes.

2.3 Set up Connection

Set up wired connection

Connect PC with HGU Ethernet port by RJ-45 CAT5 cable.

Set up wireless connection

Choose the wireless network name (SSID) “FTTH-xxxx”, default security mode is WPA2 mixed, password is *12345678*.

Chapter 3 Configuration

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

3.1 Login

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

1、 Conform "2.2 Quick Installation" to install;

2、 The device default IP is 192.168.1.1;

3、 Open web browser, type the device IP in address bar;

4、 Entry of the username and password will be prompted. Enter the default login User Name and Password:

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



Figure 3-1: 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 and so on.

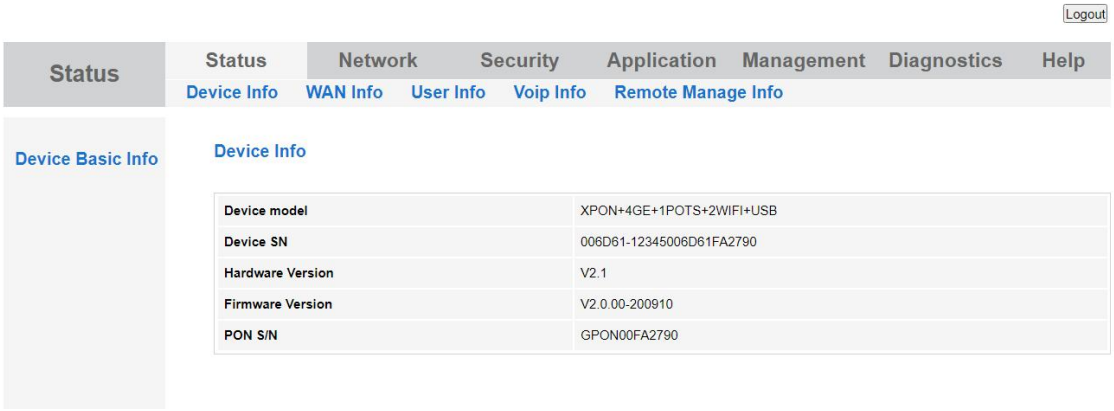


Figure 3-2: Device Information

3.2.2 WAN Connection Info

3.2.2.1 IPv4 Connection Info

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

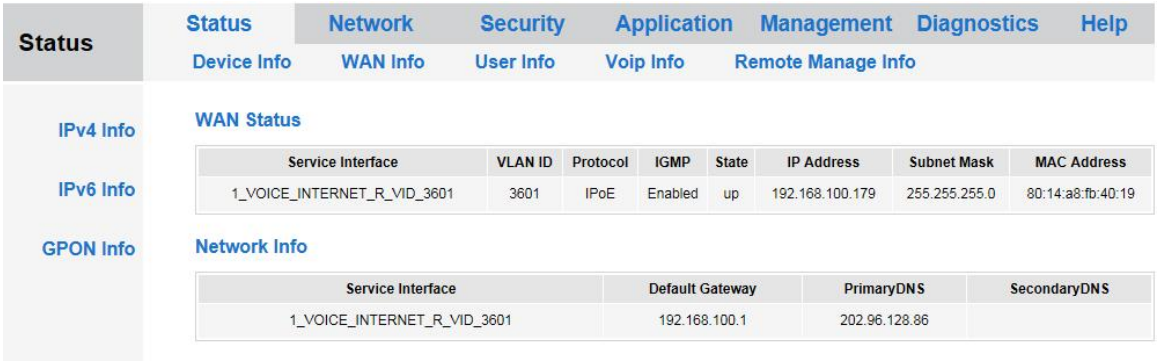


Figure 3-3: IPv4 WAN Information

3.2.2.2 IPv6 Connection Info

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

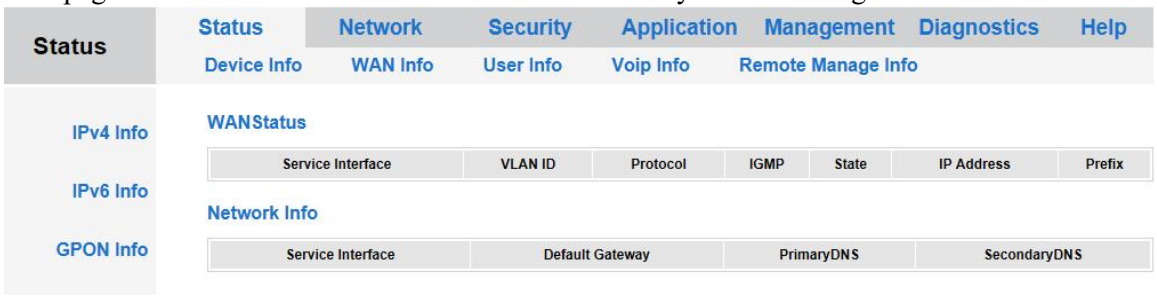


Figure 3-4: IPv6 WAN Information

3.2.2.3 PON Information

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.

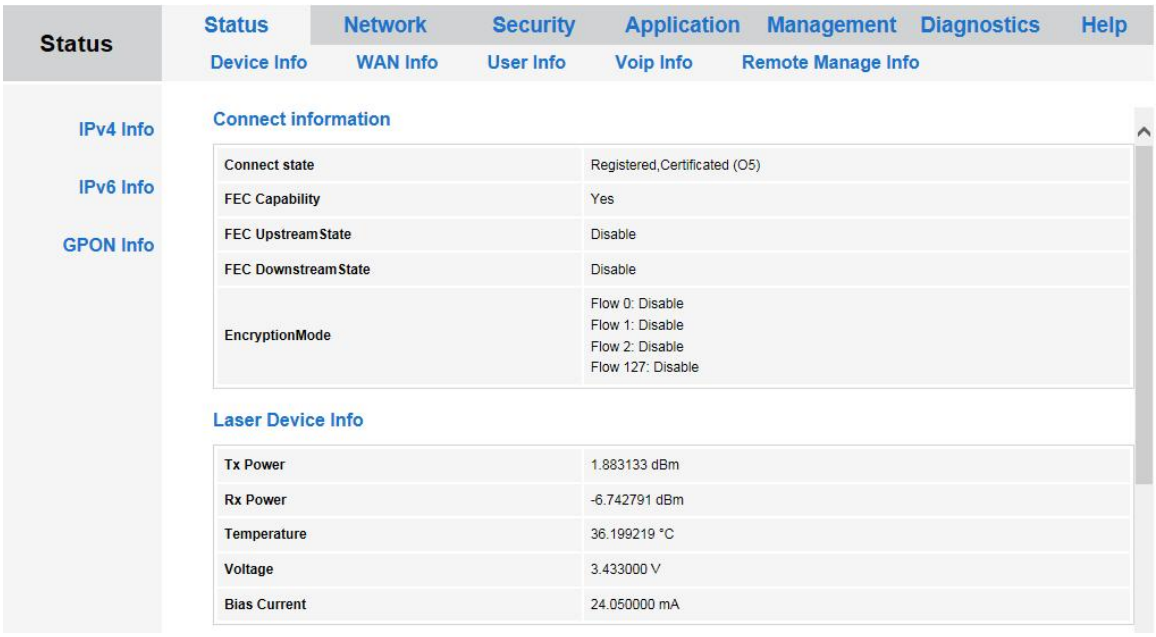


Figure 3-5: PON Information

3.2.3 User Information

3.2.3.1 WLAN Interface Info

This page shows WLAN information, including SSID name, channel, whether enable security or not, statistics of the packet on both send and receive direction and so on.

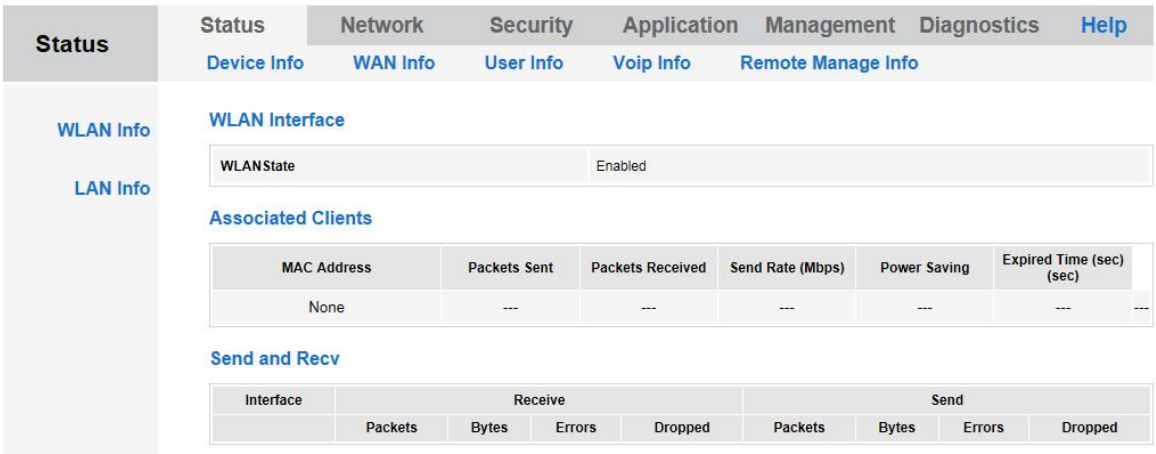


Figure 3-6: WLAN Interface info

3.2.3.2 LAN Interface Info

This page shows LAN information, such as LAN gateway, receive or send packet statistics of LAN interface, list of connected clients.

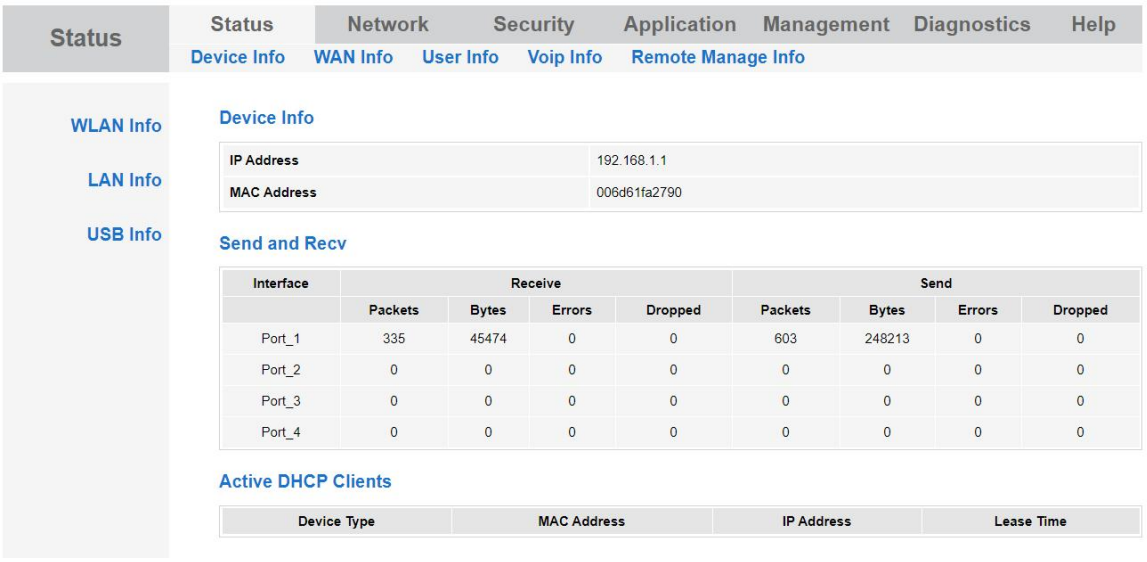


Figure 3-7: LAN Interface info

3.2.4 VoIP Information

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



Figure 3-8: VoIP Info

3.2.5 TR069 Status

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

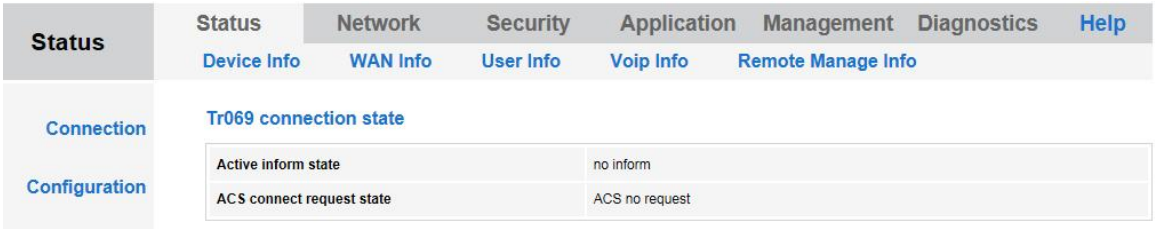


Figure 3-9: TR069 connection Status

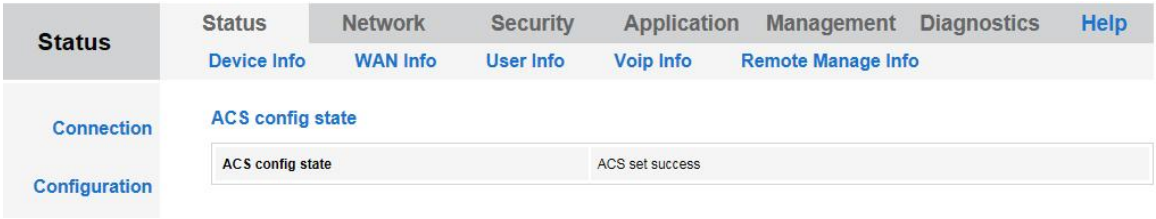


Figure 3-10: TR069 configuration Status

3.3 Network

3.3.1 Internet

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

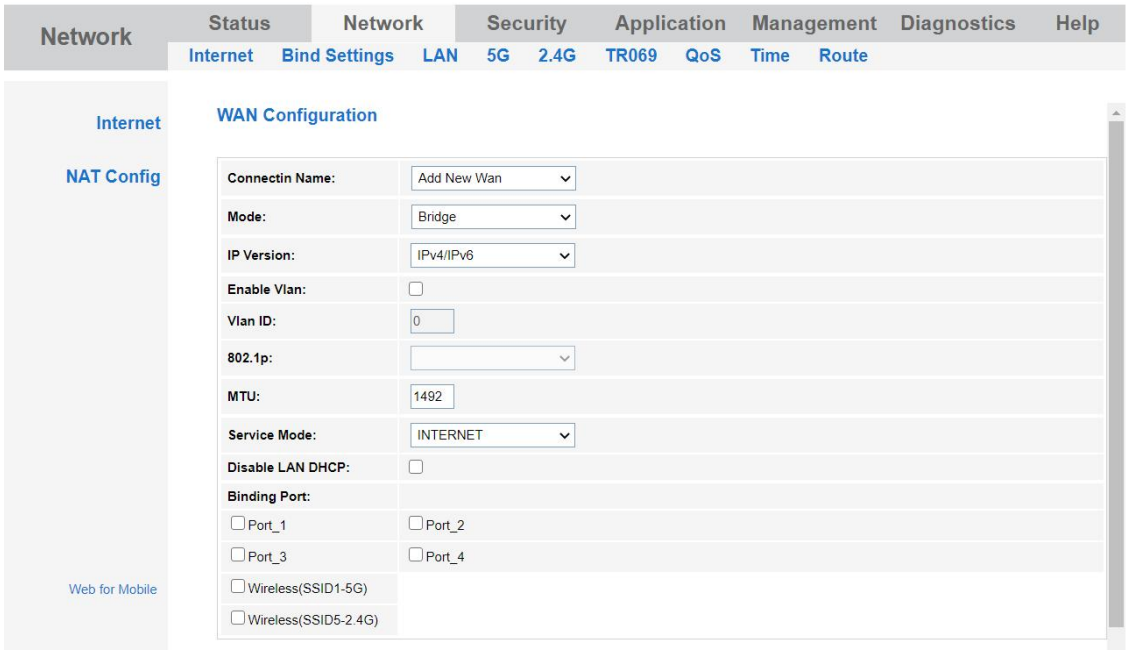


Figure 3-11: Internet

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 "Apply" button. If you want to edit WAN connection, please select the wan connect name you want to edit and change parameters and then click "Apply" button. If you want to delete one connection, please select the wan connection you want to delete and then click "Delete" button.
Mode	**Bridge**: The LAN ports you have selected in this WAN connection and PON port are in the bridge mode. **Route**: The LAN ports you have selected in this WAN connection and PON port are in the route mode.
IP Version	**IPv4**: WAN connections use IPv4 protocol. **IPv6**: WAN connections use IPv6 protocol. **IPv4 & IPv6**: WAN connections use both IPv4 and IPv6 protocol.
IP Mode	**DHCP**: Automatically obtain an IP address from your ISP **Static**: Set the IP address manually

	PPPoE: Select this option if your ISP uses PPPoE
Enable Vlan	**unchecked**: In this wan connection, the packets transmitted by the PON port without VLAN tag. **checked**: In this wan connection, the packets transmitted by the PON port with VLAN tag. **Vlan ID**: input the VLAN ID you want to set. **802.1p**: select the port priority you want to set.
MTU	MTU: max transfer unit. Default Value: 1500 in bridge mode, 1492 in route mode.
NAT	**checked**: enable NAT function **unchecked**: disable NAT function
Request DNS	**Enable**: DHCP server assigns DNS. **Disable**: set DNS manually.
Service Mode	Service mode indicates what the wan connection is used for. E.g.: If this wan connection is used for VoIP, you should select the service mode which contains VOICE, such as TR069_VOICE_INTERNET, TR069_VOICE, VOICE or VOICE_INTERNET.
Disable LAN DHCP	**Checked**: LAN DHCP will not work at the port which binds with the WAN. **Unchecked**: LAN DHCP will work at the port which binds with the WAN.
Port Binding	Showing which LAN port or SSID the wan connection has included.

3.3.2 NAT2 Config

This page is used to configure NAT type. Some devices require NAT type 2 for their services; in this case, you need to enable NAT2.

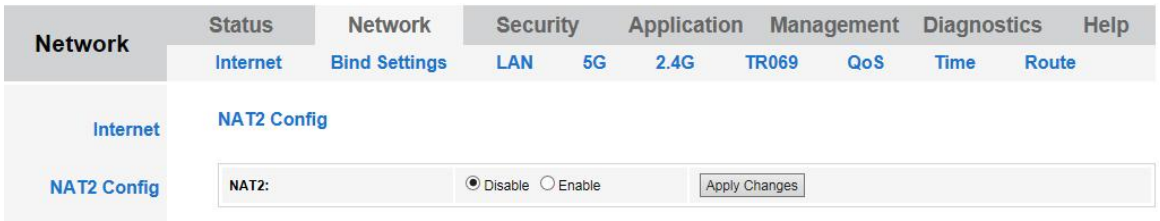


Figure 3-12: NAT2

3.3.3 Binding Settings

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

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

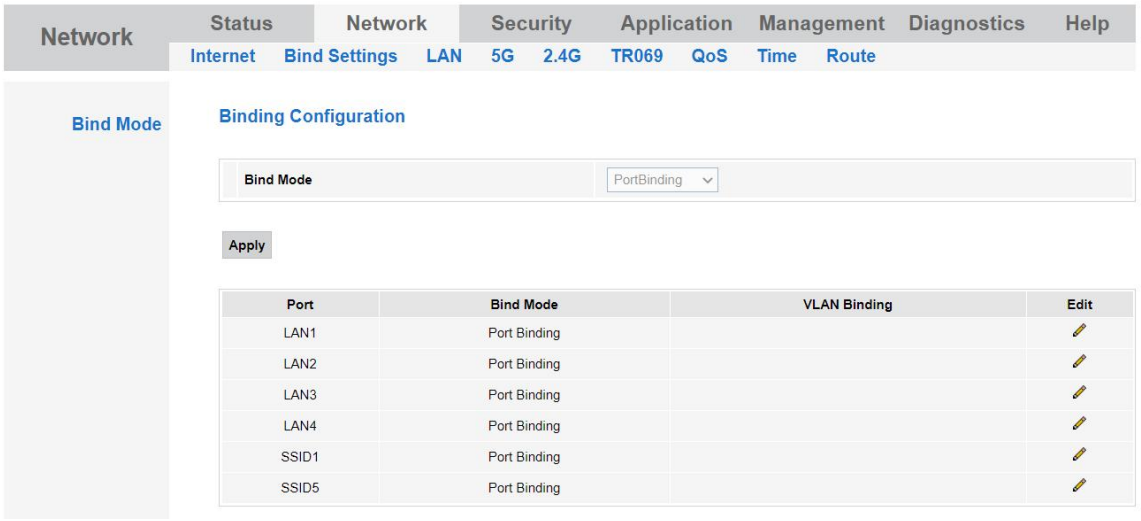


Figure 3-13: Binding Settings

3.3.4 LAN Settings

3.3.4.1 IPv4

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

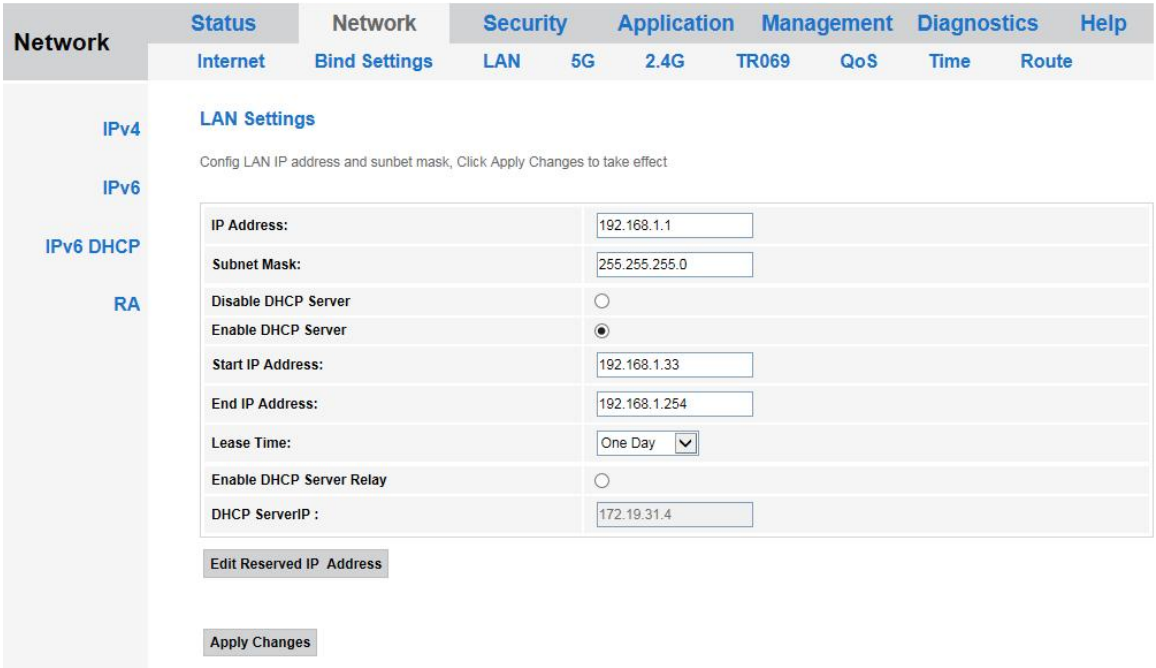


Figure 3-14: IPv4 configuration

Parameters	Illustration

IP Address	LAN IP address.
Subnet Mask	LAN IP mask.
Disable DHCP Server	DHCP Server is disabled.
Enable DHCP Server	Enable HGU DHCP server. **Start IP Address:** The start IP address of address pool. **End IP Address:** The end IP address of address pool. **Lease Time:** Lease time of the IP address.
Enable DHCP Server Relay	Enable DHCP relay. When HGU works on router mode and DHCP server is at WAN side, need to enable DHCP relay so that LAN side devices can get IP addresses by DHCP.
Reserved IP Address	Click "Edit"-"Add" button to configure IP address you want to reserve. If you want to delete one reserve IP configuration, click "Delete" button in "Delete" column.

3.3.4.2 IPv6

This page allows you to configure LAN IPv6 address, LAN IPv6 DNS and IPv6 prefix.

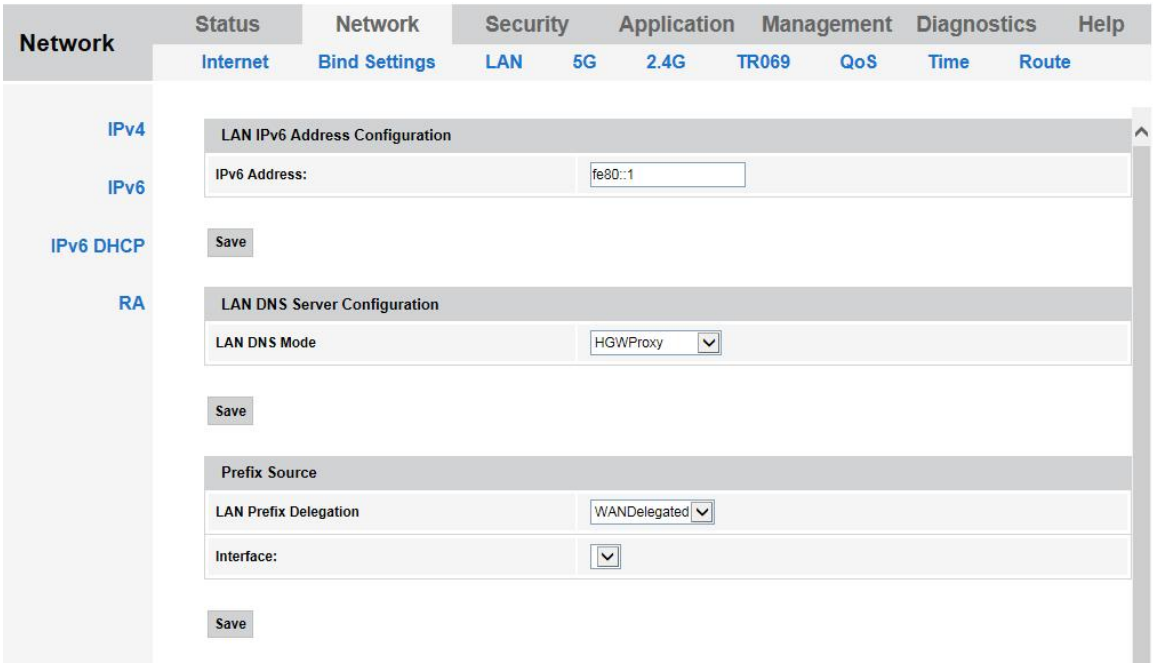


Figure 3-15: IPv6 configuration

Parameter	Illustration
IPv6 address	LAN IPv6 address.
LAN DNS	LAN IPv6 DNS.
LAN IPv6 prefix	LAN IPv6 address prefix.

3.3.4.3 IPv6 DHCP

This page allows you to configure IPv6 DHCP server. This is only switch for IPv6 DHCP server. It is auto configure mode when IPv6 DHCP server is disabled.

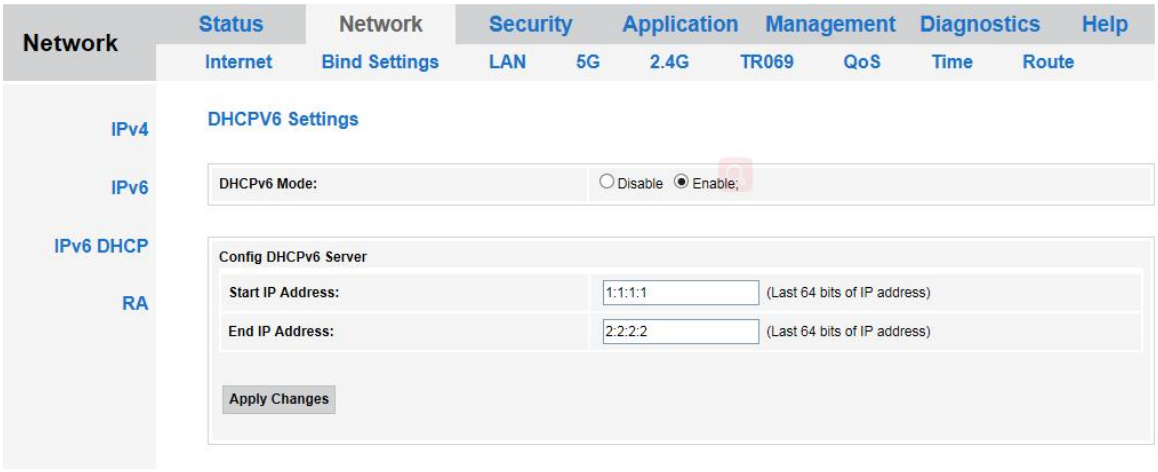


Figure 3-16: IPv6 DHCP server

3.3.4.4 RA Configuration

This page allows you to do RA configuration.



Figure 3-17: RA configuration

3.3.5 WLAN (5G)

This part is used to configure WIFI (5G) parameters. On each page, after configured you should click “Apply Changes” button to save it.

3.3.5.1 WLAN Basic

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.

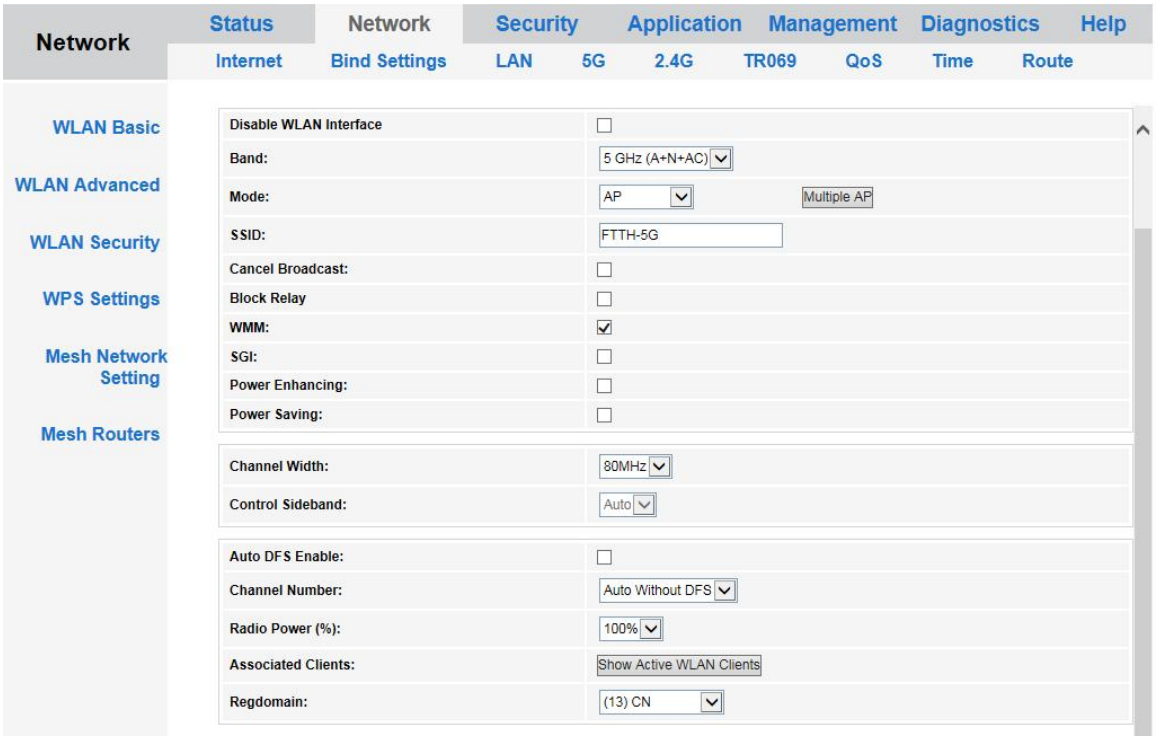


Figure 3-18: WLAN Basic

Parameter	Illustration
Disable WLAN Interface	Enable or Disable WLAN.
Band	Choose 5G WiFi band.
Mode	WLAN work mode, only supports AP mode.
Multiple AP	Configure multiple AP parameters.
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.
SGI	Short Guard Interval. The Guard Interval is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device. To increase data rates, the 802.11n standard added optional support for a 400 nsec guard interval. This would provide an 11% increase in data rates.
Power enhancing	Enhance power.
Power saving	Enable power saving.
Channel width	WLAN channel width.
Auto DFS enable	Enable auto DFS.
Channel Number	WLAN channel, default value is auto.

Radio power	Configure wifi transmit power.
Associated Clients	Show the active WLAN clients
Regdomain	Configure country or region.

3.3.5.2 WLAN advanced

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

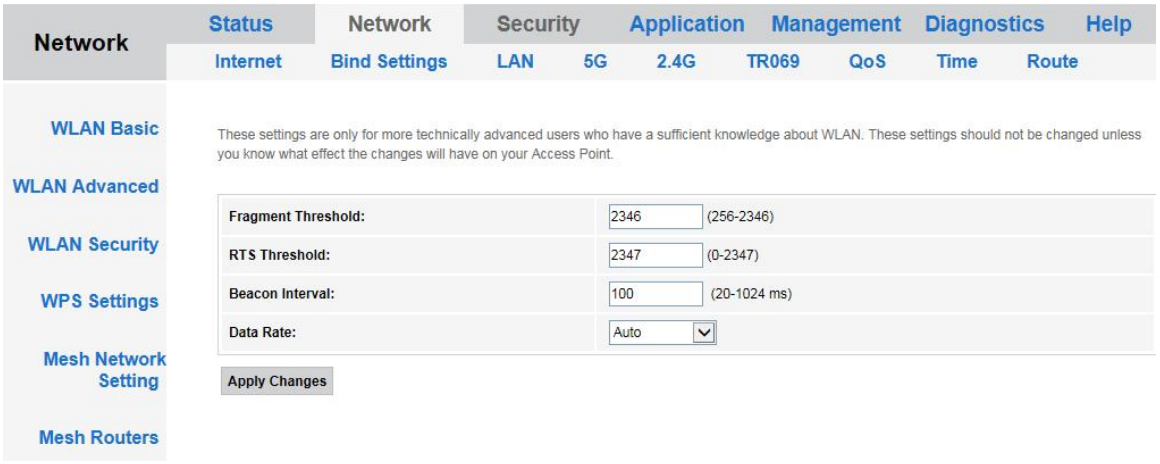


Figure 3-19: WLAN Advanced

3.3.5.3 WLAN security

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

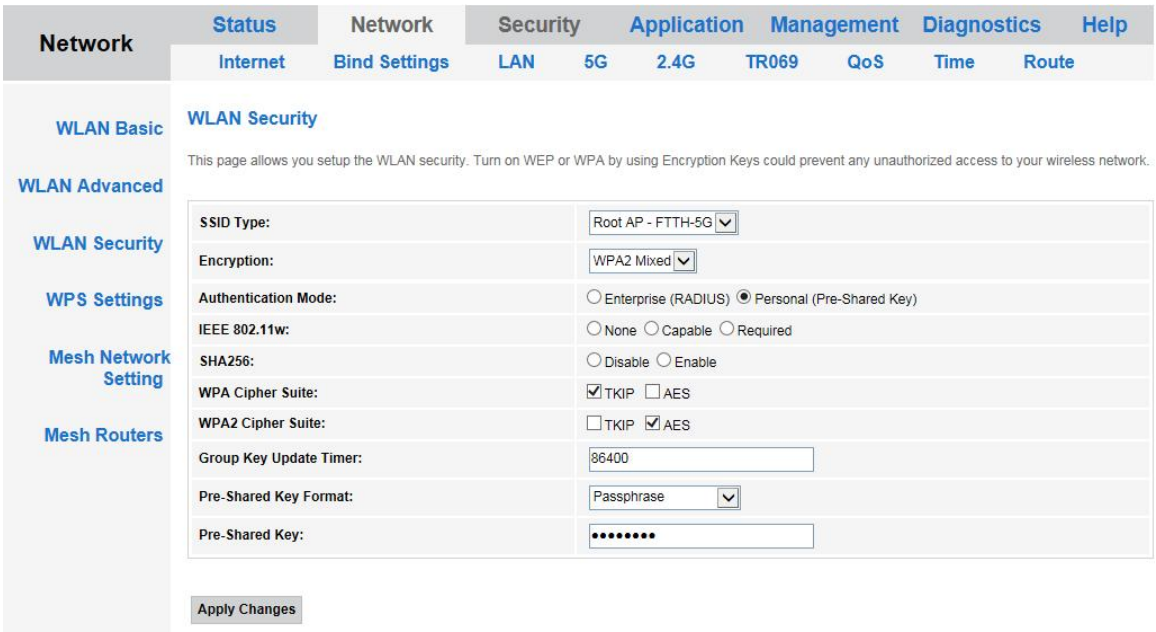


Figure 3-20: WLAN Security

3.3.5.4 WPS settings

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this

feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

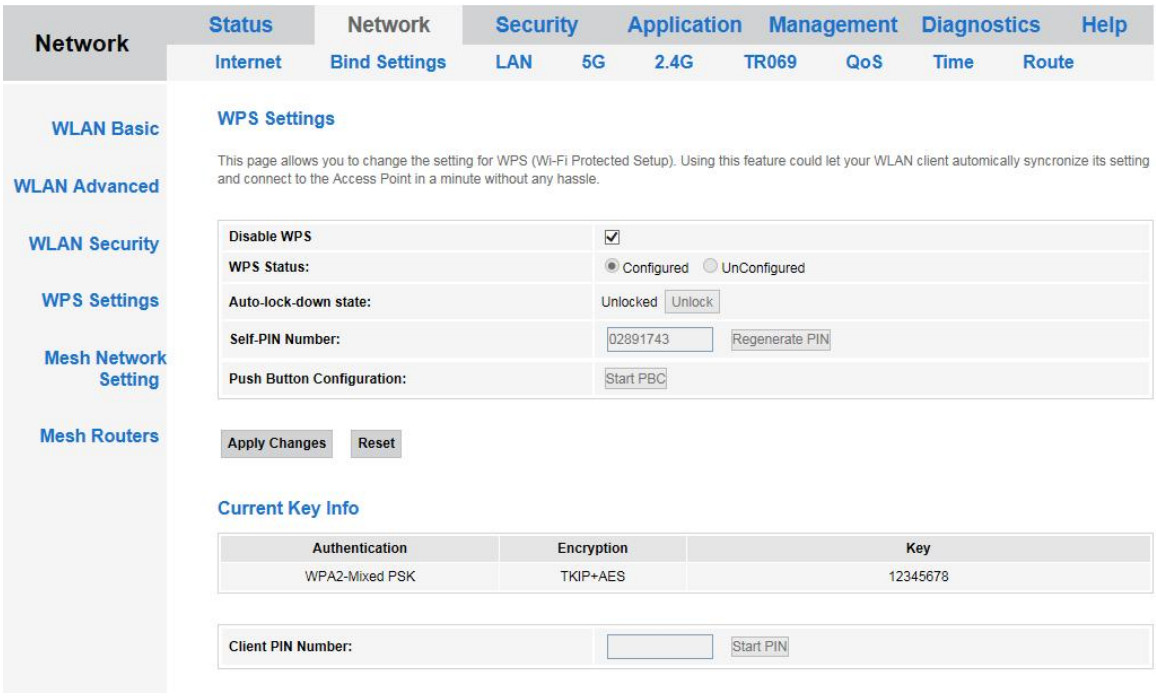


Figure 3-21: WPS Settings

3.3.5.5 Mesh Network Settings

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

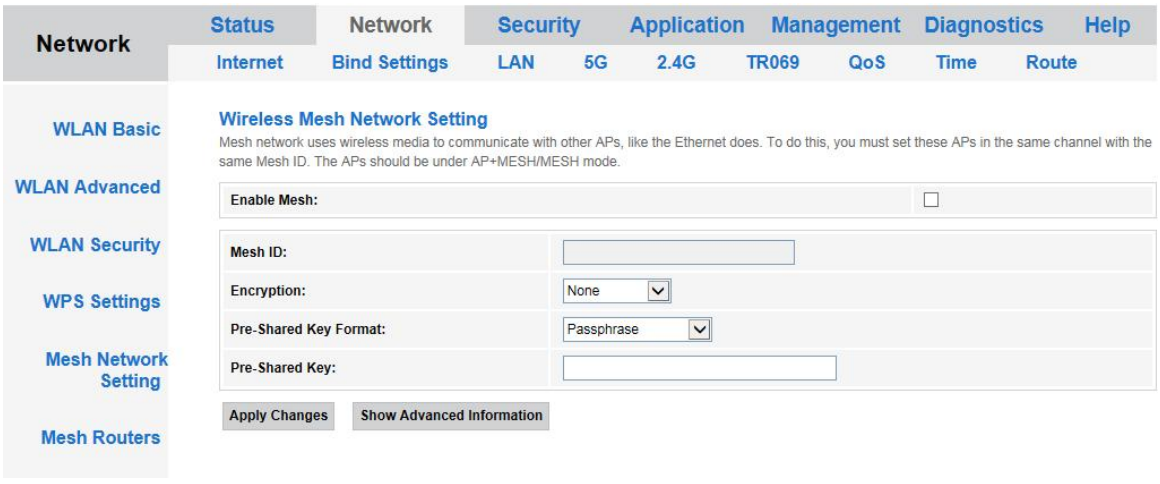


Figure 3-22: Mesh Network Settings

3.3.5.6 Mesh Routers

This page displays the routers in the mesh network.

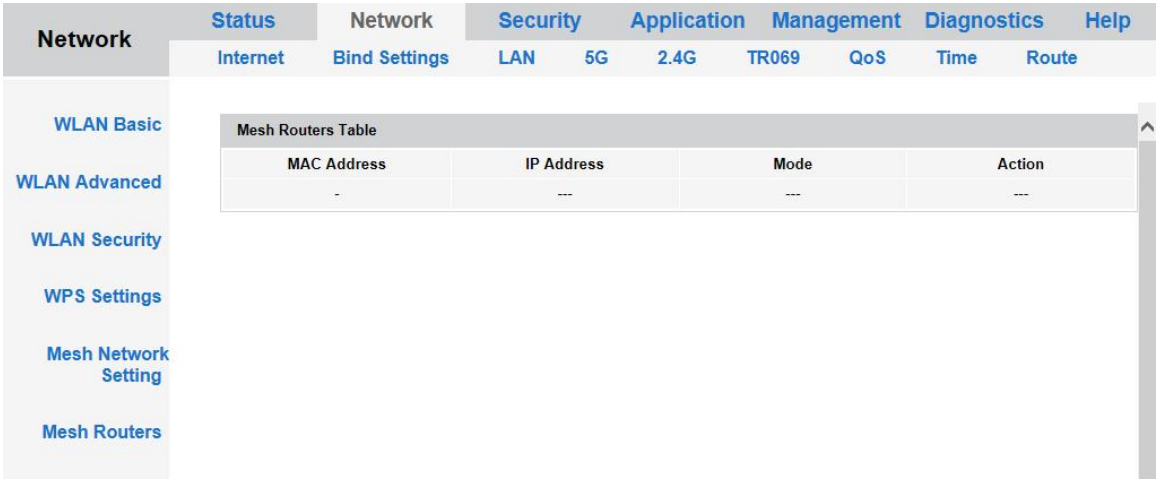


Figure 3-23: Mesh Routers

3.3.6 WLAN (2.4G)

This part is used to configure WIFI (2.4G) parameters. On each page, after configured you should click “Apply Changes” button to save it.

3.3.6.1 WLAN Basic

This page allows you to configure wireless basic settings. Basic settings include wireless switch, WLAN access to web switch, SSID name, channel and so on.

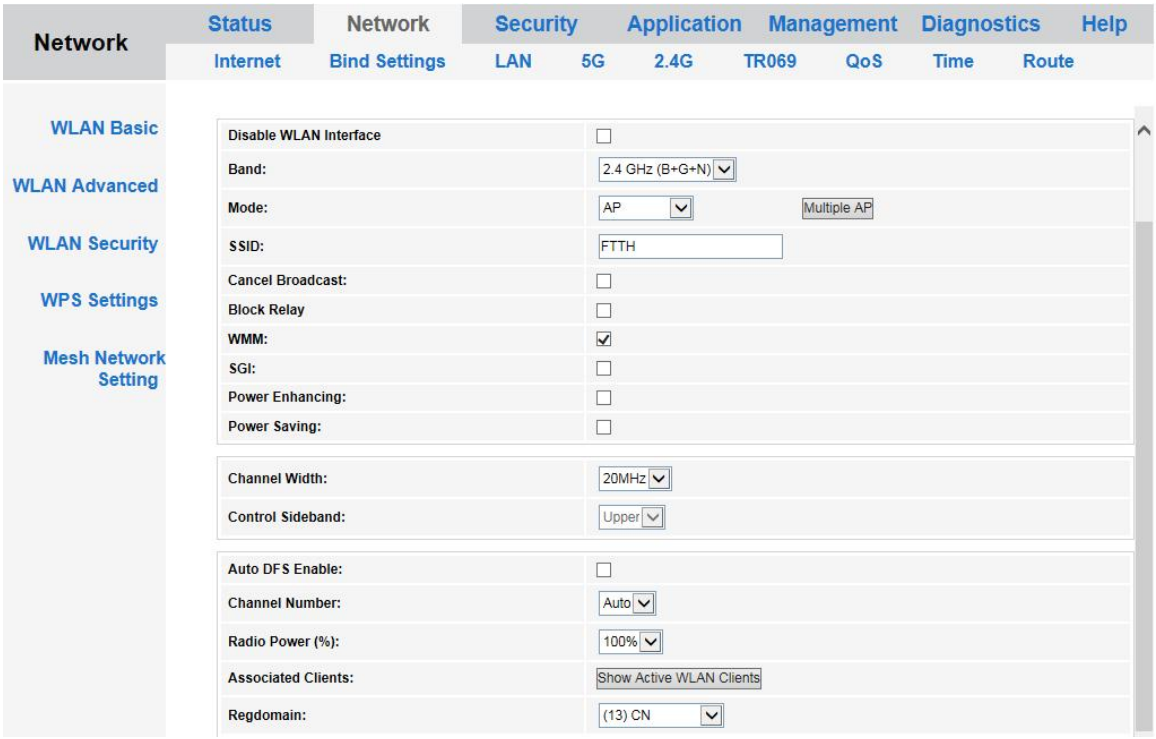


Figure 3-24: WLAN Basic

Parameter	Illustration
Disable WLAN	Enable or Disable WLAN.

Interface	
Band	Choose 2.4G WiFi band.
Mode	WLAN work mode, only supports AP mode.
Multiple AP	Configure multiple AP parameters.
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.
SGI	Short Guard Interval. The Guard Interval is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device. To increase data rates, the 802.11n standard added optional support for a 400 nsec guard interval. This would provide an 11% increase in data rates.
Power enhancing	Enhance power.
Power saving	Enable power saving.
Channel width	WLAN channel width.
Auto DFS enable	Enable auto DFS.
Channel Number	WLAN channel, default value is auto.
Radio power	Configure wifi transmit power.
Associated Clients	Show the active WLAN clients
Regdomain	Configure country or region.

3.3.6.2 WLAN advanced

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

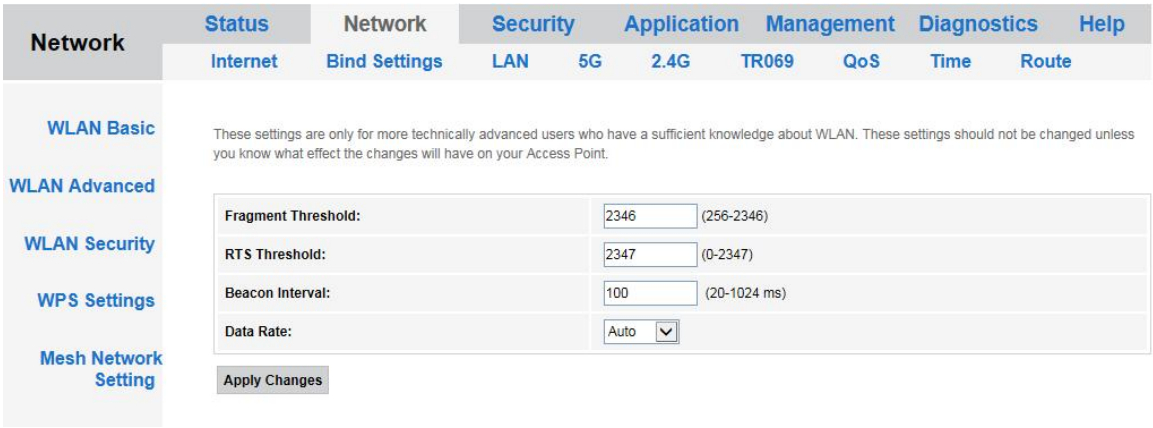


Figure 3-25: WLAN Advanced

3.3.6.3 WLAN security

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

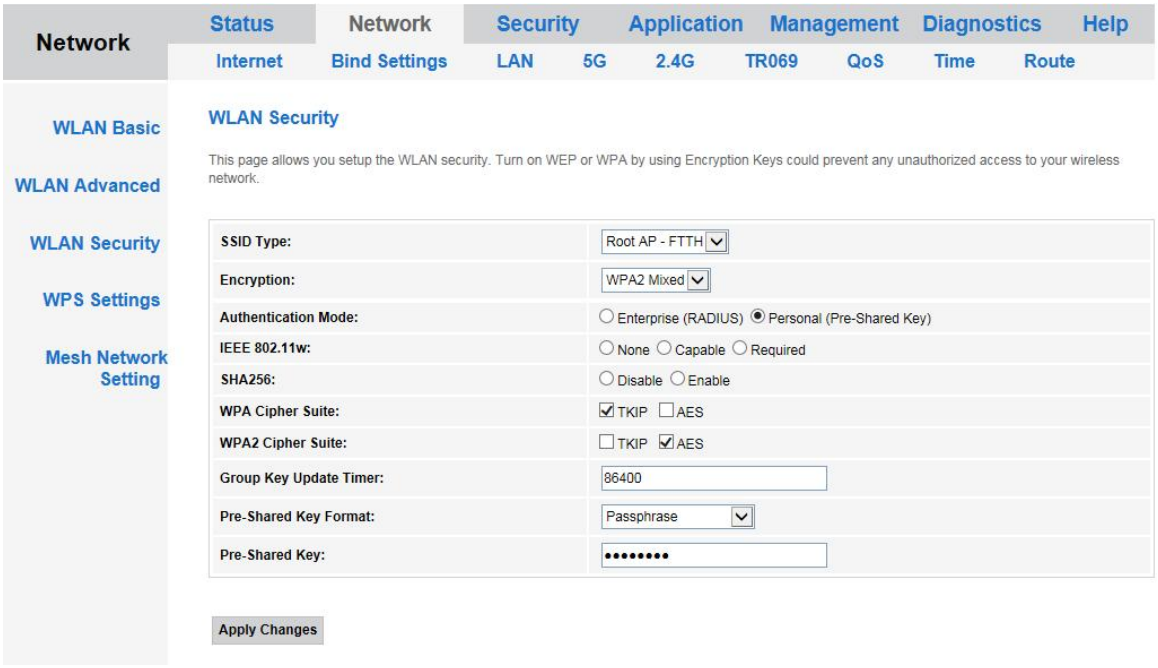


Figure 3-26: WLAN Security

3.3.6.4 WPS Settings

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

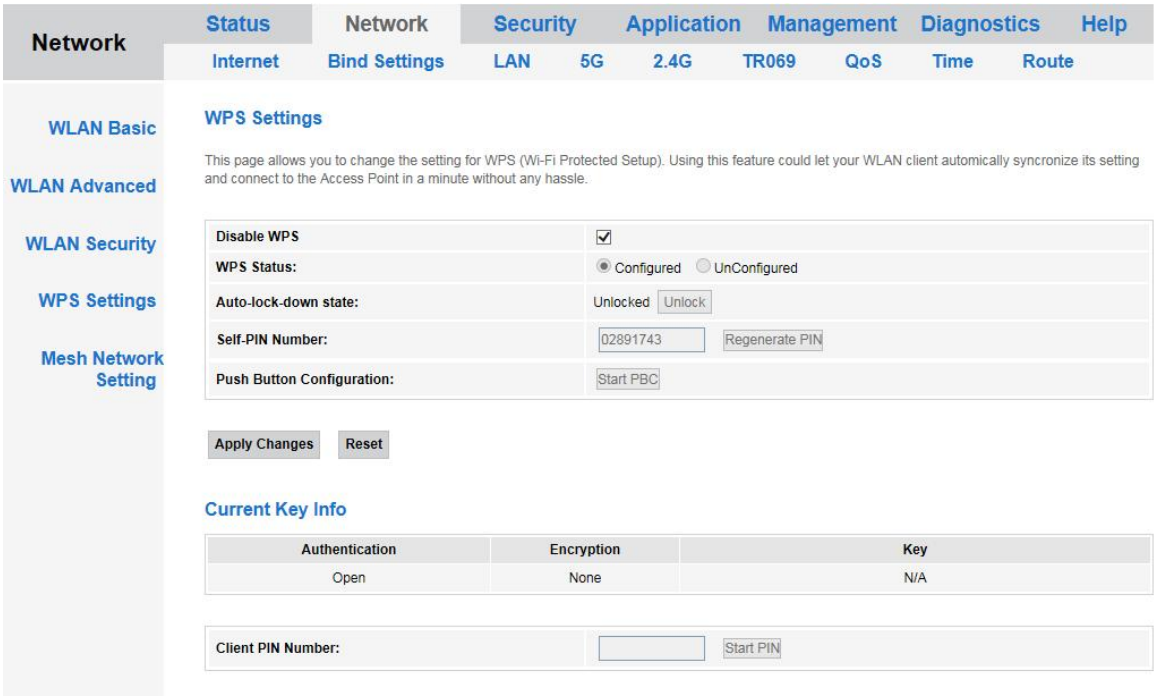


Figure 3-27: WPS Settings

3.3.6.5 Mesh Network Settings

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

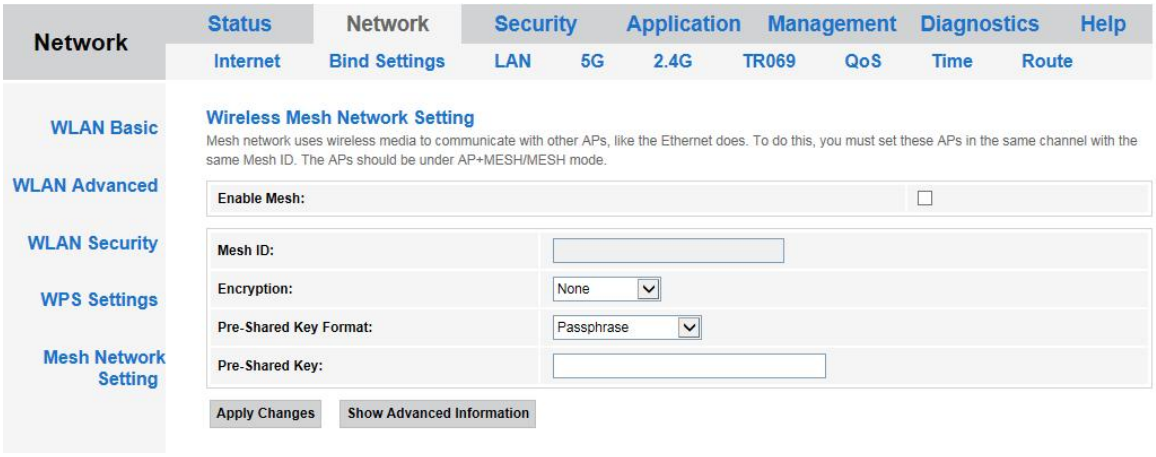


Figure 3-28: Mesh Network Settings

3.3.7 TR069

3.3.7.1 ACS Server

This page allows you to configure ACS connection parameters.

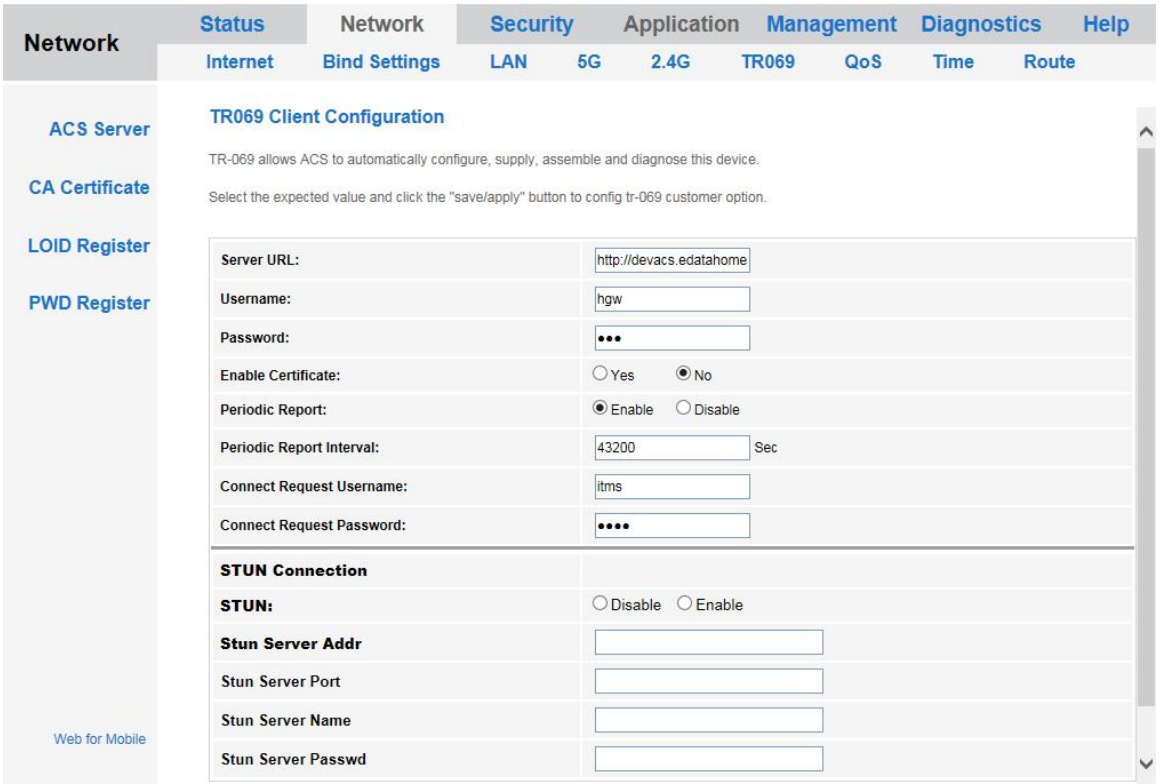


Figure 3-29: ACS server configuration

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.
Enable Certificate	Whether needs certificates or not.
Periodic Report	Switch of inform interval.
Periodic Report Interval	Reconnection interval. HGU will verify connection with ACS server when inform interval times up.
Connection request username	Authentication username for ACS connects to HGU.
Connection request password	Authentication password for ACS connects to HGU.

3.3.7.2 CA Certificate

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

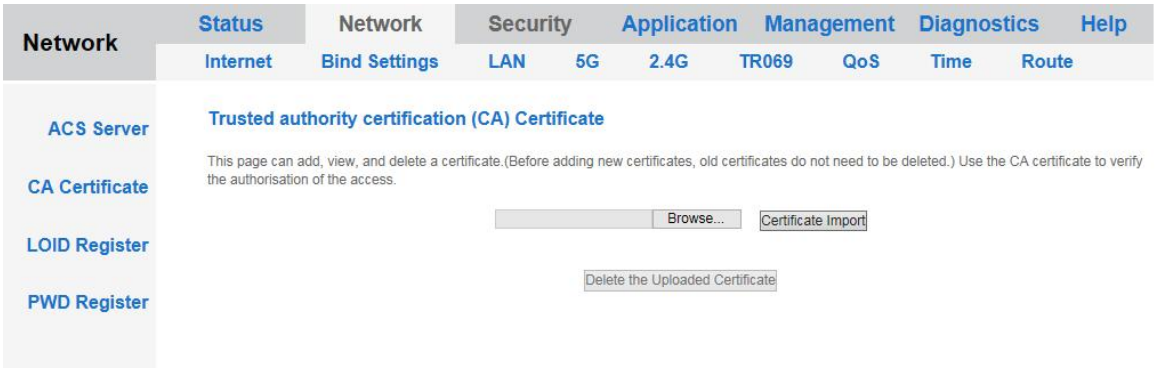


Figure 3-30: upload CA certificate

3.3.7.3 LOID Register

LOID is used for PON authentication.

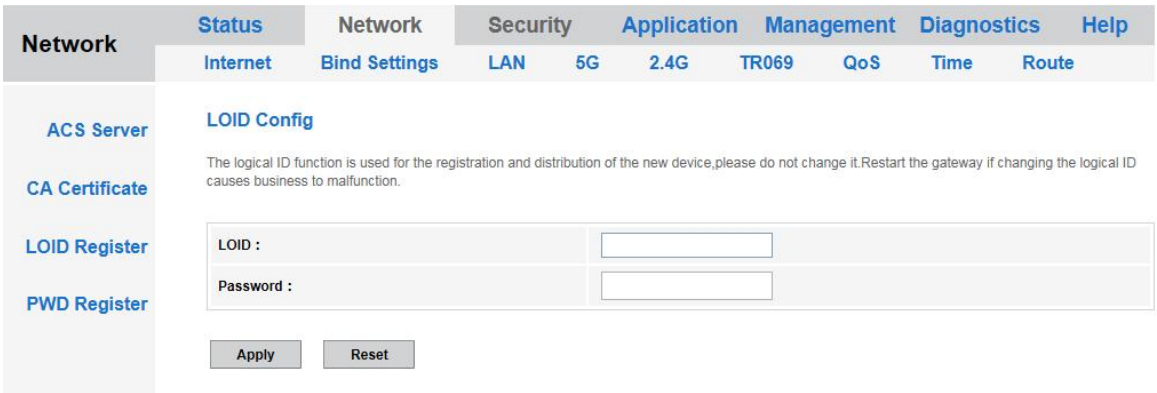


Figure 3-31: LOID configuration

3.3.7.4 PWD Register

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.

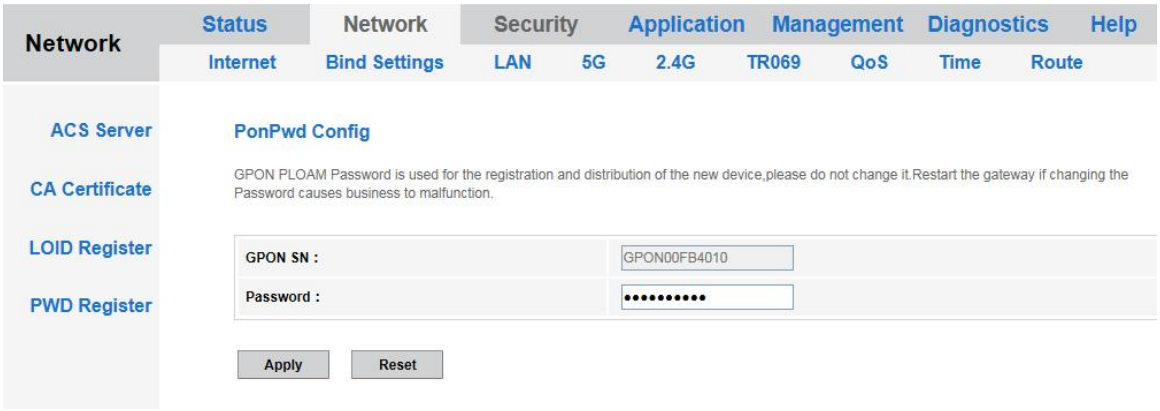


Figure 3-32: Password configuration

3.3.8 QoS

3.3.8.1 QoS Config

This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply greater precedence. If select WRR of policy, please input the weight of this queue. Default is 40:30:20:10. After configuration, please click 'Apply Changes'.

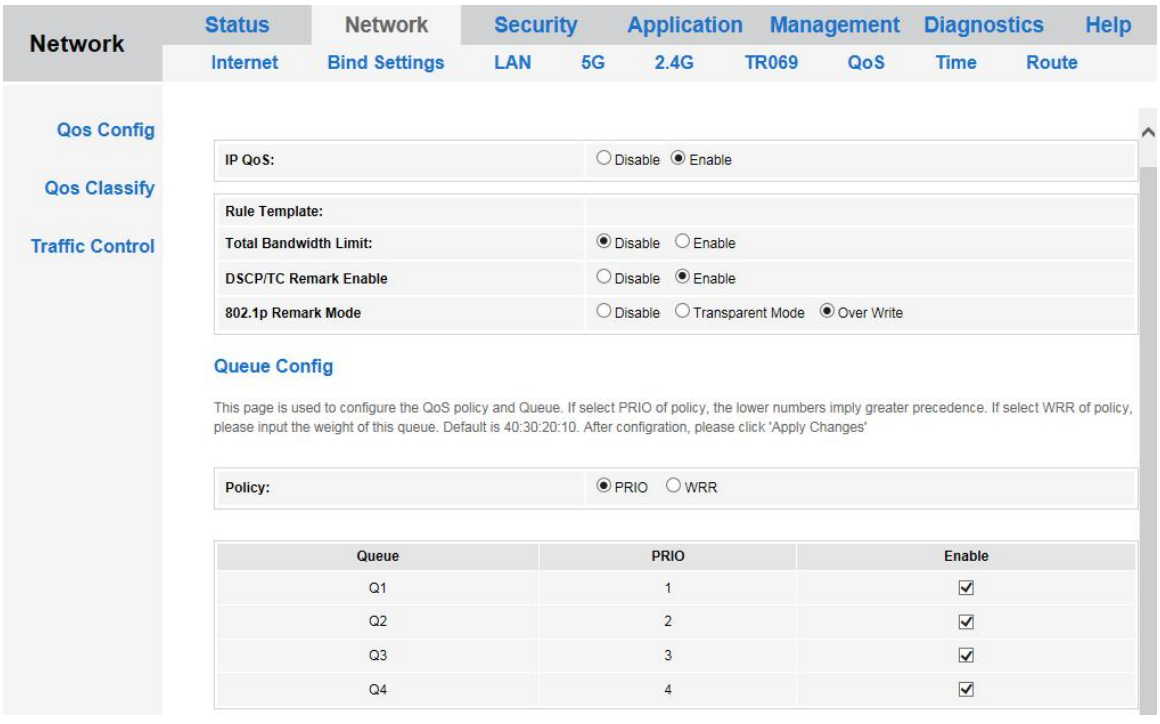


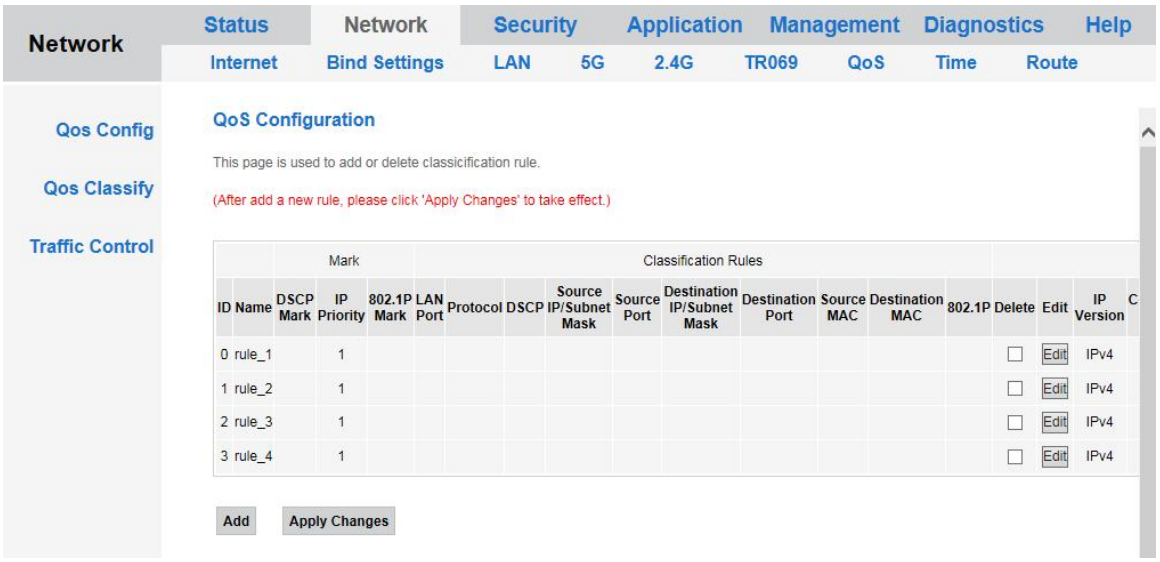
Figure 3-33: QoS Configuration

Parameter	Illustration
IP QoS	Enable or disable QoS.
Total bandwidth limit	Switch of upstream bandwidth limit.

DSCP/TC remark switch	Switch of DSCP/TC remark function.
802.1p remark mode	Switch of 802.1p remark function and remark mode.
Policy	Scheduling policy, including PRIO and WRR.
Queue	Enable queue.

3.3.8.2 QoS classify

This page is used to configure QoS classification rules. Once the data stream is matched to the rule and the rule has bound to the special queue, the data stream's rate will be in schedule depending on the queue setting.



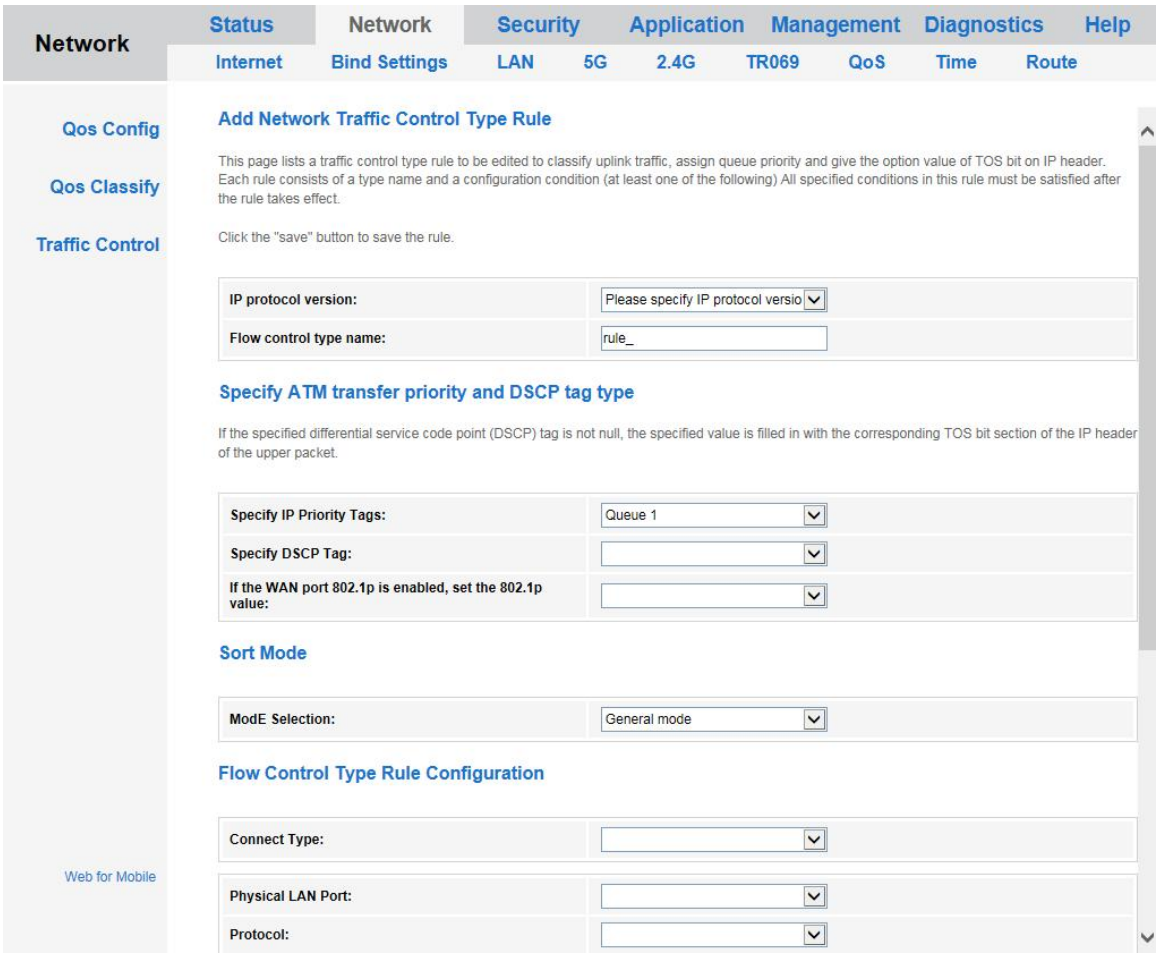


Figure 3-34: QoS classification rule

Parameters	Illustration
DSCP mark	Re-mark DSCP when the data match the QoS classification rules.
IP Priority	The priority which the queue is mapped to.
802.1P mark	Re-mark 802.1p when the data match the QoS classification rules.
LAN port	Classify and mark according to LAN port.
Protocol	Specify IP protocol, which includes TCP, UDP, TCP/UDP, ICMP and RTP.
DSCP	Classify and re-mark according to DSCP field in IP message.
Source IP/subnet mask	Classify and re-mark according to source IP address.
Source port	Classify and re-mark according to source port.
Destination IP/subnet mask	Classify and re-mark according to destination IP address.
Destination port	Classify and re-mark according o destination port.
Source MAC	Classify and re-mark according to source MAC address.

Destination MAC	Classify and re-mark according to destination MAC address.
802.1P	Classify and re-mark according to 802.1p.

3.3.8.3 Traffic control

This page is used to configure total bandwidth and rate of special streams.

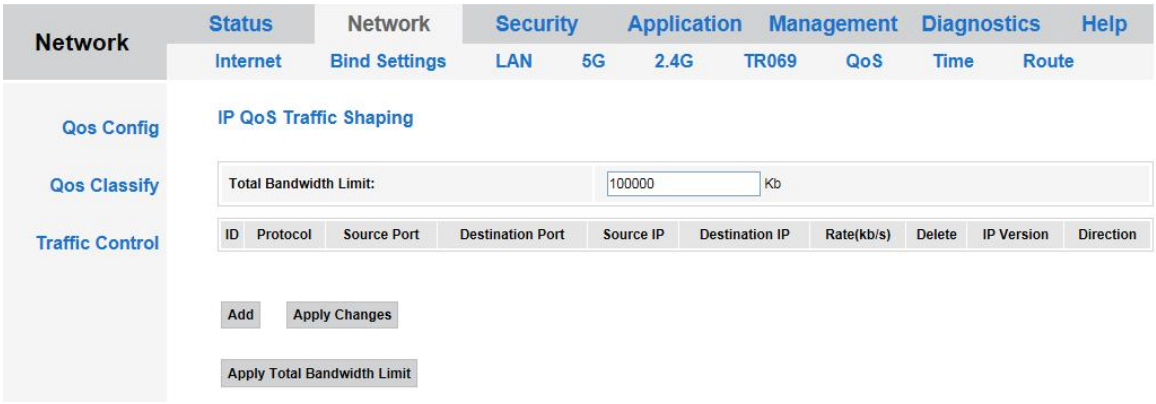


Figure 3-35: Traffic shaping rule

Parameter	Illustration
Protocol	Specify IP protocol type of streams.
Source Port	Specify source port of streams.
Destination Port	Specify destination of streams.
Source IP	Specify source IP address of streams.
Destination IP	Specify destination IP address of streams.
Rate	Set limited rate of streams.
IP version	Specify IP protocol version of streams.
Direction	Specify direction of streams.

3.3.9 Time

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

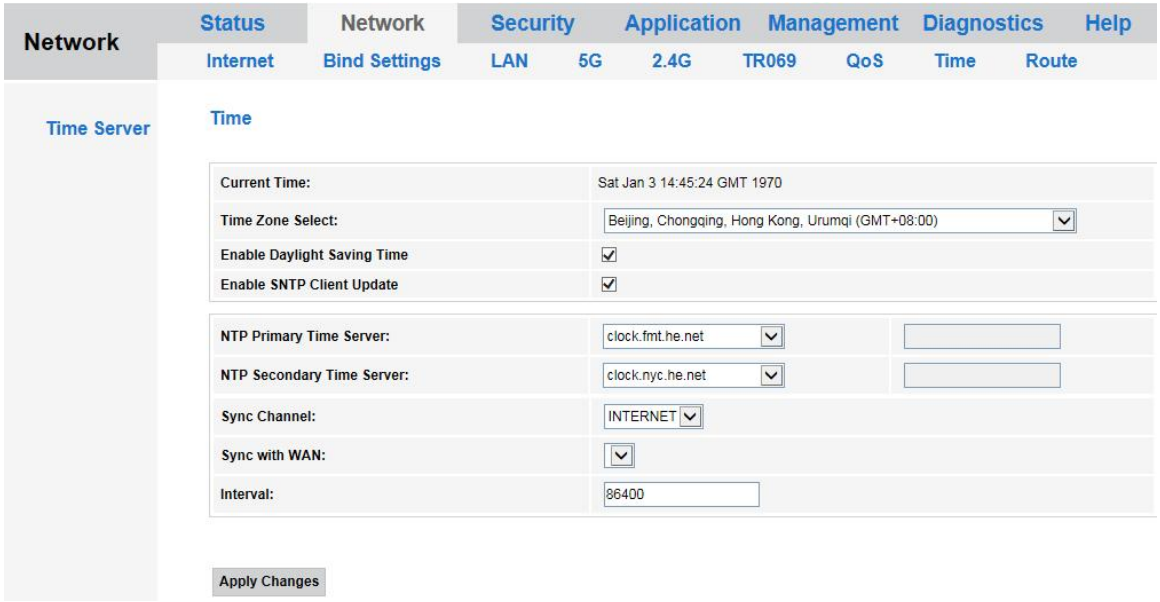


Figure 3-36: Time server

3.3.10 Route

3.3.10.1 RIP Configuration

This page allows you to configure RIP function.

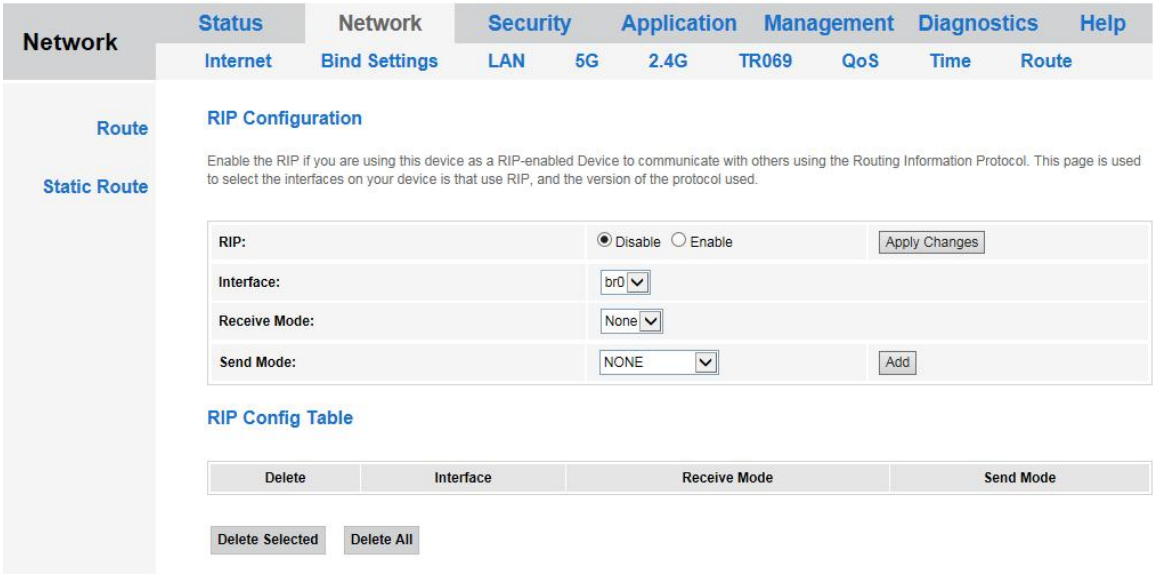


Figure 3-37: RIP configuration

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

RIP configuration table	RIP configuration that has been added.

3.3.10.2 Static route

This page is used to configure static route.

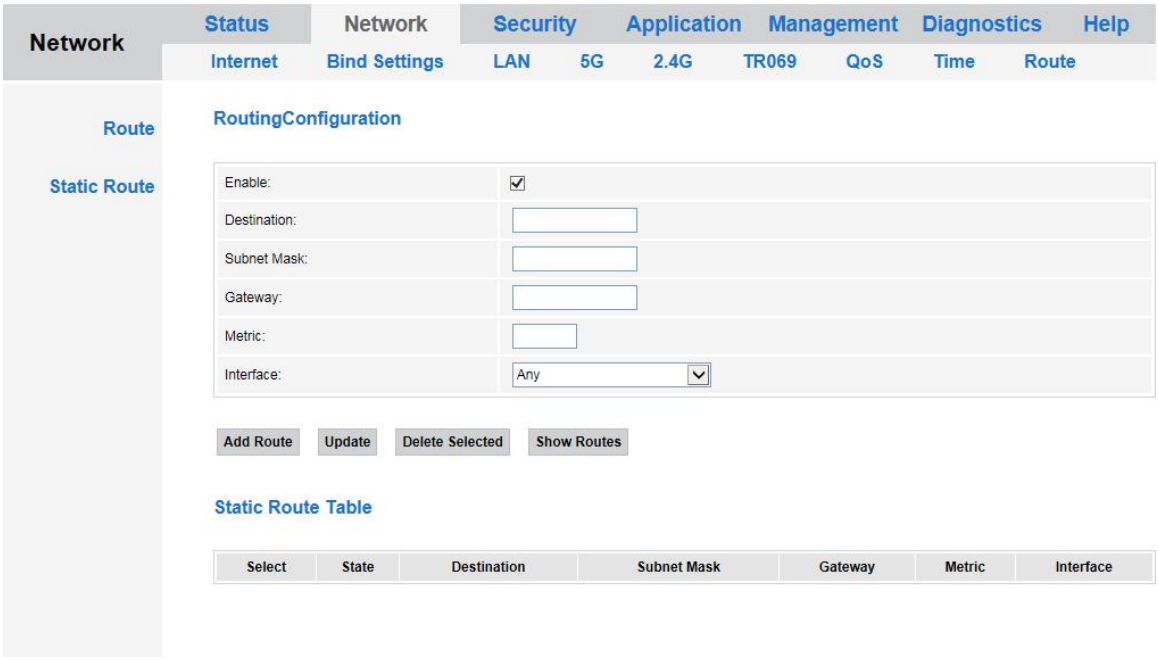


Figure 3-38: Static Route configuration

Parameter	Illustration
Enable	Switch of static route.
Destination	Destination network address. The last several bits should be zero, just like 192.168.5.0.
Subnet mask	Destination network mask.
Gateway	The gateway IP address.
Metric	Please input the metric value.
Interface	Select the wan interface you want to add static route

3.4 Security

3.4.1 WAN Access

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 3-39: URL Filter

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

3.4.2 Firewall

3.4.2.1 Security Classify

This page allows you to configure firewall level. Firewall has three levels: Low and High.

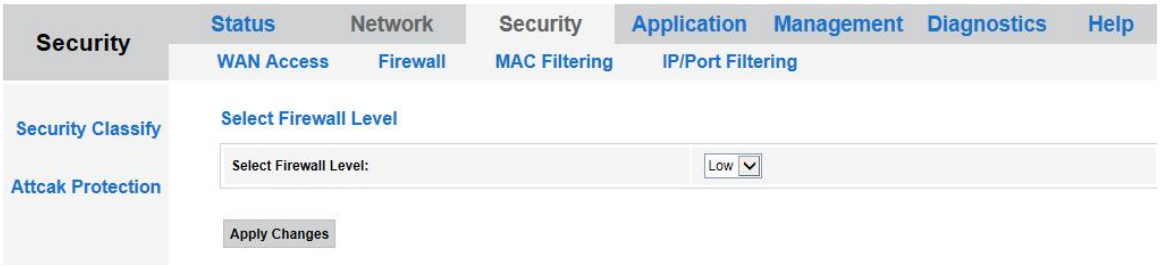


Figure 3-40: Firewall Level

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

3.4.2.2 Attack Protection

This page allows you to enable/disable attack protection function.

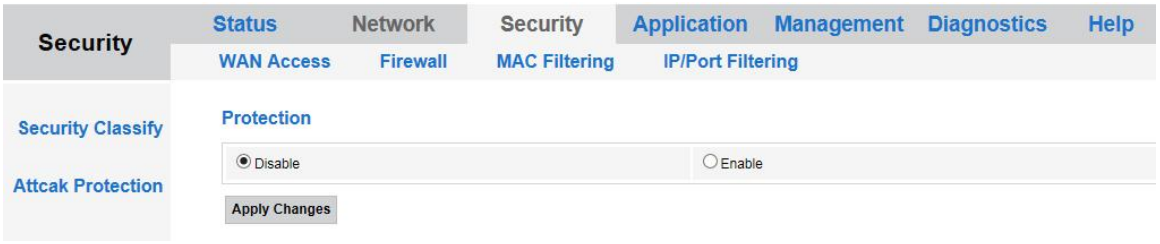


Figure 3-41: DoS Protect

3.4.3 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.

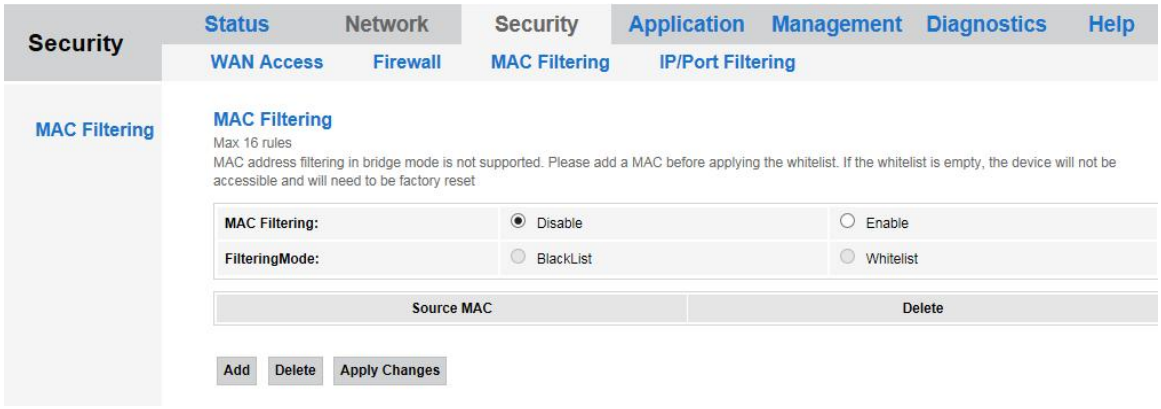


Figure 3-42: MAC Filtering

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

3.4.4 IP/Port Filtering

3.4.4.1 IP/Port Filtering

This page is used to configure port filter. Port filter includes many kinds of filters, such as

MAC filter, IP filter, protocol filter and port filter. Black list and white list take effect simultaneously. Black list is used for upstream and white list is used for downstream.

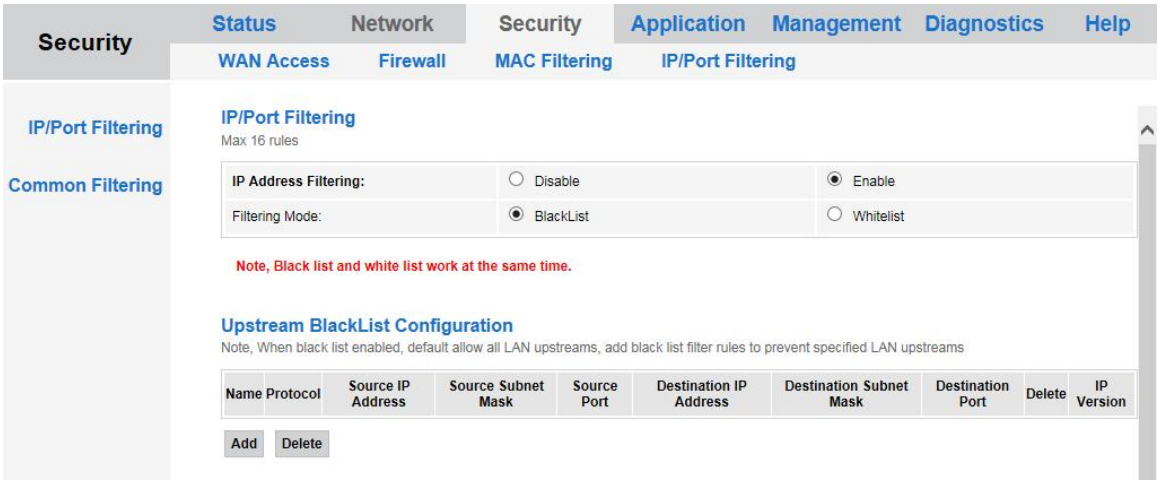


Figure 3-43: Port Filter

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

3.4.4.2 Common Filtering

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.

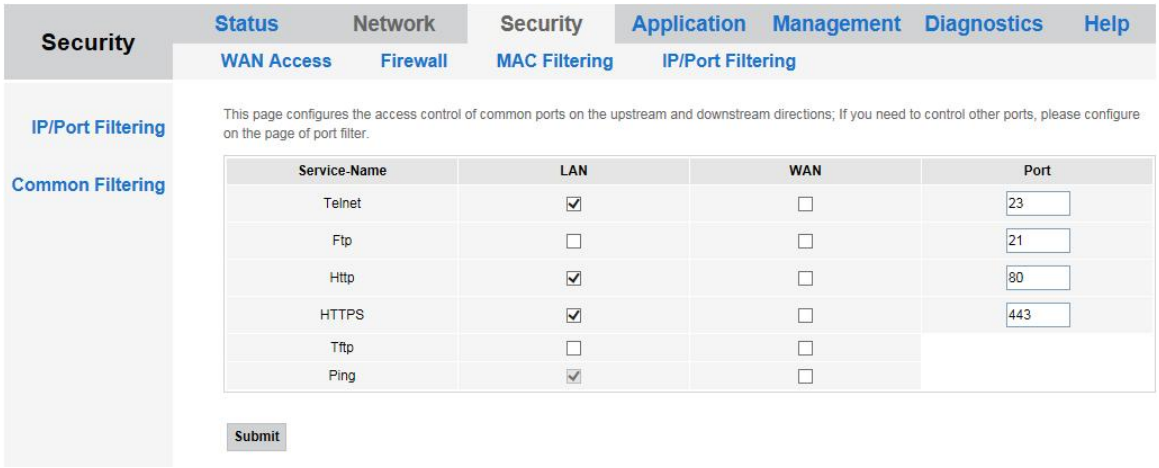


Figure 3-44: Common Port Filter

3.5 Application

3.5.1 DDNS

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

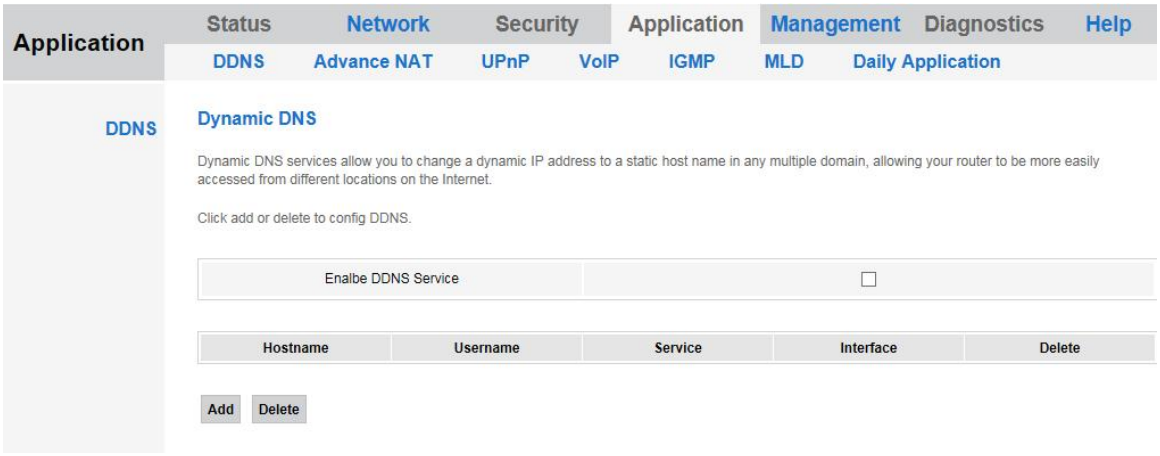


Figure 3-45: DDNS

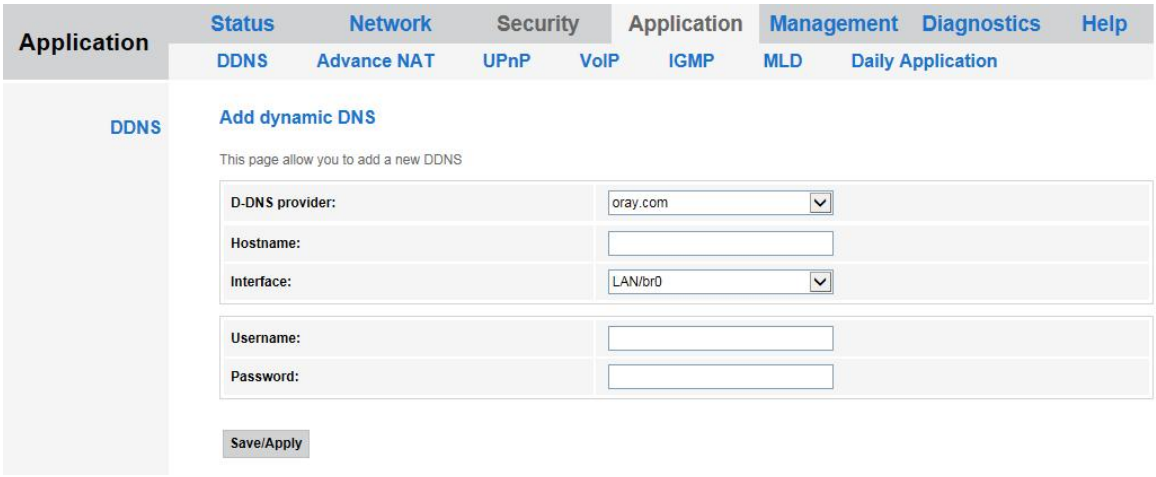


Figure 3-46: Add DDNS

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

3.5.2 Advanced NAT

3.5.2.1 ALG configuration

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

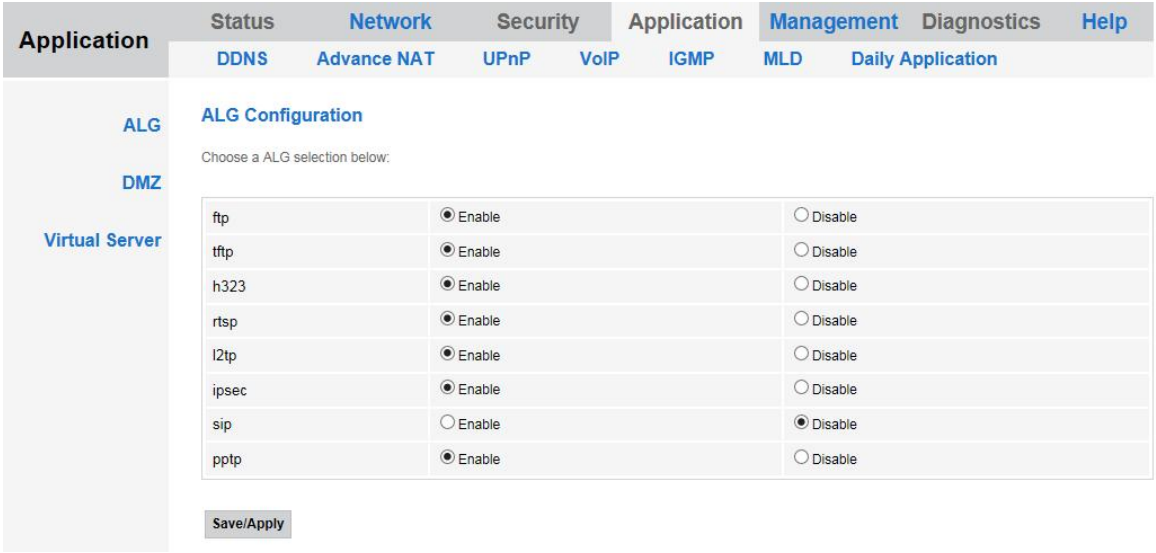


Figure 3-47: ALG configuration

3.5.2.2 DMZ configuration

This page allows you to configure DMZ server.

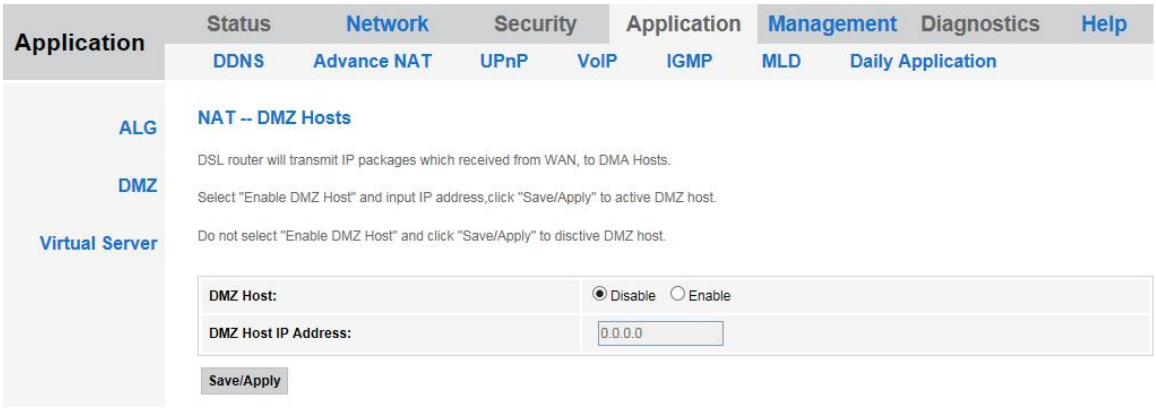


Figure 3-48: DMZ configuration

3.5.2.3 Virtual Server

This page allows you to configure virtual server. You should create a wan connection with NAT function enabled before you configure the virtual server. After you click the “Add” button, you will see the page show as in Figure 3-48.

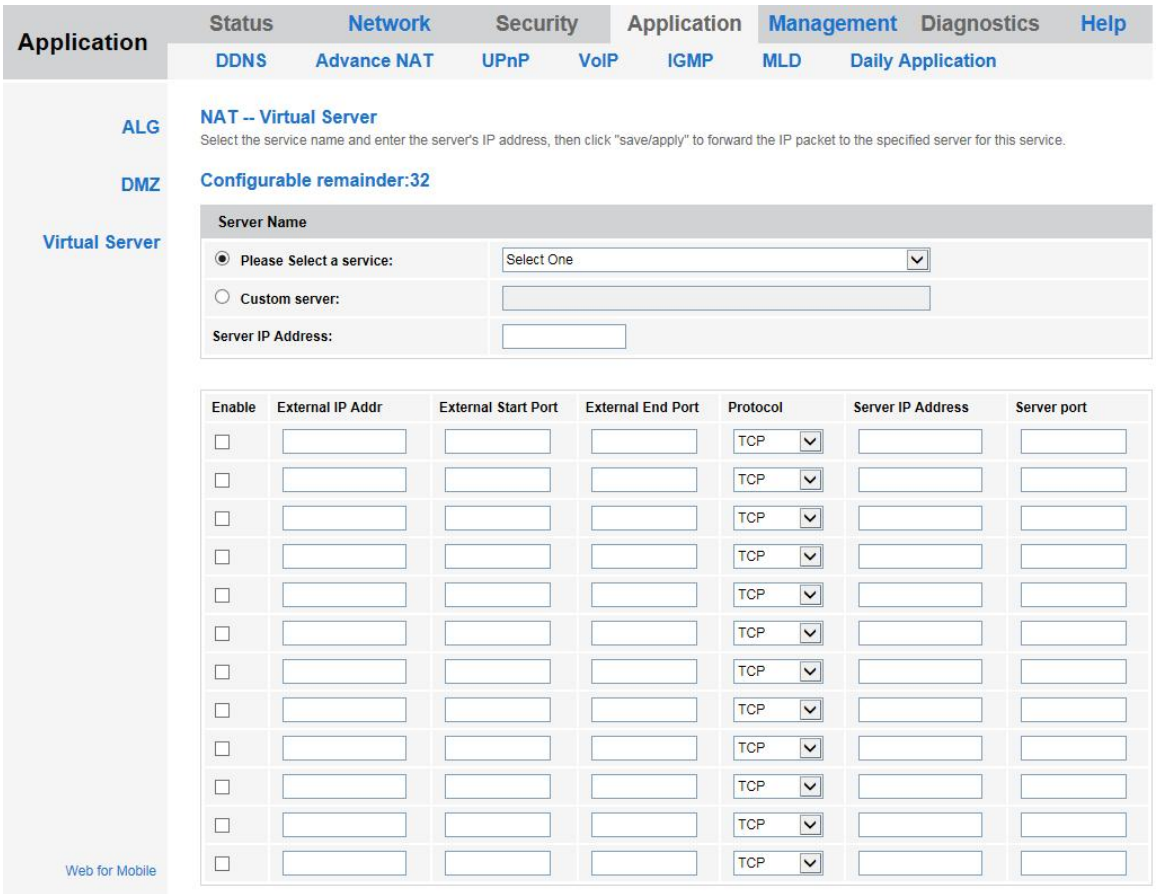


Figure 3-49: Add Virtual Server

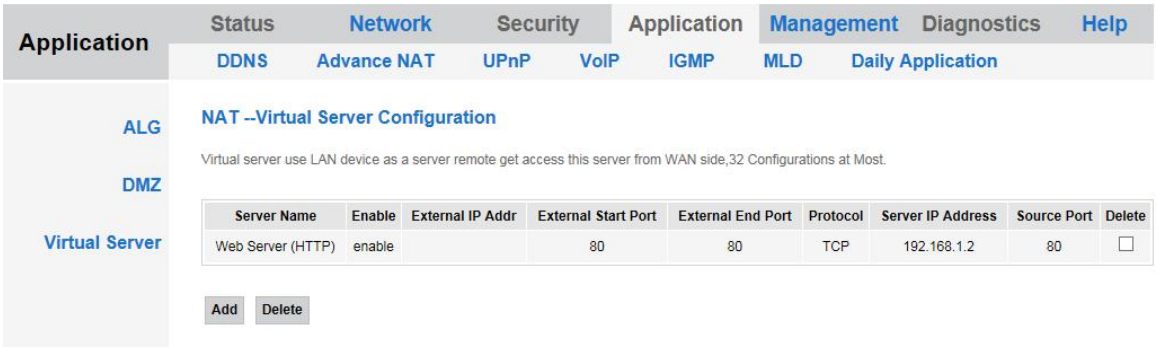


Figure 3-50: Virtual Server configuration

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

3.5.3 UPNP

This page is used to configure UPNP.

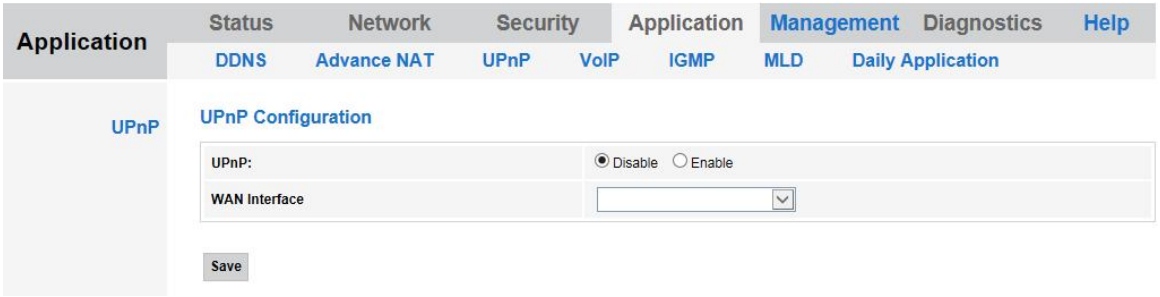


Figure 3-51: UPNP configuration

3.5.4 VoIP

3.5.4.1 Basic Settings

This page allows you to do VoIP basic configurations.

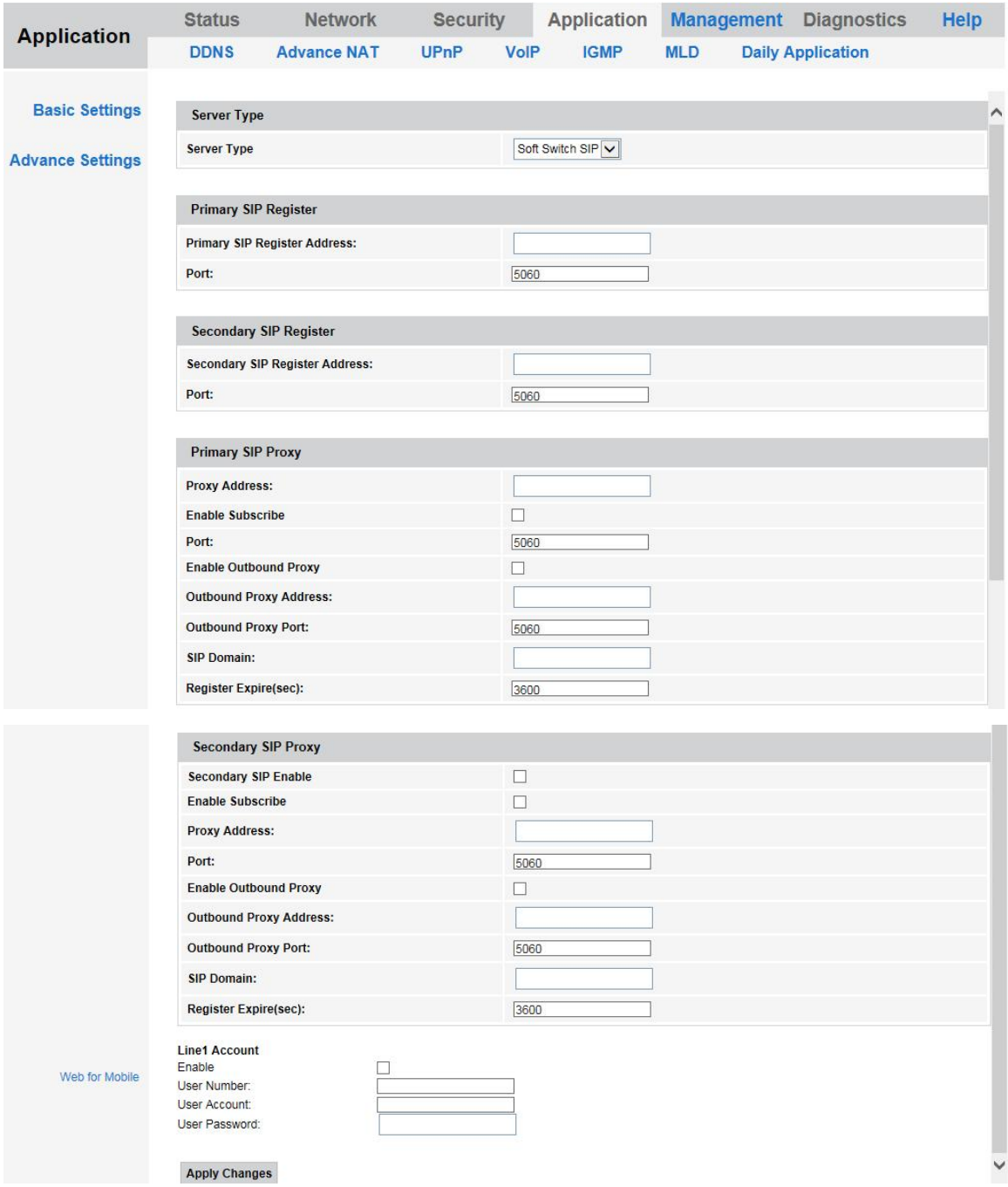


Figure 3-52: VoIP Basic Configuration

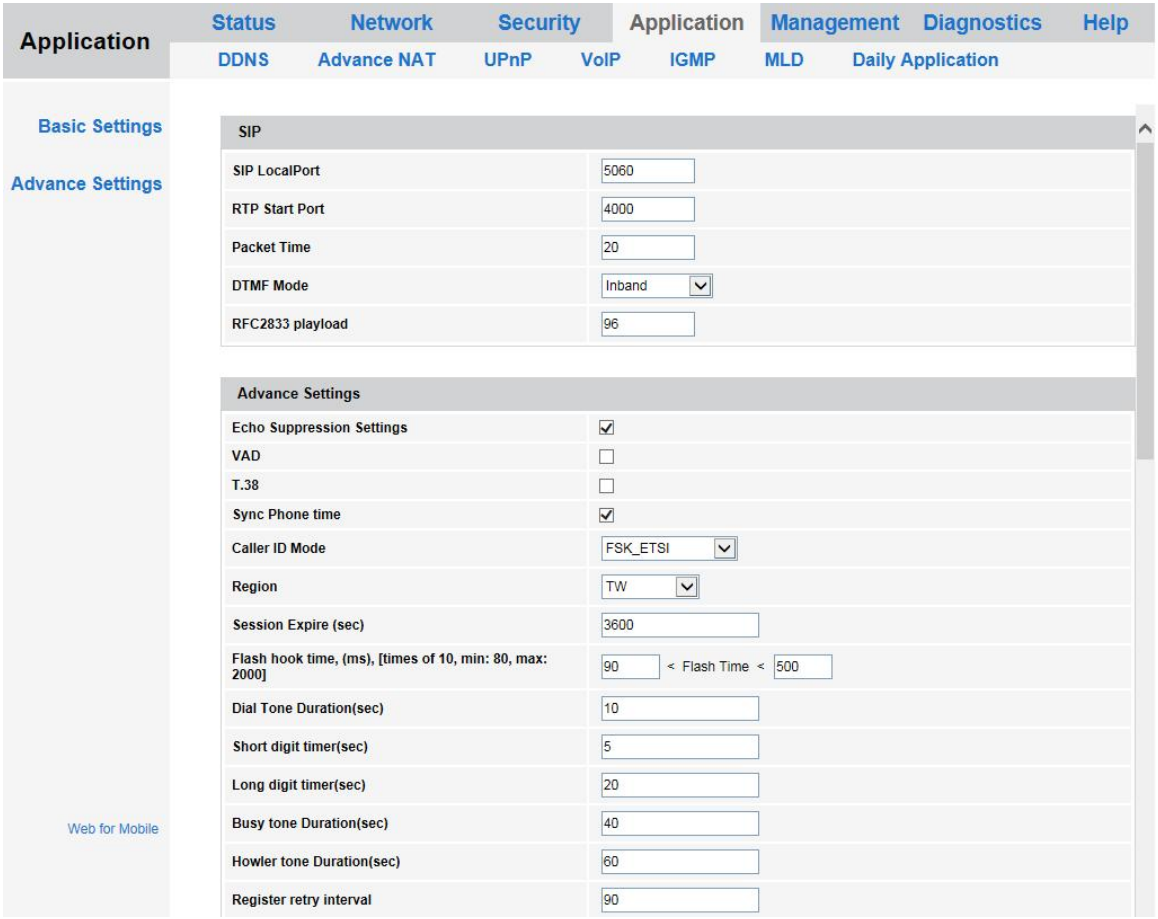
Parameter	Illustration
Server type	SIP server type, soft switch and IMS.
Primary SIP register Addr	Primary SIP register server address.
Secondary SIP Register Addr	Secondary SIP register address.
Port	The port of SIP protocol, default port is 5060.
Primary SIP Proxy	Primary SIP proxy server IP address.

Outbound Proxy Addr	Outbound proxy server IP address.
SIP domain	Enter the domain address of SIP server.
Register expire	Register expire of SIP account.
Enable Subscribe	To enable subscribe.
Line Enable	Enable: Enable VoIP function. Disable: Disable VoIP function.
Account Number	Enter phone number as it should appear on caller ID.
Account name	Enter the registration ID of the user with the registrar.
Account Password	Enter the password used for authentication with the registrar.

For VOIP WAN connection, service mode must contain VOICE.

3.5.4.2 Advance Settings

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



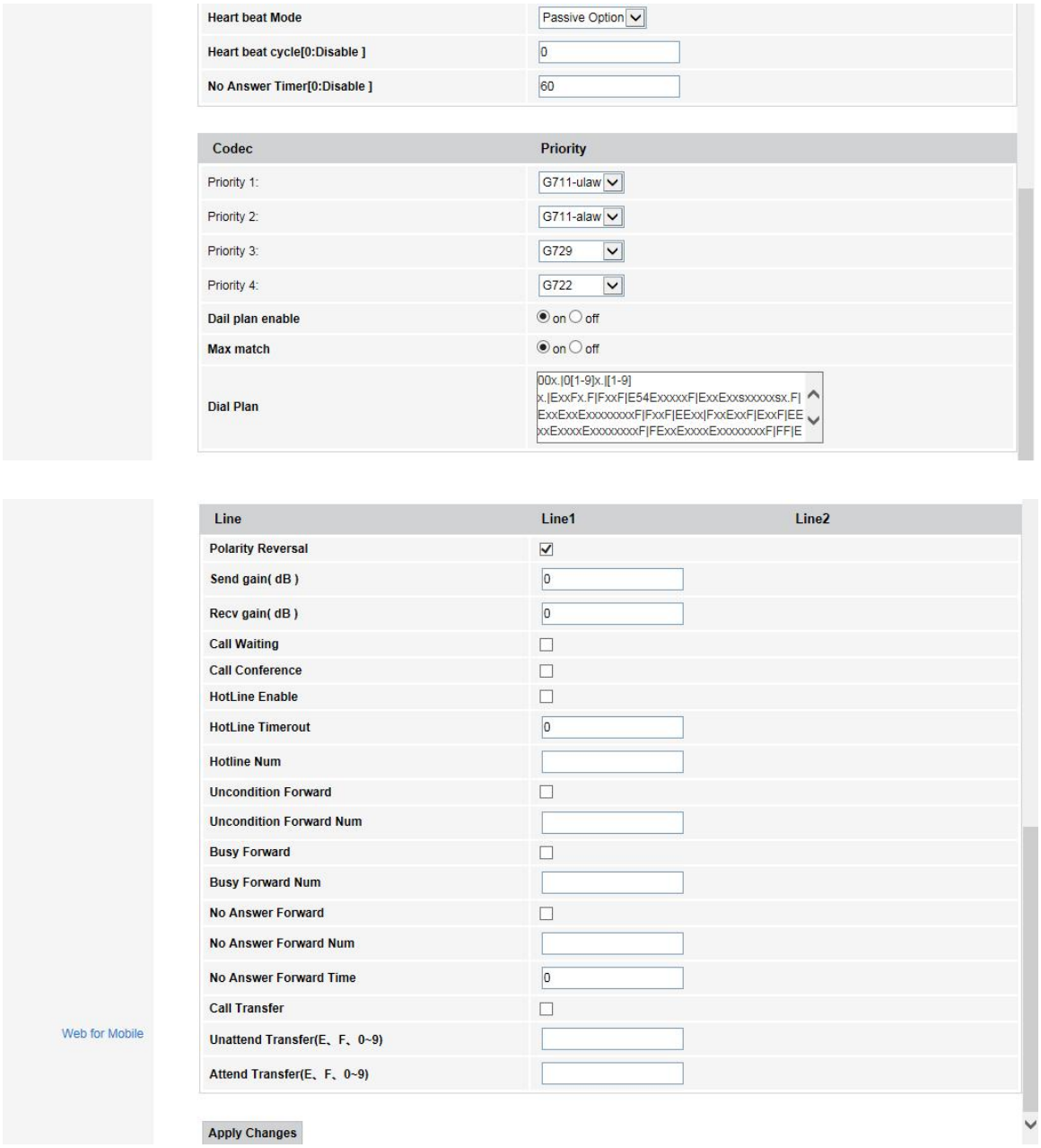


Figure 3-53: VoIP Advance Settings

Parameter	Illustration
SIP Local Port	Set local port of SIP messages.
RTP initial port	Set beginning port of RTP messages.
Packet time	Set packet time of RTP messages, in millisecond.
DTMF mode	Set DTMF mode.
RF2833 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.
T38	Enable or disable T38 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 hook time	Set flash time of phone.
Dial Tone Duration	Set the off-hook dialing expire time, default value is 10. (range: 10s~20s).
Short Digit Timer	Set the short digit timer value, default value is 5. (range: 4s~30s).
Long Digit Timer	Set the long digit timer value, default value is 5. (range: 4s~30s).
Busy tone Duration	Set the busy tone time, default value is 40. (range: 30s~180s).
Howler tone Duration	Set the howler tone time, default value is 60. (range: 30s~180s).
Register retry interval	Set register failed and retry interval.
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 mode, but one of those modes must be chosen as the priority.
Dial Plan enable	Set dial rule of device.
Polarity Reversal	Enable or disable polarity reversal function.
Send gain	Set codec send gain.
Recv gain	Ser codec receive gain.
Call waiting	Enable or disable call waiting.
Call conference	Enable or disable call conference.
Hotline	Set hotline function.
Un-condition forward	Enable or disable un-condition forward.
Un-condition forward Num	Set un-condition forward number.
Busy forward	Enable or disable 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 functional code of unattend call transfer.

Attend Transfer	Set functional code of attend call transfer.

3.5.5 IGMP

3.5.5.1 IGMP Snooping

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

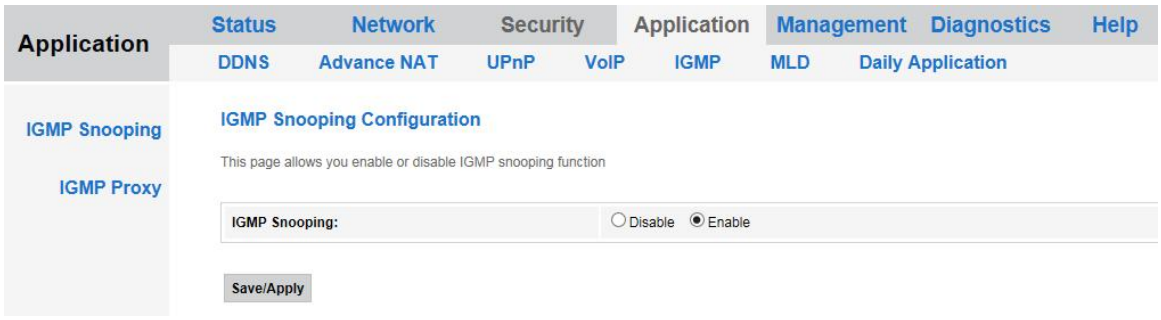


Figure 3-54: IGMP Snooping

3.5.5.2 IGMP Proxy

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



Figure 3-55: IGMP Proxy

3.5.6 MLD

3.5.6.1 MLD Snooping

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

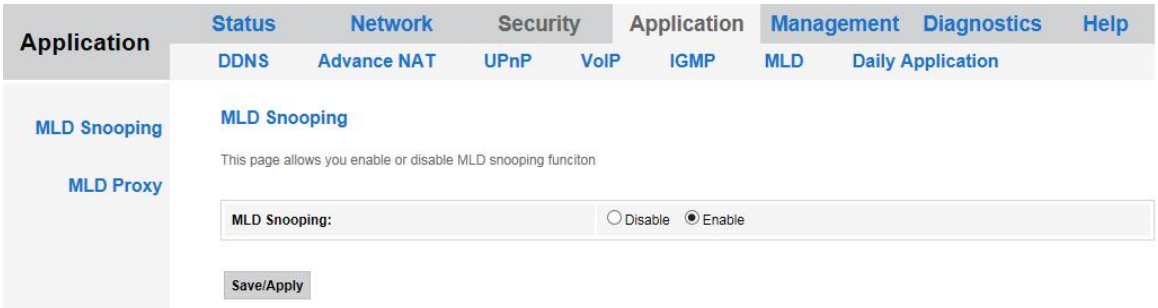


Figure 3-56: MLD Snooping

3.5.6.2 MLD Proxy

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



Figure 3-57: MLD Proxy

3.5.7 Daily Application

This page allows you to configure multicast VLAN for route mode WAN connections.

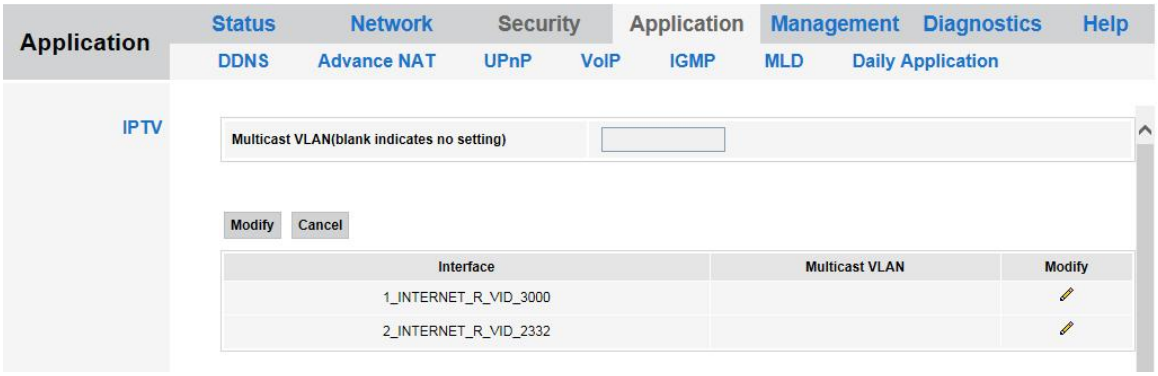


Figure 3-58: Multicast VLAN

3.6 Management

3.6.1 User Management

This page allows you to change login password of current user. There are two User level accounts: admin and user.

The admin account is able to access and modify all settings of HGU.

The user account can only be used to view configurations, status and configure few parameters such as LAN IP address and DHCP server, wireless parameters, configure filter, firewall, reboot HGU and so on.

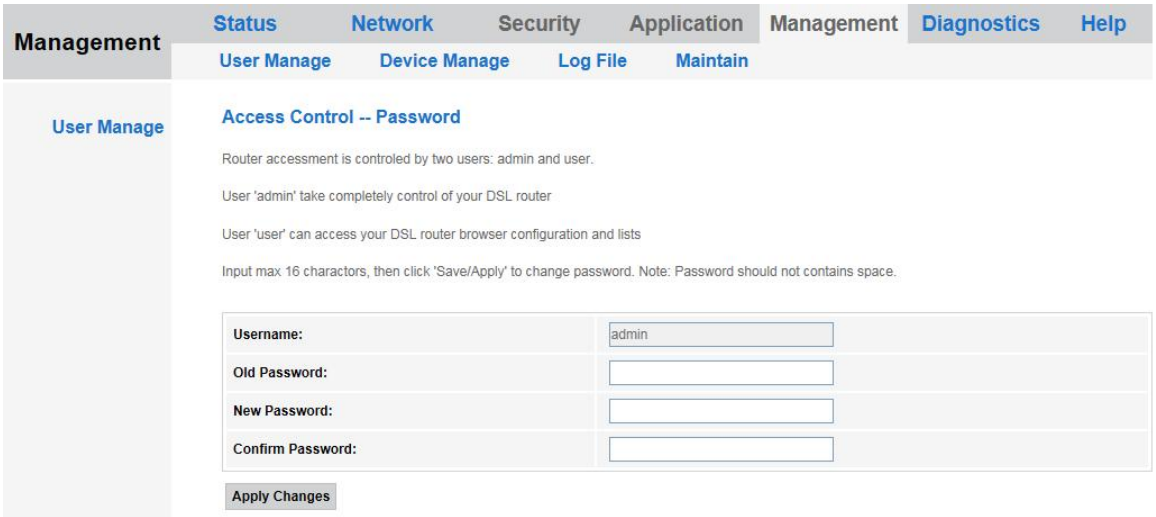


Figure 3-59: User management

3.6.2 Device Management

3.6.2.1 Device Reboot

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

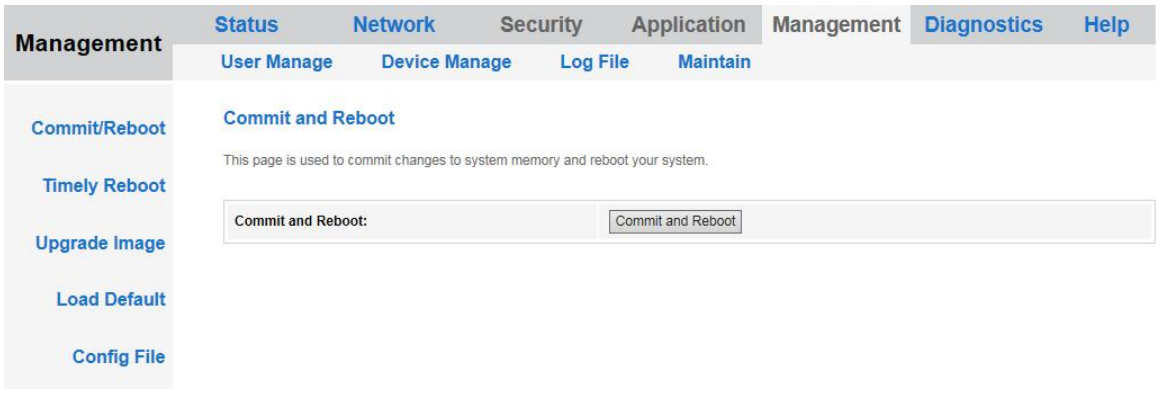


Figure 3-60: Device reboot

3.6.2.2 Timely Reboot

This page is used to set device reboot time. Only when you have been synchronized the network time can you take effect the timely reboot.

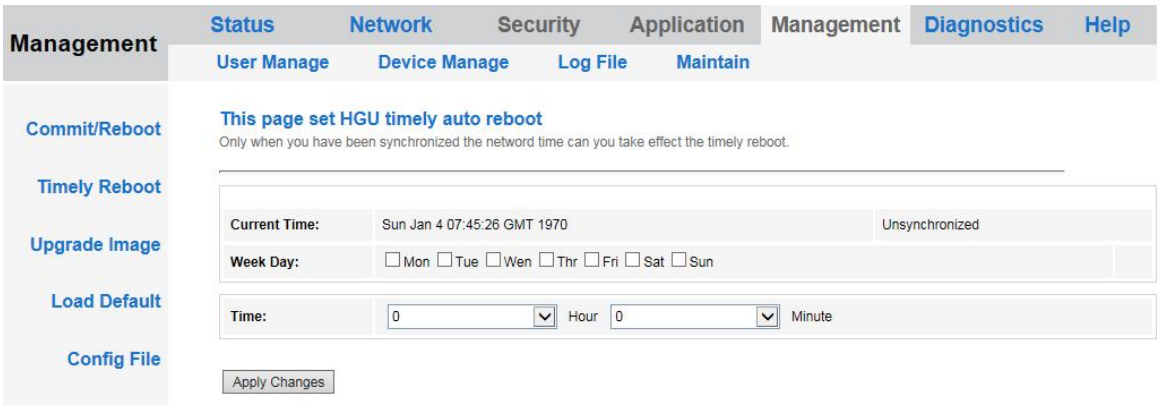


Figure 3-61: Device timely reboot

3.6.2.3 Upgrade

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.

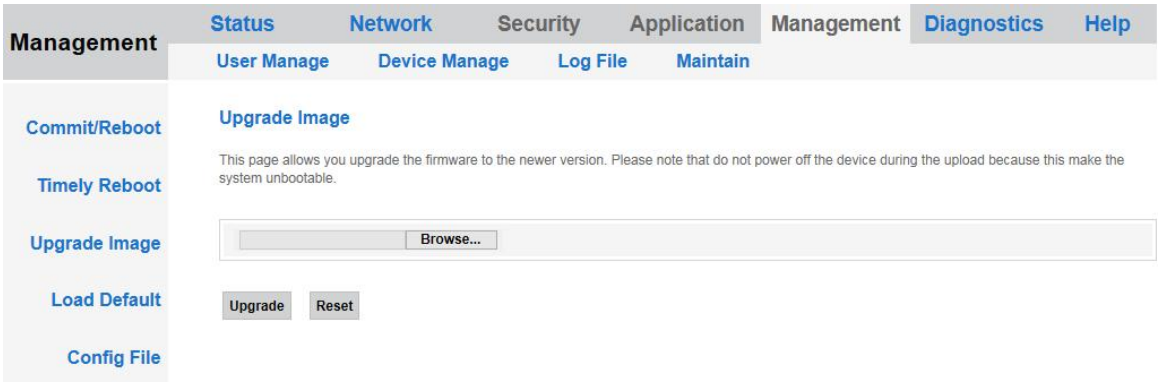


Figure 3-62: Device upgrade

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 default" button to restore settings of the device. "Restore Default" button restore the LAN parameter, "Restore Factory Default" button restore all the ONU configurations. After restored, it will restart automatically.

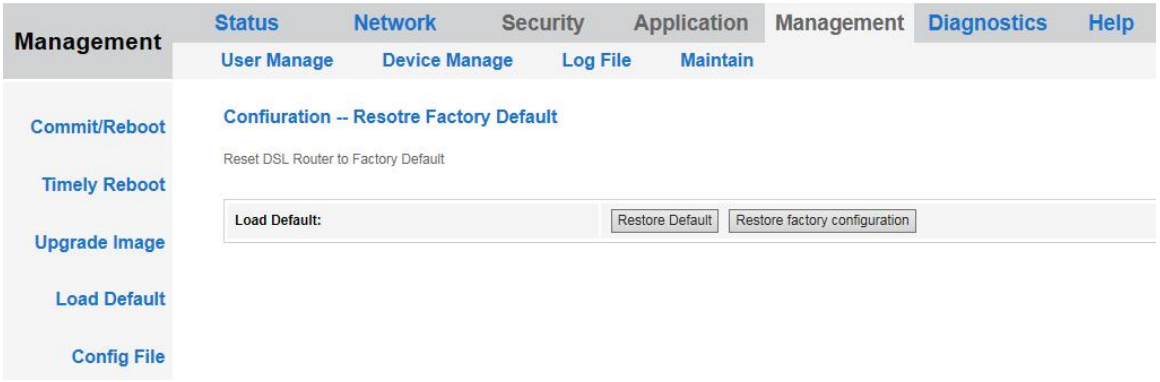


Figure 3-63: Load default

3.6.2.5 Config file Management

This page allows you to backup and restore the configurations of HGU.

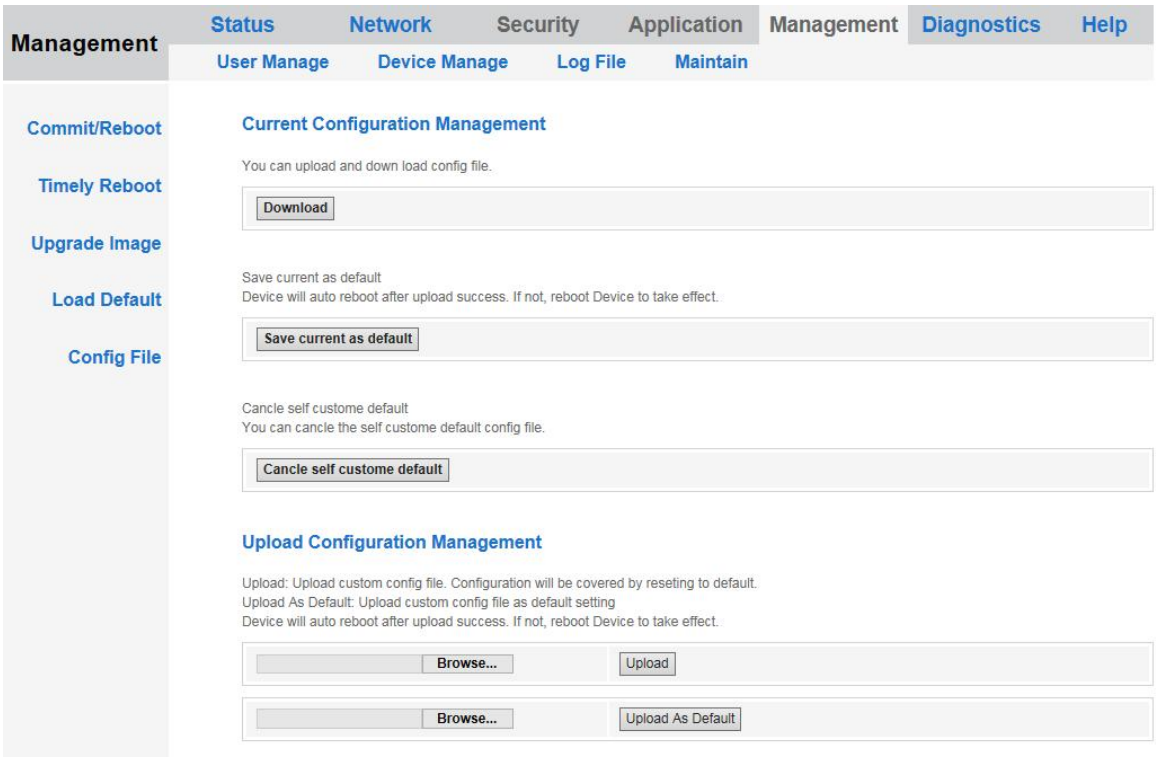


Figure 3-64: Config file management

3.6.3 Log File

3.6.3.1 System Log

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

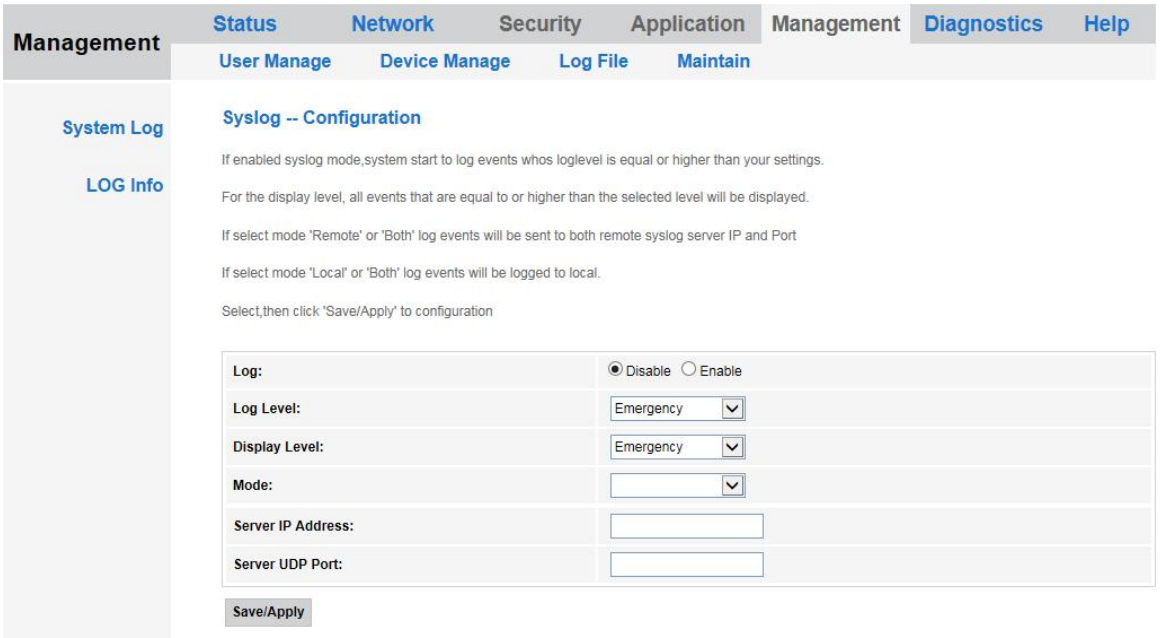


Figure 3-65: Log settings

Parameters	Illustration

Log Level	Log record level, include Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debugging.
Display Level	Log display level, include Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debugging.
Mode	Local: Log will be saved locally. Remote: Log will be sent to remote specific host. Both: Log will be saved locally and be sent to remote specific host meanwhile.

3.6.3.2 View system log

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

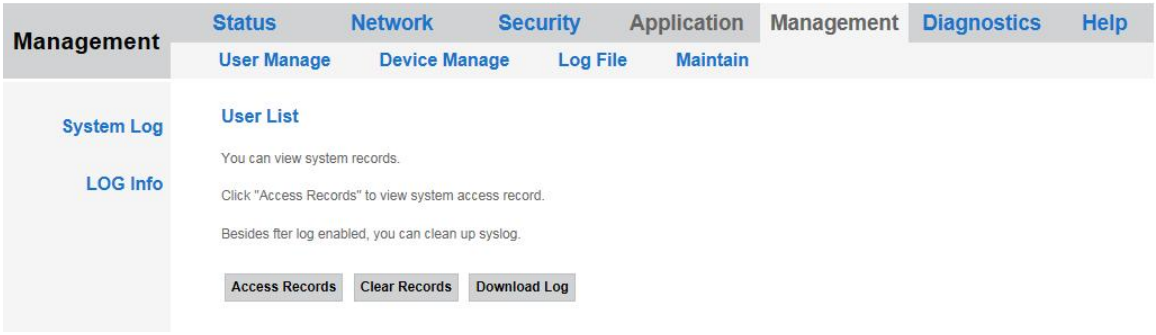


Figure 3-66: Log Info

3.6.4 Maintain

This page shows about the maintenance. Click "End maintain" button, the new data will be reported to server automatically.

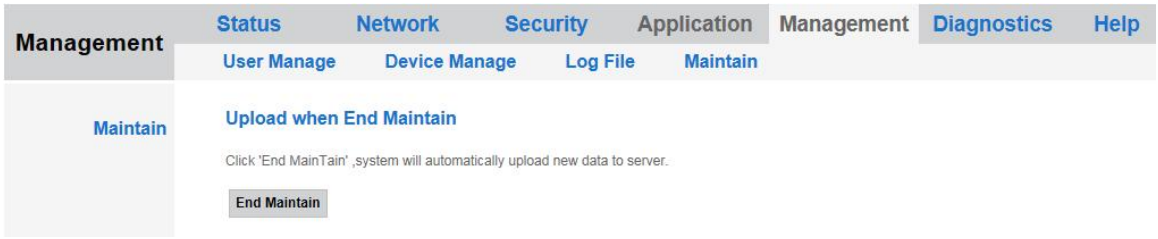


Figure 3-67: Maintain

3.7 Diagnose

3.7.1 Network diagnostics

3.7.1.1 PING Test

This page is used for ping test. You can diagnose connection status between HGU and other devices.

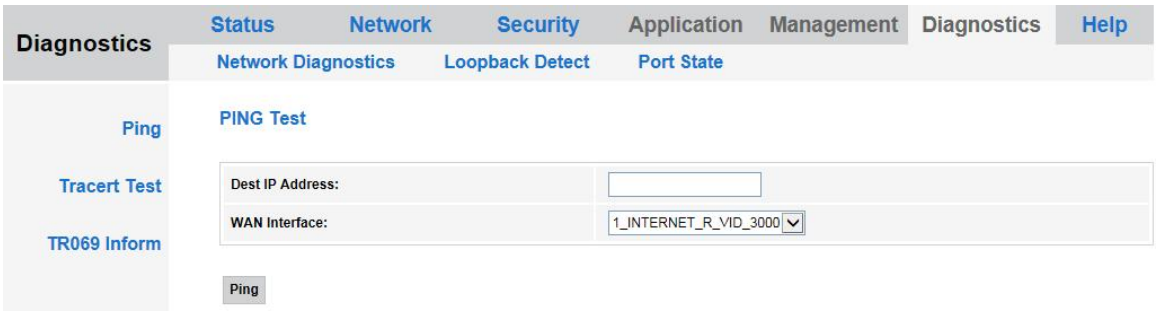


Figure 3-67: PING test

Parameters	Illustration
Interface	Select the interface that needs to diagnose.
Destination IP or host name	Input the destination IP you want to ping.

3.7.1.2 Tracert Diagnose

This page is used for tracert test.

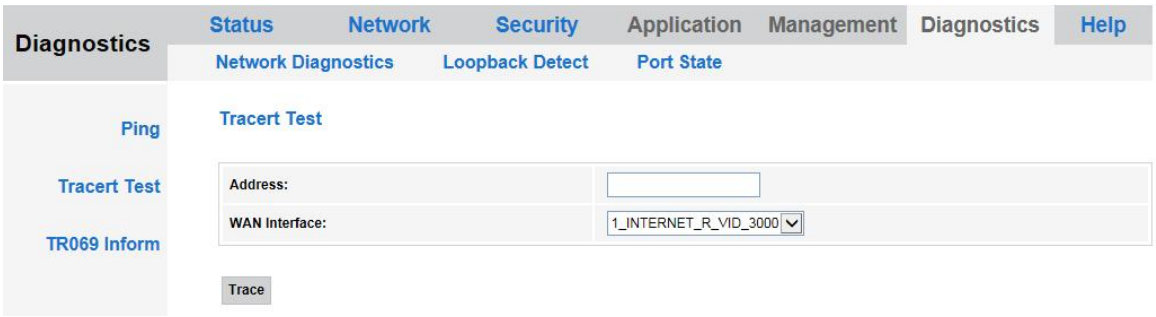


Figure 3-68: Tracert test

Notice:

Do not do trace route test again when the trace route in running status.

3.7.1.3 TR069 Inform

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

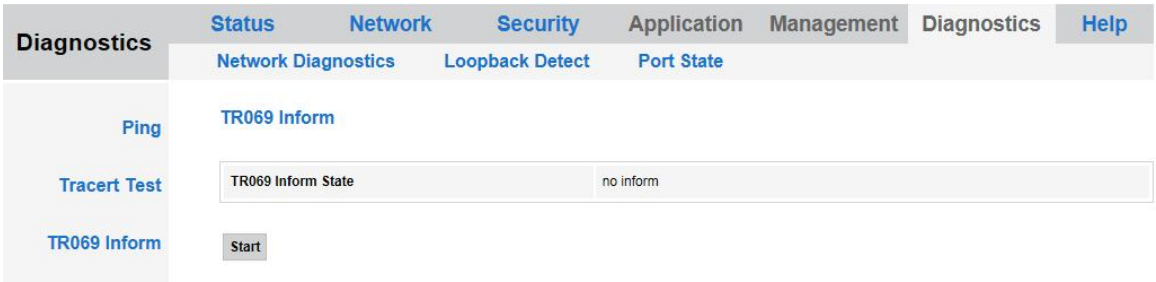


Figure 3-69: TR069 Inform

3.7.2 Loopback detect

This page is used to configure loopback detect function.

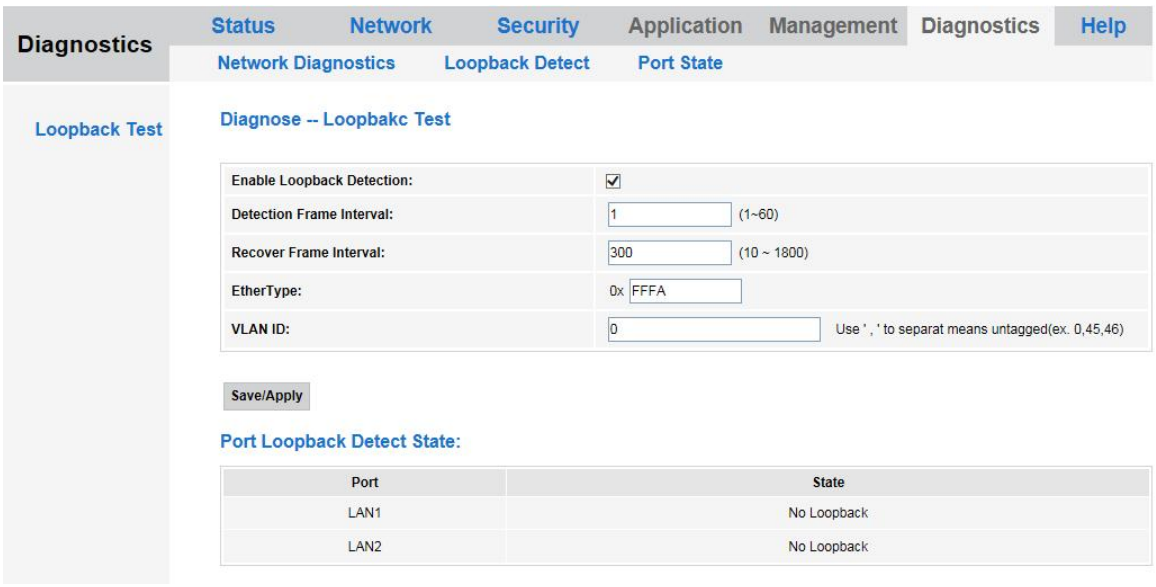


Figure 3-70: Loopback detect settings

3.7.3 Port state

This page shows link status of LAN ports.

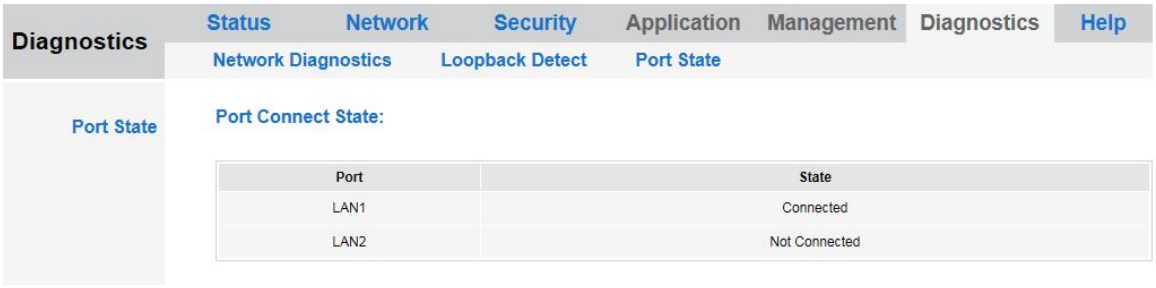


Figure 3-71: Port state

3.8 Help

The Help information of HGU displays instruction and prompt of each web UI.

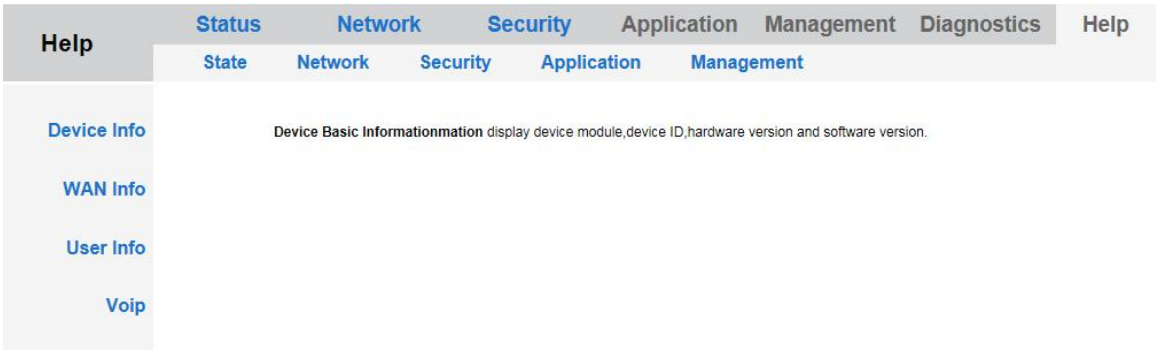


Figure 3-72: Help information

Chapter 4 Examples

4.1 Internet service

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

4.1.1 Requirement

1) 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 > Internet > Internet” in navigation menu. Add a bridge mode WAN connection as the following parameters.

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

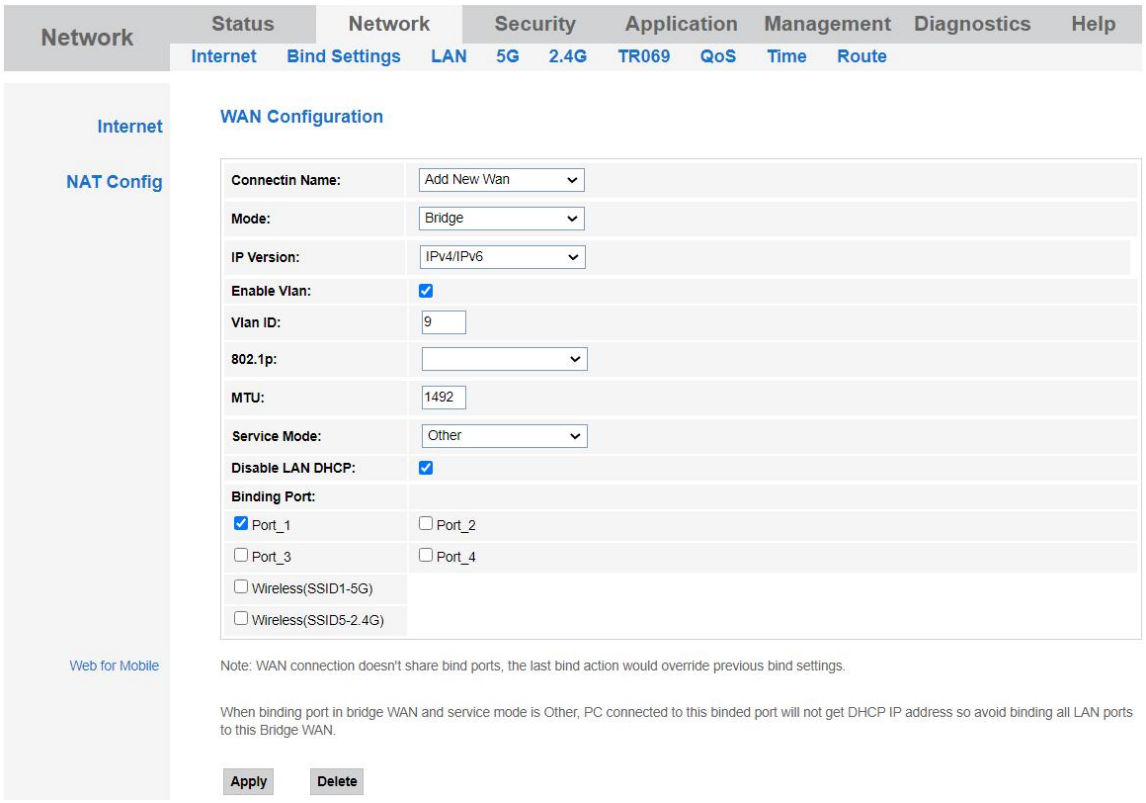


Figure 4-1: Add a bridge WAN connection

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

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

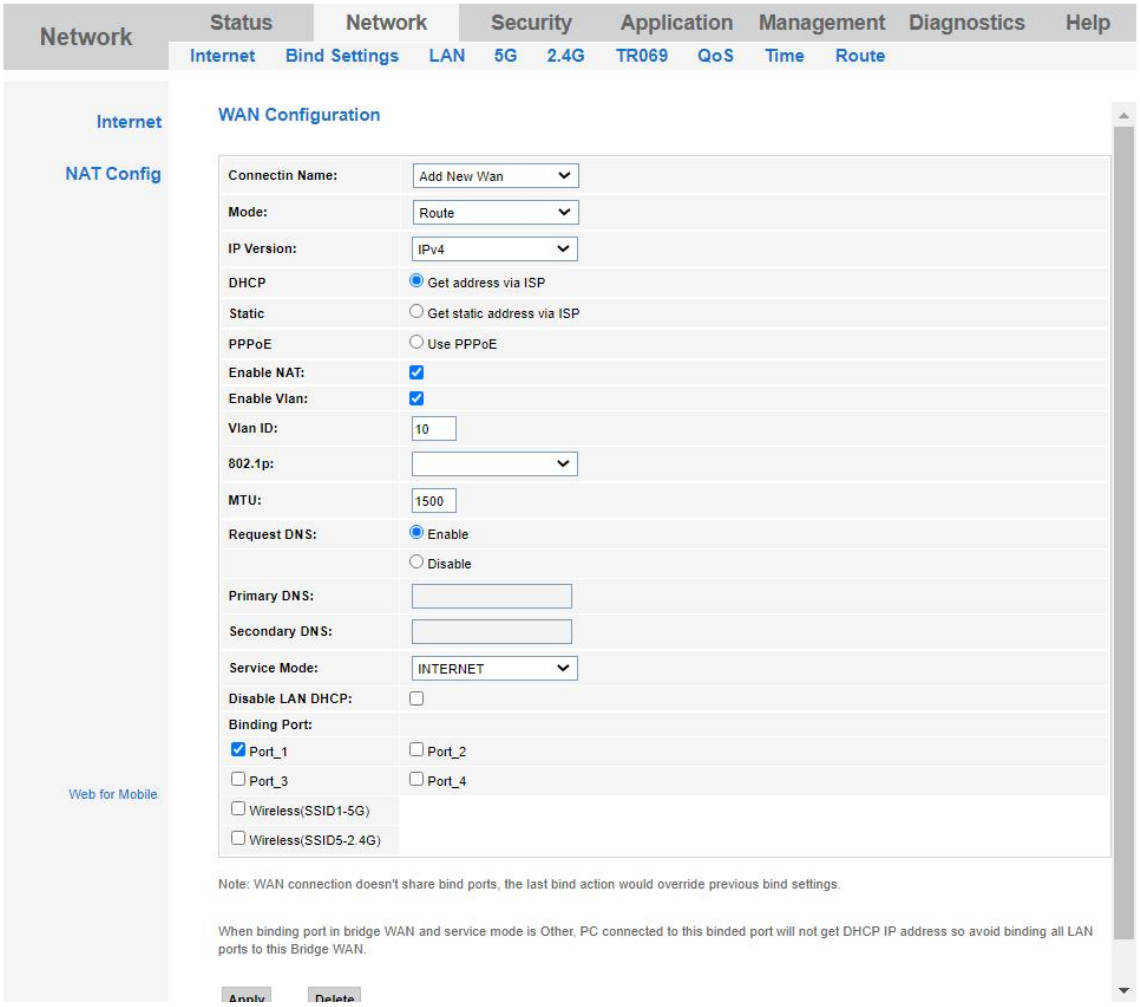


Figure 4-2: Add a route WAN connection

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 > Internet > Internet” in navigation menu. Add a bridge mode WAN connection as the following parameters.

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

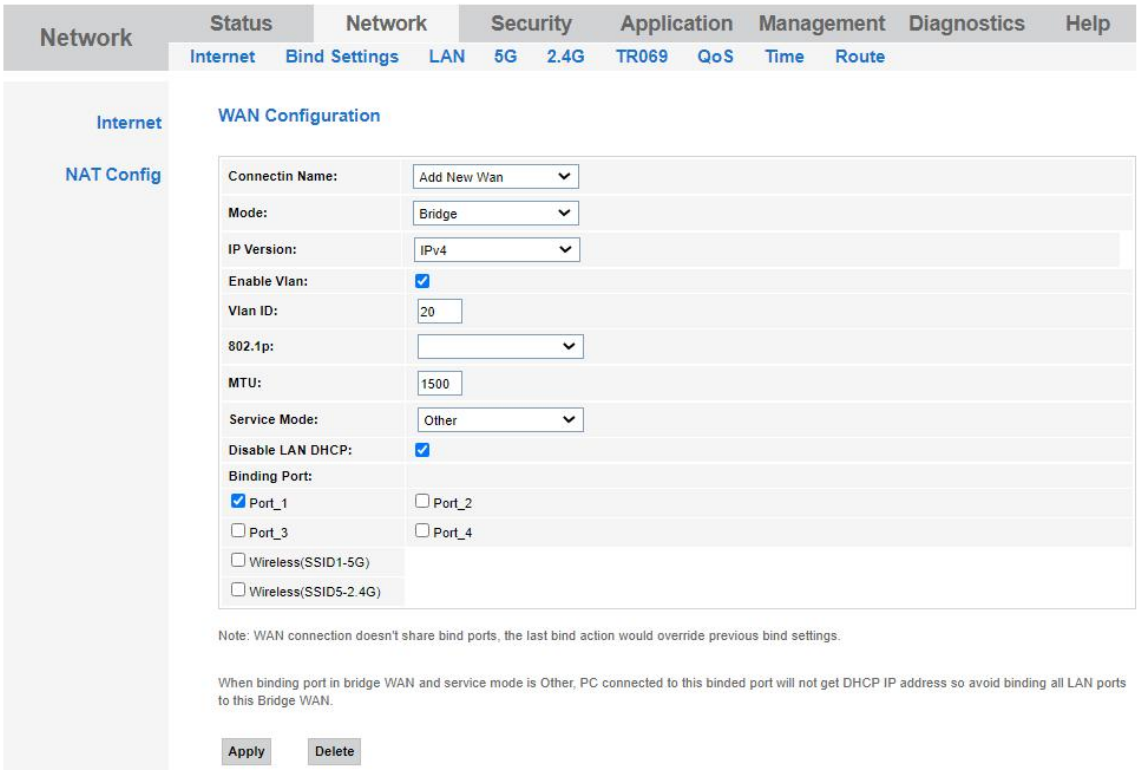


Figure 4-3: Add a bridge WAN connection

2) Enable IGMP snooping

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

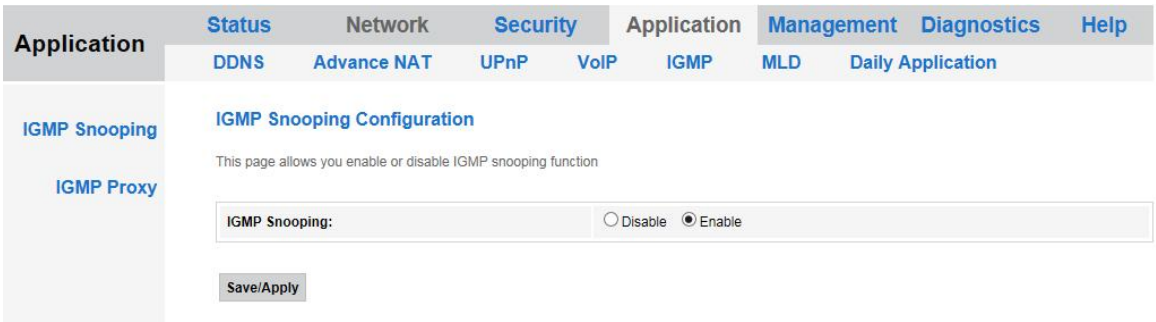


Figure 4-4: Enable IGMP snooping

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 > Internet > Internet" 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.

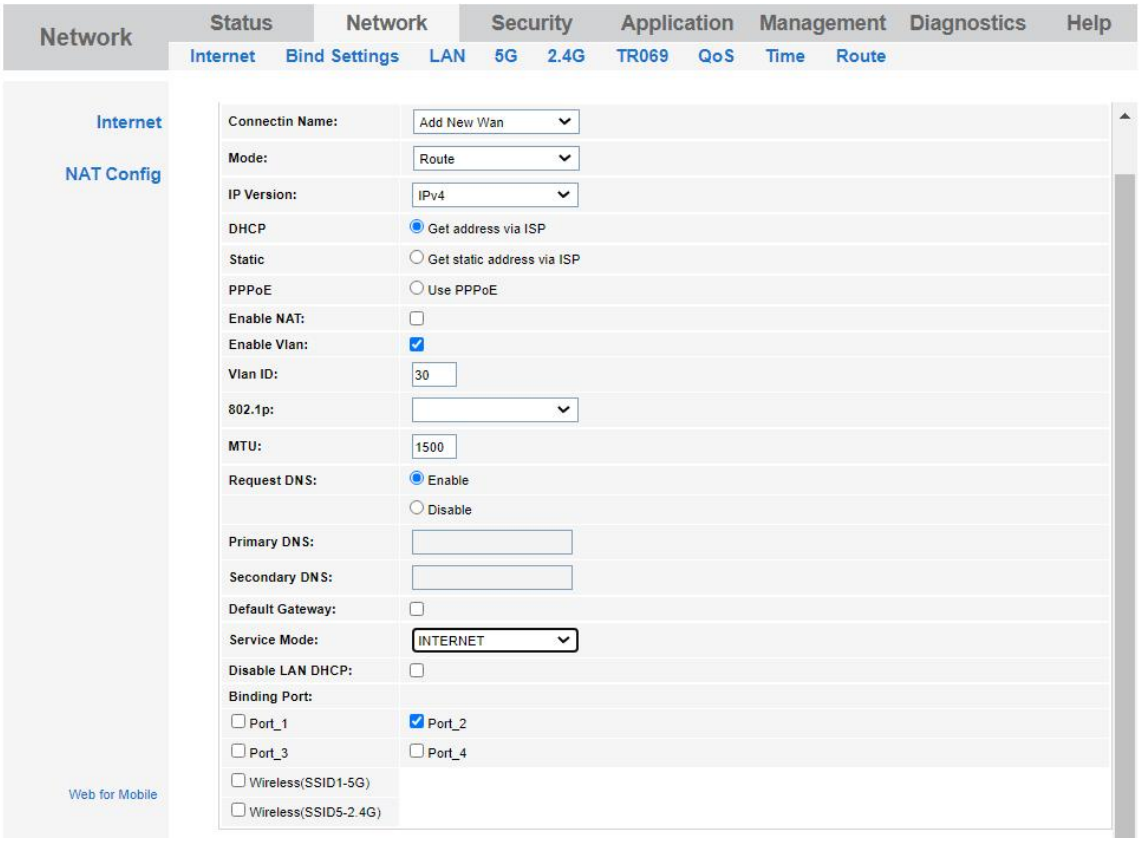


Figure 4-5: Add a route WAN connection

2) Enable IGMP proxy

Choose "Application > IGMP > IGMP PROXY" in navigation menu. Choose the relevant

WAN connection and enable IGMP proxy.



Figure 4-6: 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 > Internet > Internet” 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.
- ✧ DNS is 192.168.1.1.
- ✧ Service mode is VOIP.

✧ Other parameters keep default.

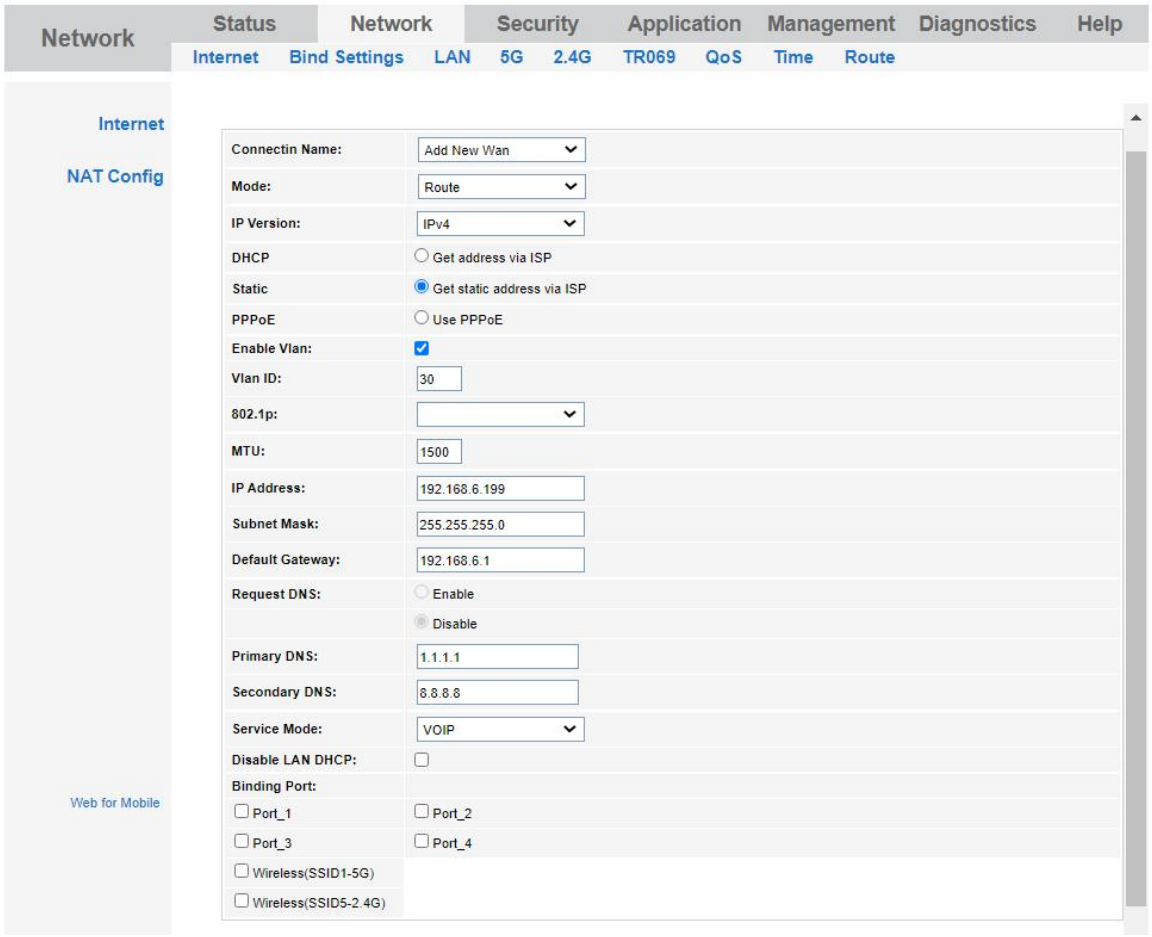


Figure 4-7: Add a route WAN connection

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.

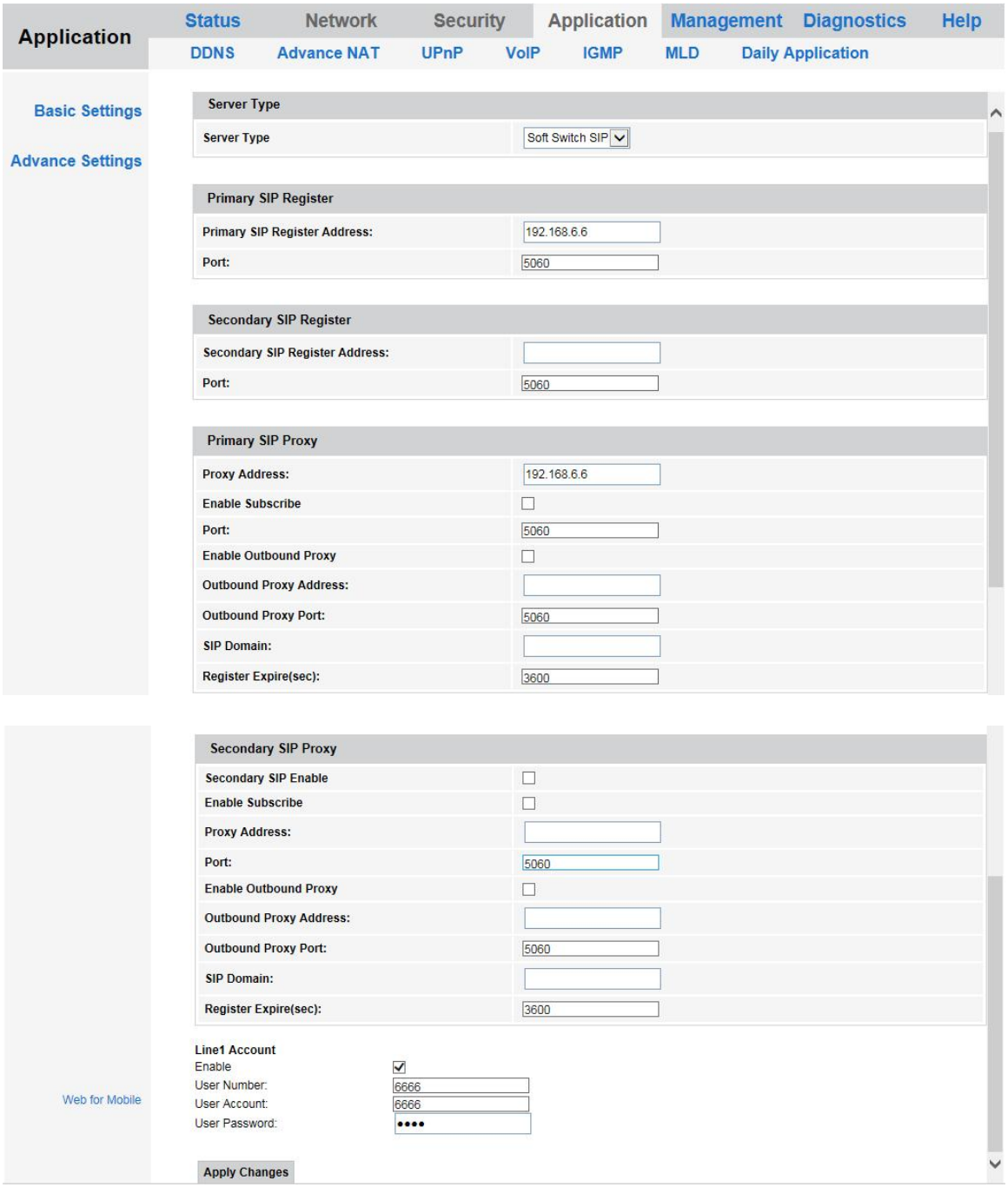


Figure 4-8: VoIP Basic settings

3) Look up register status

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

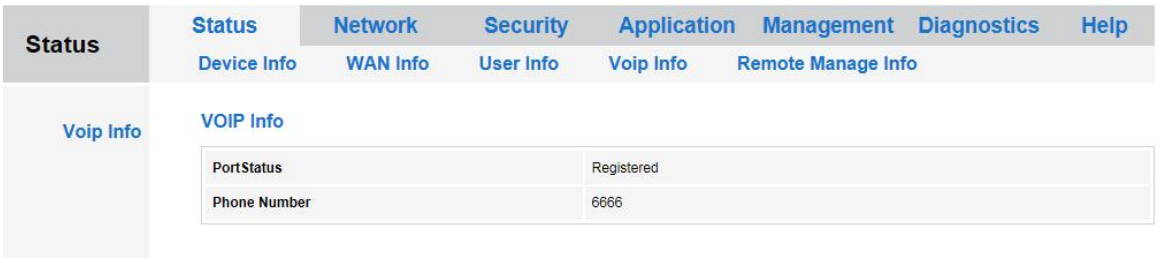


Figure 4-9: VoIP registering status

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 > Internet > internet” in navigation menu. Add a route mode WAN connection as the following parameters.

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

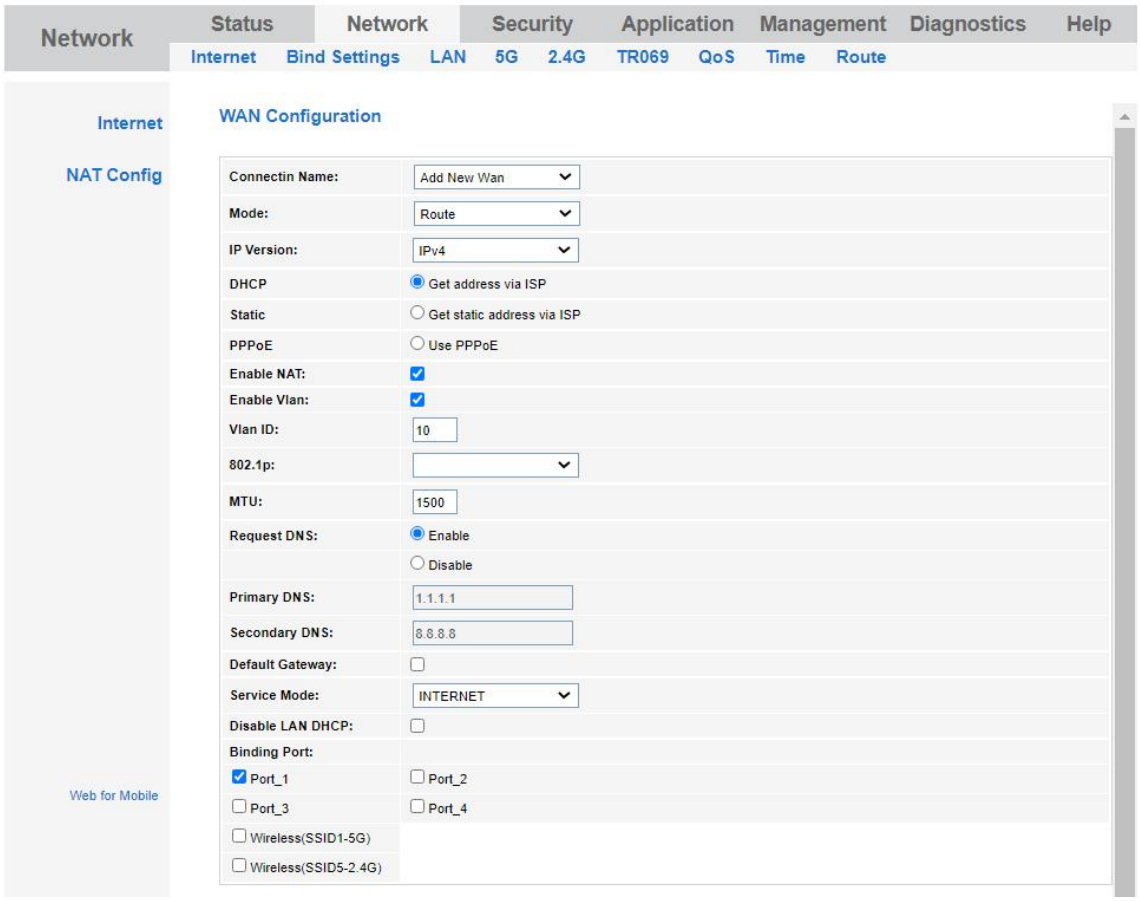


Figure 4-10: Add a route mode WAN

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

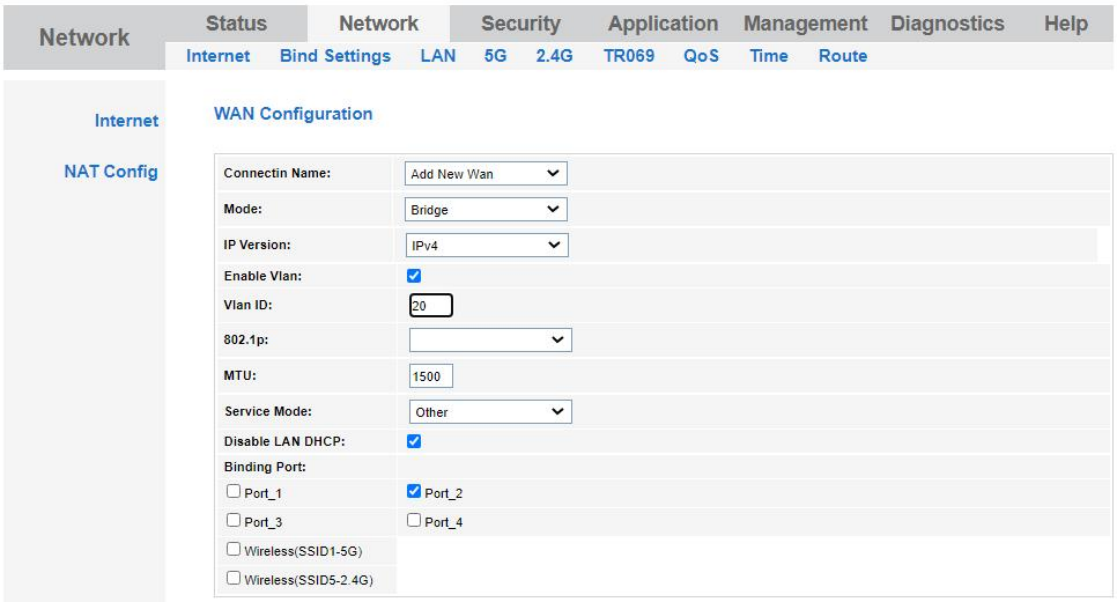


Figure 4-11: Add a bridge mode WAN

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 > Internet > internet" 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.

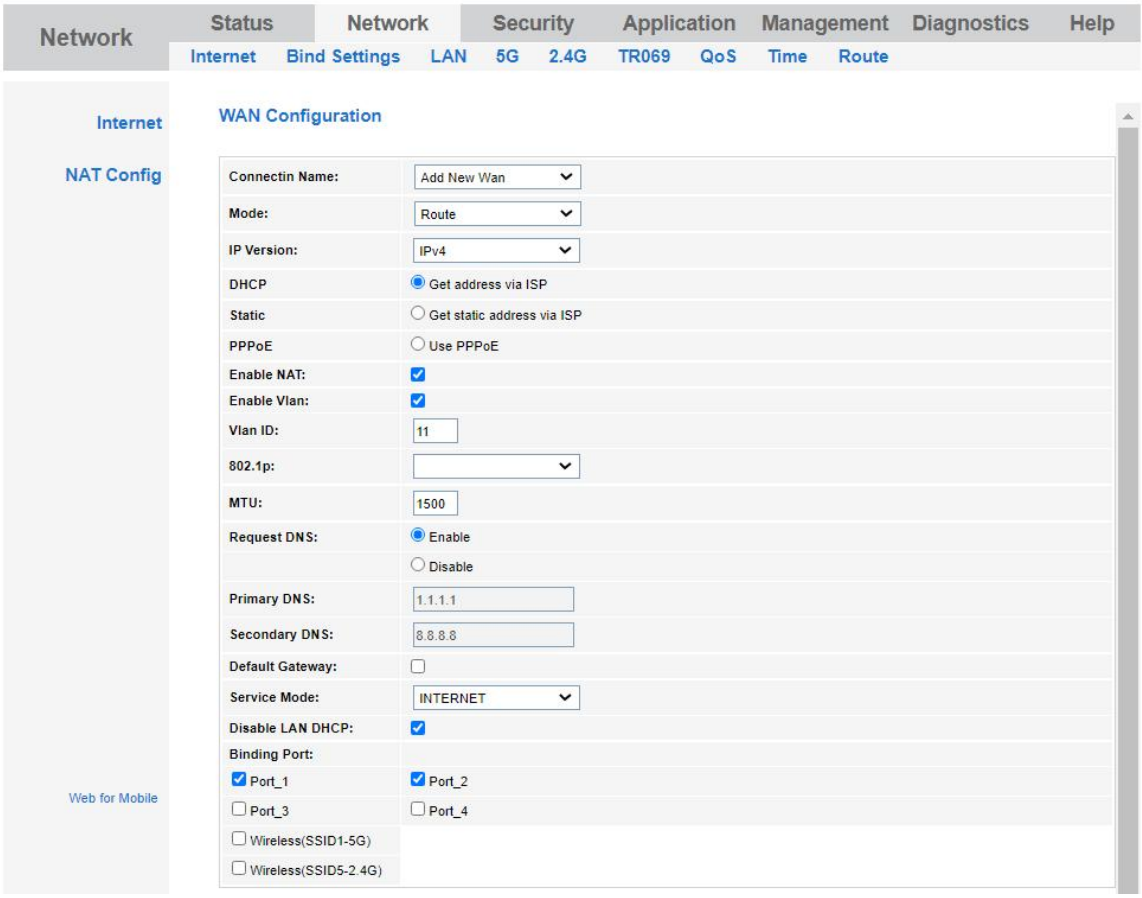


Figure 4-12: Add a route mode WAN connection

2) Enable IGMP proxy

Choose "Application > IGMP > IGMP PROXY" in navigation menu. Choose the relevant WAN connection and enable IGMP proxy.



Figure 4-13: Enable IGMP proxy

6）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.

7）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 192.168.6.199, and SIP server is 192.168.6.6. The proxy server is 192.168.6.6 too;

Username and password of SIP account: 6666, 6666.

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

- ✧ Protocol mode is IPv4.
- ✧ Choose PPPoE.
- ✧ NAT function is checked.
- ✧ Enable VLAN and VLAN ID is 10.
- ✧ Service mode is INTERNET.

- ✧ Bind port 1.
- ✧ Other parameters keep default.

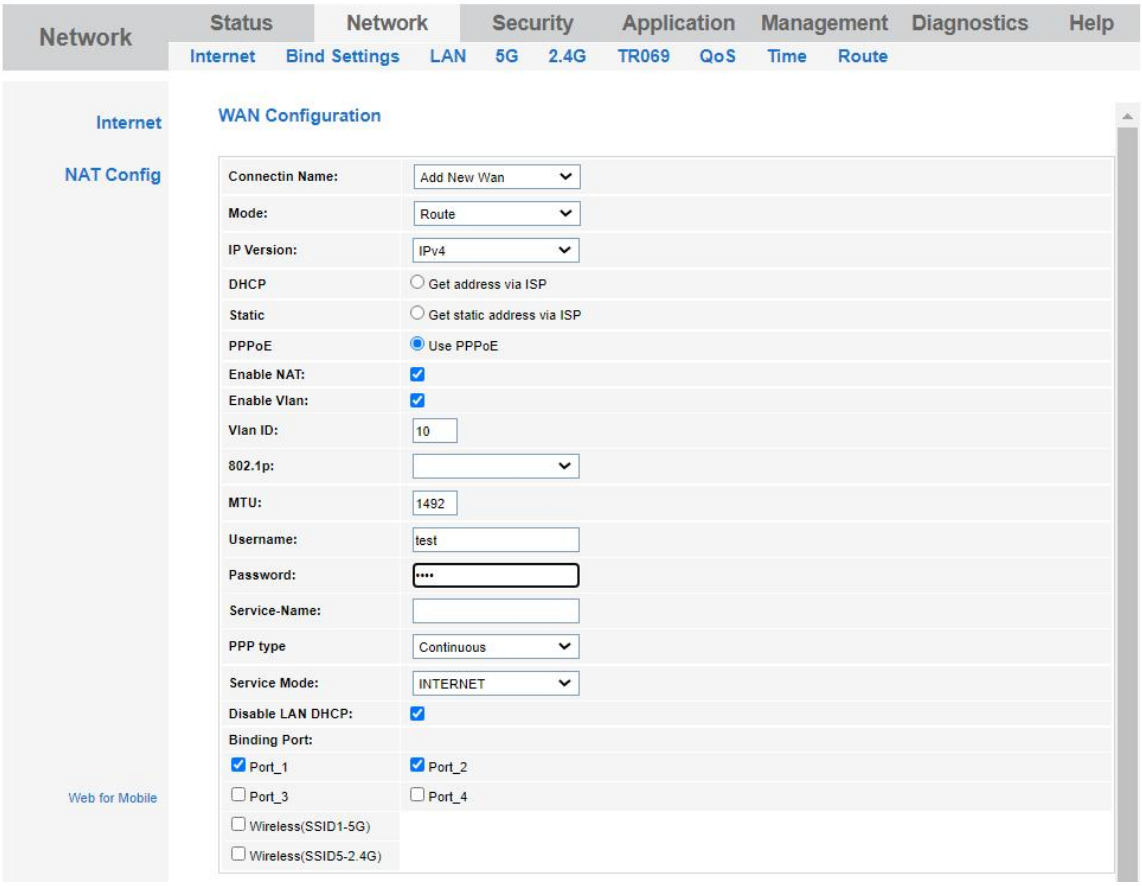


Figure 4-14: Add a WAN connection for Internet service

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

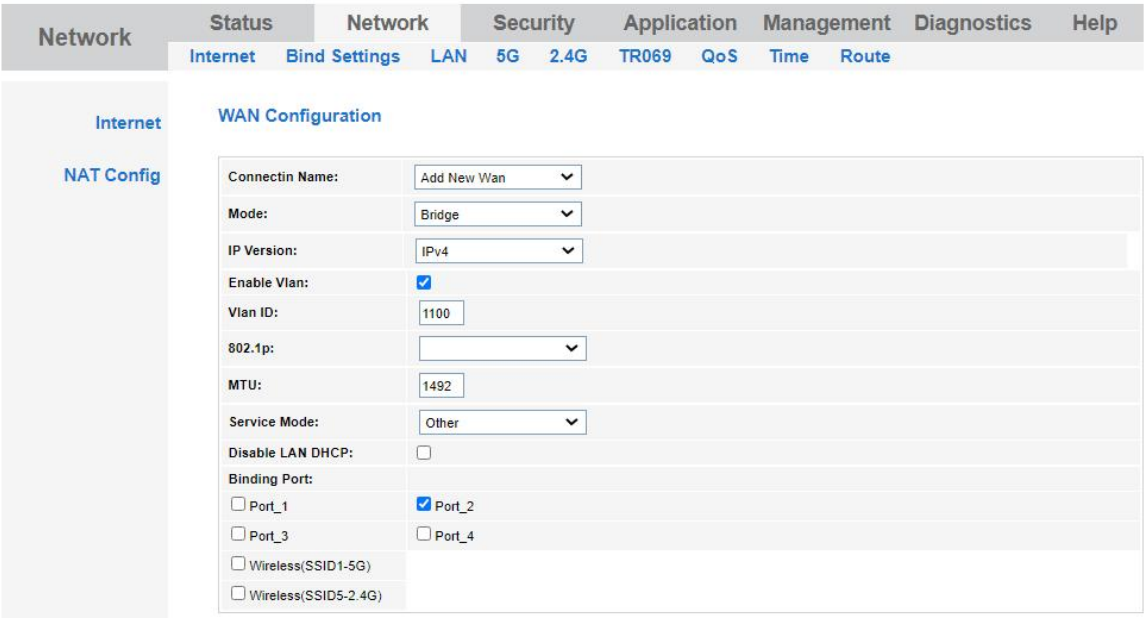


Figure 4-15: Add a WAN connection for IPTV service

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.

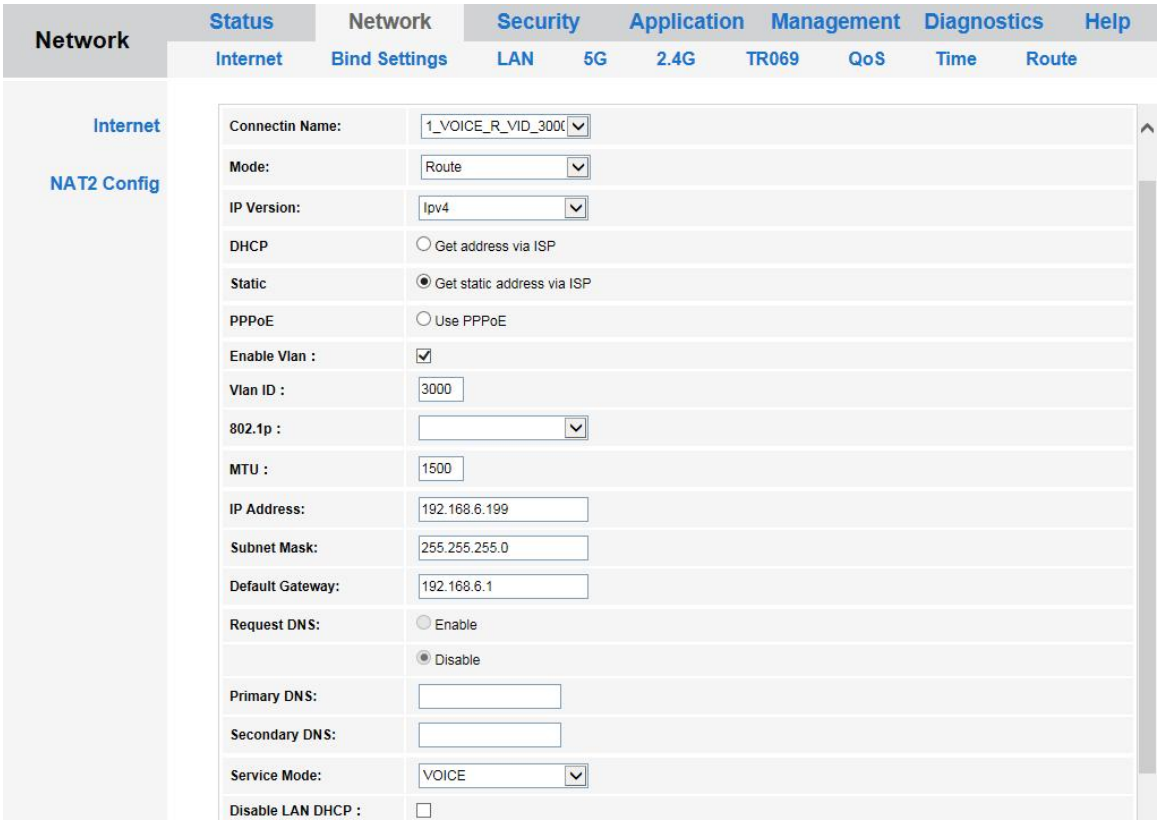


Figure 4-16: Add a WAN connection for VOIP service

2) Configure VOIP general parameters

Choose “Application > VOIP > VOIP Configuration” 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 192.168.3.19, port is 5060;
- ✧ Fill up phone number, username and password of each line.
- ✧ Choose packing time, default is 20ms.

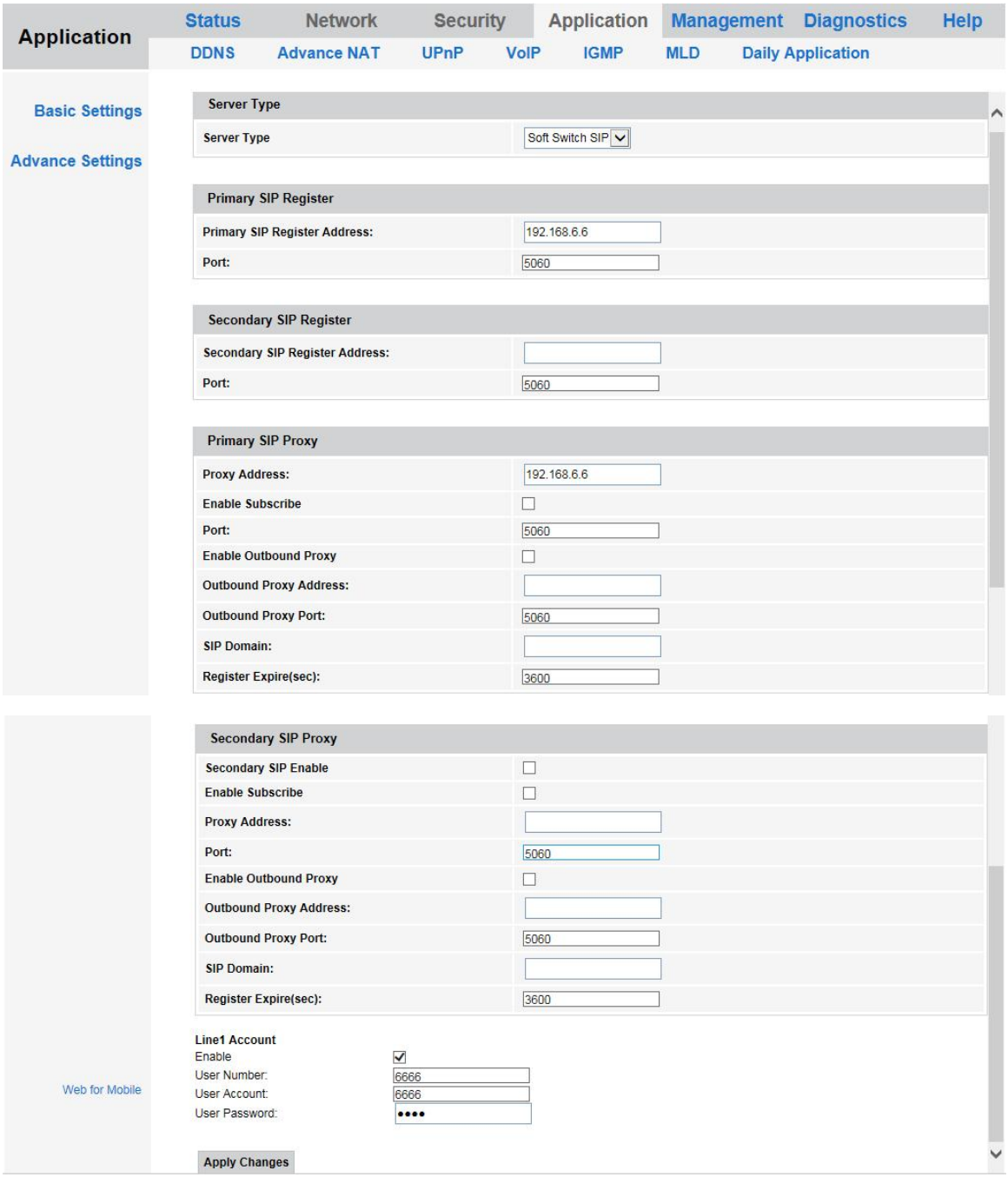


Figure 4-17: VOIP general settings

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 > VoIP Information > VoIP Information” in navigation menu. You can use VoIP service when register status is successful.



Figure 4-18: VOIP information

4.6 WLAN service

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

4.6.1 Requirement

1) HGU works on Route mode, HGU gets IP by DHCP mode,VLAN ID is 11.

2) Only enable SSID 1, its name is “xyz”. Network authentication method is WPA-PSK, and encryption method is TKIP+AES.

4.6.2 Steps

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

1) Add a WAN connection

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

- ✧ Obtain IP address by DHCP.
- ✧ Enable VLAN and VLAN ID is 11.
- ✧ Service mode is INTERNET and bind SSID1.
- ✧ Other parameters keep default.

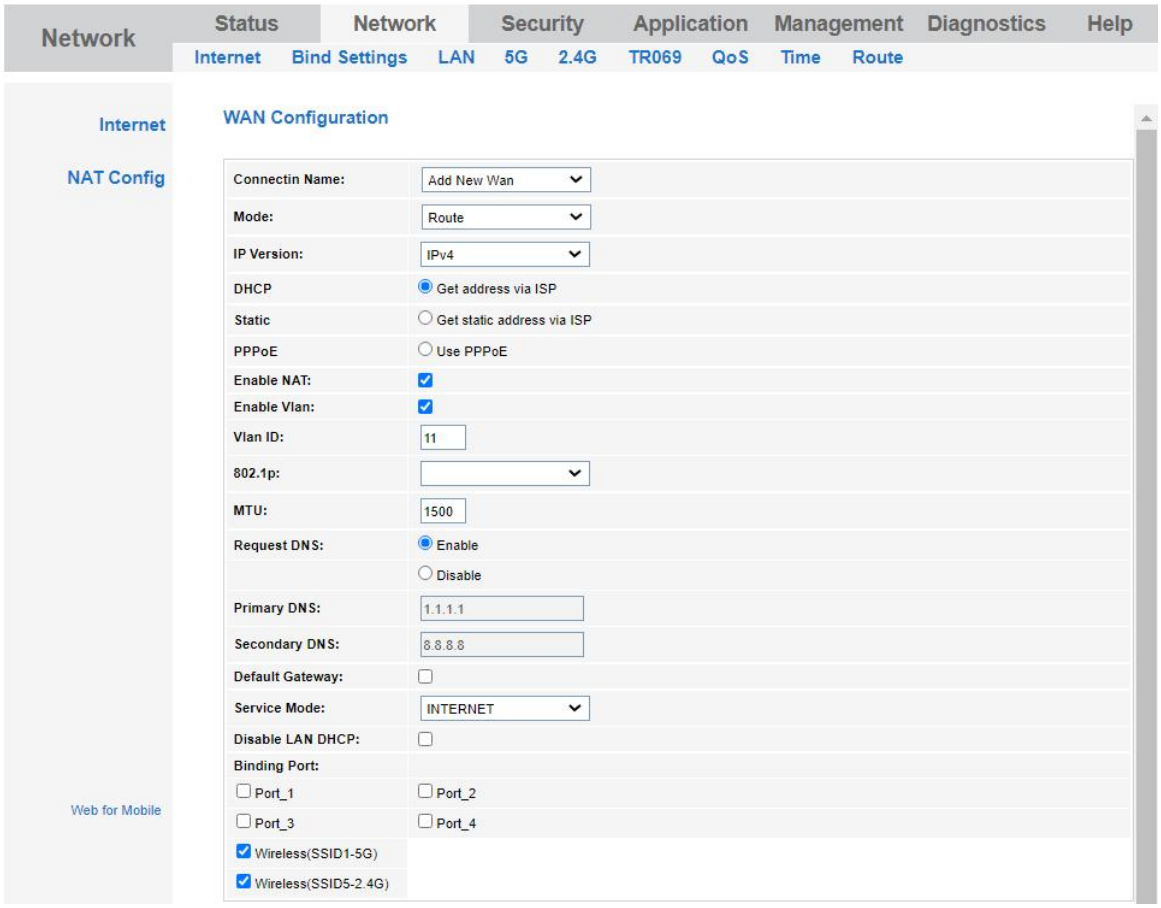


Figure 4-19: Add a route WAN connection

2) Configure WLAN basic parameters

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

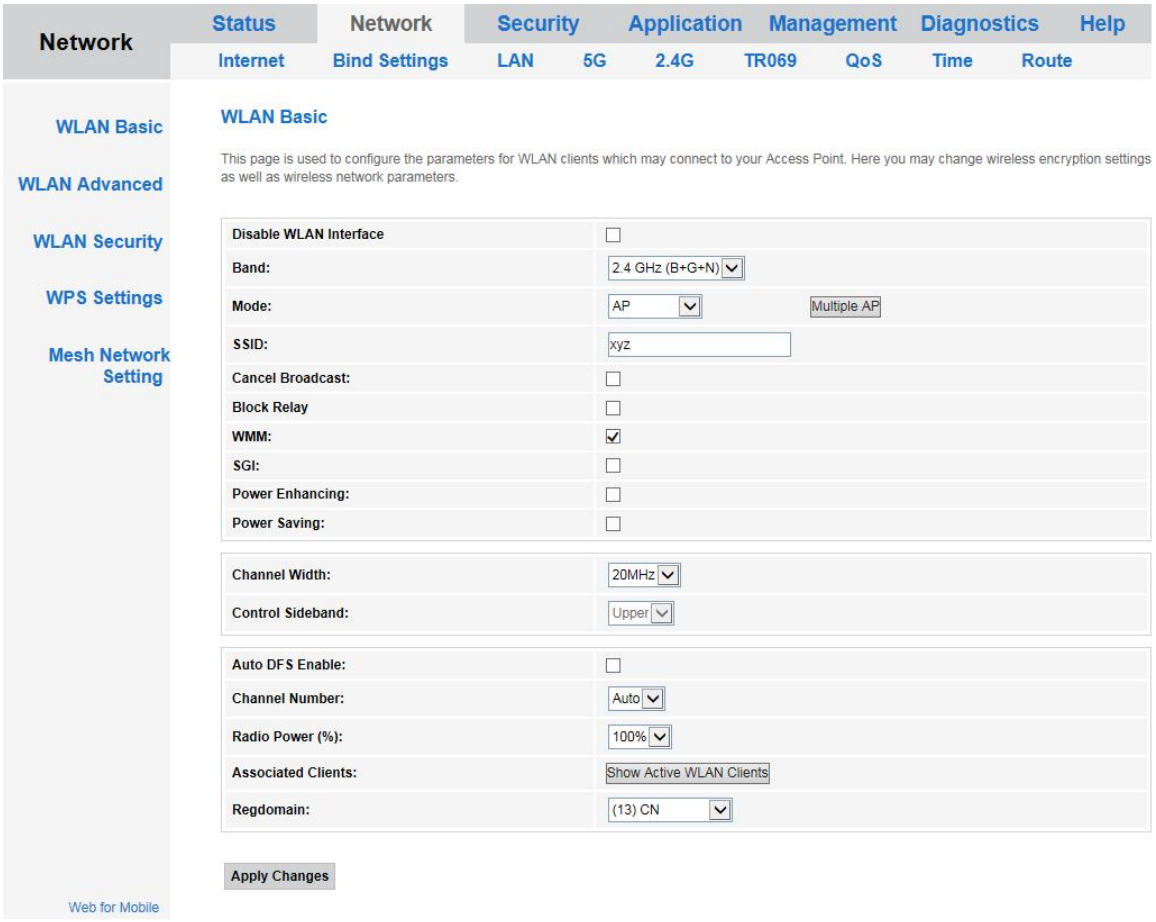


Figure 4-20: WLAN basic settings

3) Configure network authentication

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

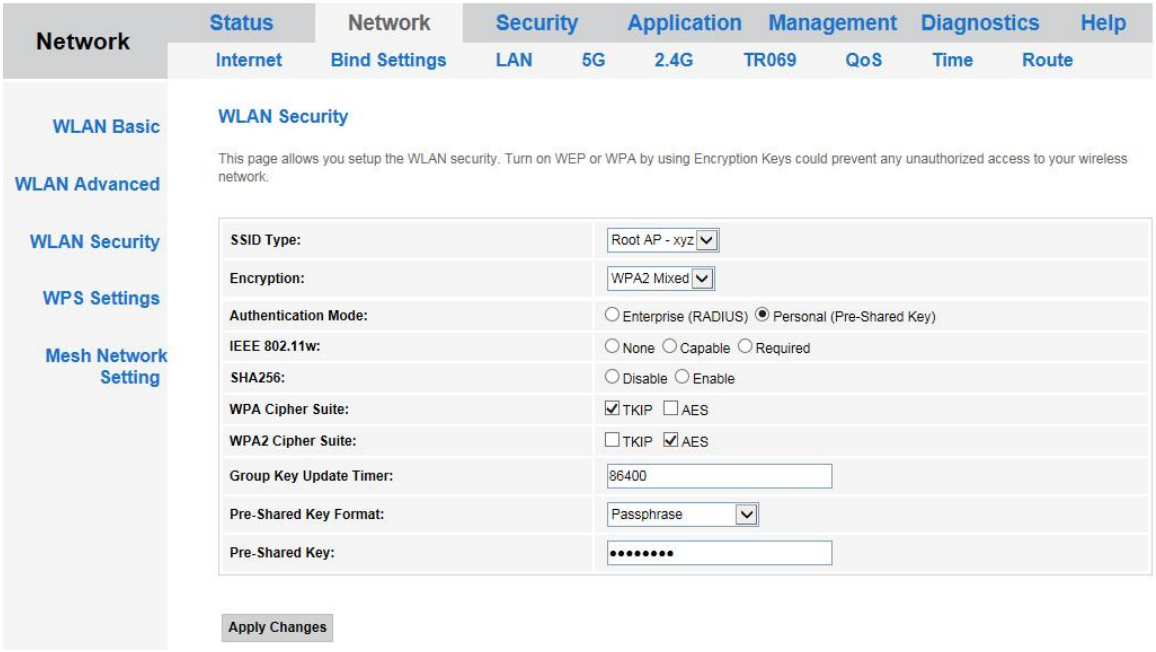


Figure 4-21: WLAN security settings

4) Surf the Internet

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

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

4.7 Update image

You can update software image on webpage.

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

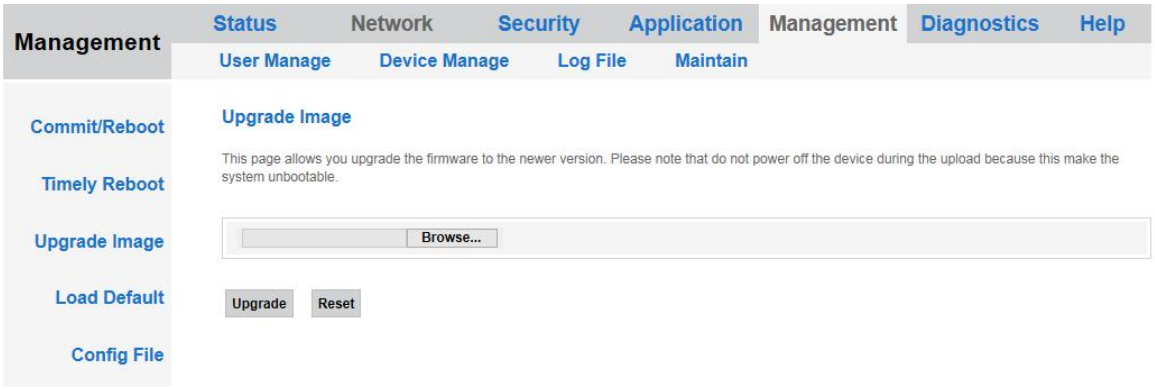


Figure 4-22: Update software

Chapter 5 FAQ

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

   A: (1) Power is off or power adapter is bad.

   (2) Indicator LED switch is turned off.

2. **Q:** Why Los indicator flashes?

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

   (2) Optical power is too low.

   (3) The fiber is dusty.

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

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

   (2) The cable breaks down or connection loosened.

   (3) The cable type incorrect or too long.

4. **Q:** FXS indicators are not lit?

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

   (2) SIP accounts aren't registered.

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

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

   (2) The cable breaks down.

   (3) IP conflict or have loopback.

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

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

   (2) There is loopback or attack in network.

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

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

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

   (2) SIP accounts aren't registered.

   (3) Dial plan is wrong.

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

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

   (2) The device overheats.