ASCENT
Communication Technology

ACT AP224S
GPON HGU

User Manual

Revision A

ACT AP224S GPON HGU

User Manual

ACT Document Number: ACT AP224S User Manual Revision A

This document is produced to assist professional and properly trained personnel with installation and maintenance issues for the product. The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.

For more information, contact ACT: support@ascentcomtec.com

Revision History

Revision	Date	Reason for Change
A	8/03/2016	Initial Release

Table of Contents

Chapter 1. Product Introduction 4

1.1 Product Description 4
1.2 Special Features 5
1.3 Technical Parameters 5
1.4 Application Chart 6
1.5 Panel Description 6

Chapter 2. Quick Installation 8

2.1 Standard Packing Contents 8
2.2 Quick Installation 8
2.3 Set up Connection 9

Chapter 3. Configuration 10

3.1 Login 10
3.2 Status 10
3.3 Network 14
3.4 Security 29
3.5 Application 33
3.6 Management 43
3.7 Diagnose 47
3.8 Help 49

Chapter 4. Examples 50

4.1 Internet Service 50
4.2 IPTV service 53
4.3 VoIP service 58
4.4 Internet and IPTV service mixed 60
4.5 Internet, IPTV and VoIP service mixed 67
4.6 WLAN service 73
4.7 Update image 77

Chapter 5. Troubleshooting 78

Chapter 1. Product Introduction

1.1 Product Description

AP224S GPON HGU ONT is a GPON optical network unit designed to meet the requirements of broadband access networks. It is ideal for FTTH/FTTO applications to provide data, voice, and video services based on a GPON network.

AP224S GPON ONT meets the ITU-T G.984 GPON standard and delivers higher bandwidth and higher efficiency using larger variable-length packets. It provides two POTS ports, four GE auto-adapting Ethernet ports, one CATV output, and one 802.11 n/b/g Wi-Fi port. It features high-performance forwarding capabilities to ensure excellent experience with VoIP, internet, and HD video services. AP224S provides a perfect terminal solution and future-oriented service supporting capabilities for FTTH deployment.

AP224S offers efficient packaging of user traffic, with frame segmentation allowing higher quality of service (QoS) for delay-sensitive voice and video communications traffic. AP200C series GPON ONT provides the reliability and performance expected for business services and are an attractive way to deliver residential services. GPON enables Fiber to The Home (FTTH) deployments economically resulting to accelerated growth worldwide.

AP224S Home Gateway with 4GE + 2POTS + WiFi + CATV HGU terminal devices are designed to fulfill the FTTH and triple play service demands of fixed network operators and cable operators. AP224S features 802.11n WiFi (2T2R), Layer 2/3, and high-quality VoIP technlogy. AP224S units are highly reliable and easy to maintain, with guaranteed QoS for different services. They are also fully compliant with technical regulations such as ITU-T G.984.x and GPON equipment (V2.0) technical requirements as specified by China Telecom.

Figure 1-1: 4GE + 2POTS + WiFi GPON HGU

1.2 Special Features

- Plug and play, integrated auto detecting, auto configuration, and auto firmware upgrade technology.
- Integrated TR069 remote configuration and maintenance function.
- Support 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) function.
- Support NAT, Firewall function.
- Support IPv4 and IPv6 dual stack.
- Integrated line testing compliant with GR-909 on POTS.
- The WAN port supports bridge, router and bridge/router mixed mode.

1.3 Technical Parameters

Item	Description
PON Interface	1 × GPON connector
	SC single-mode/single-fiber
	Upstream 1.25 Gbps
	Downstream 2.5 Gbps
Wavelength	Tx 1310 nm
	Rx 1490 nm
	CATV 1550 nm
Optical Interface	SC/APC connector
Interface	4 × 10/100 or 10/100/1000 Mbps auto adaptive Ethernet interfaces
	10/100M Full/Half Duplex, 1000M Full Duplex. RJ45 connectors
	2 × POTS, RJ11 connectors
	1 × SCTE F connector
Wireless	Compliant with IEEE802.11b/g/n, 300 Mbps, 2T2R two internal antennas
LED	13, for SYS, POWER, PON, LOS, WPS, WiFi, POTS, LAN, CATV
Operating Temperature	-5 °C to 55 °C
Storage Temperature	-30 °C to 60 °C
Operating Humidity	10 % to 90 % (non-condensing)
Storage Humidity	10 % to 90 % (non-condensing)
Power Supply	DC 12 V, 1/1.5A
Power Consumption	≤10 W
Dimensions (L × W × H)	247 mm × 147 mm × 37 mm
Net Weight	0.5 kg

1.4 Application Chart

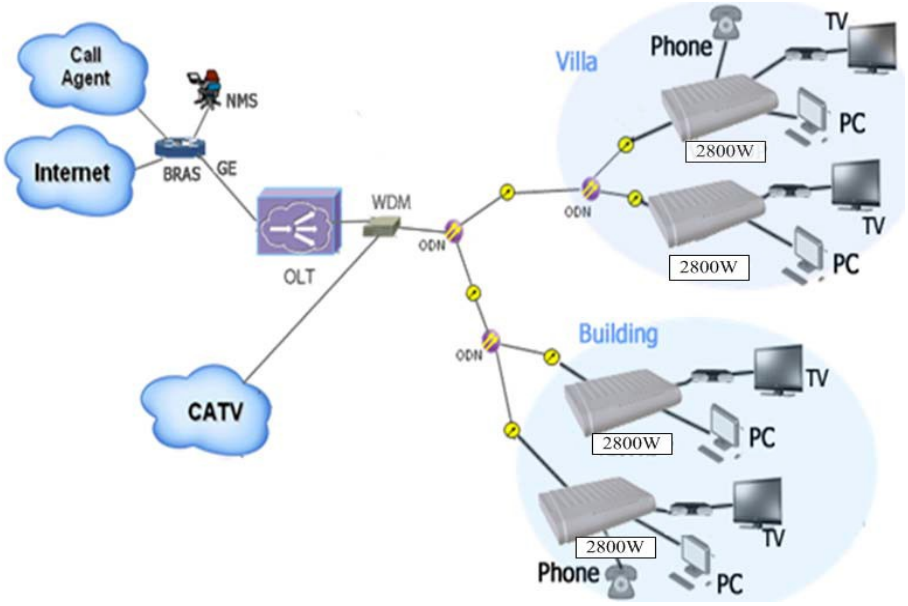

Figure 1-2: Application Chart

1.5 Panel Description

Interface Panel

Figure 1-3: Interface panel

Name	Function
PON	Connect PON port to the internet using an SC type single-mode optical fiber cable
Phone 1/2	Connect a telephone with the FXS port using a telephone wire. If you only have one telephone, you should use the FXS1 port
LAN 1/2/3/4	Connect the LAN ports to your devices using RJ45 Ethernet cables
WPS	Press down Wi-Fi turn on/off for 3 seconds to enable/disable WiFi
WiFi	Hold down the reset button for 1 to 5 seconds to make the device restart and recover from the factory default settings
Reset	Press down the WPS button for 0.1 to 3 seconds to activate the WPS function
DC12V	Connect with power adapter
PWR	Turn power on/off
CATV	SCTE type F TV antenna

Indicator Panel

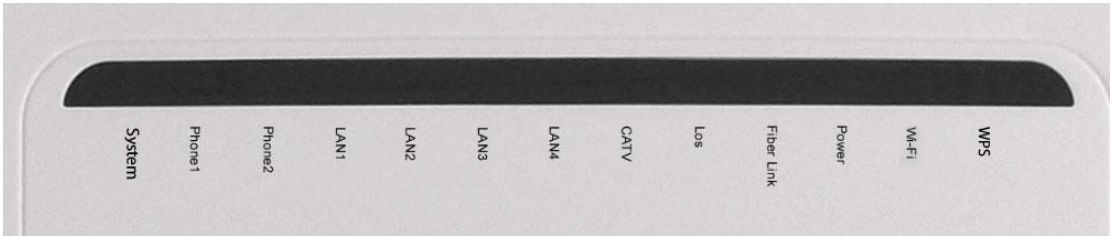

Figure 1-4: Indication panel

Name	Color	Status	Function
PWR	Green	OFF	Power is not supplied
		ON	Power is supplied
Fiber Link	Green	OFF	Device is not registered to GPON OLT
		ON	Device has been registered to GPON OLT
		Flash	Device is registering
LOS	Red	OFF	Rx optical power is normal
		Flash	Rx optical power is lower than the sensitivity of the optical receiver
CATV	Yellow	ON	CATV optical RX power <-8 dbm
	Green	ON	CATV optical RX power <-8 dbm
	Red	ON	CATV optical RX power >2 dbm
WPS	Green	OFF	Does not use WPS or WPS client is connected (LED automatically turns off after 5 minutes of successful connection)
		ON	WPS client is connected. (LED automatically turns off after 5 minutes of successful connection)
		Flash	WPS client is connecting
WiFi	Green	OFF	Device is powered off or WiFi is turned off
		ON	WiFi is turned on
		Flash	WiFi is turned on and currently transmitting data
PHONE 1/2	Green	OFF	Device is powered off or not registered to the soft-switch
		ON	Device has registered to the soft-switch
		Flash	The port is working
System	Green		
LAN1/2/3/4	Green	OFF	Device is powered off or Ethernet link is not established
		ON	Ethernet link is established but not currently transmitting data
		Flash	The port is currently transmitting data

Chapter 2. Quick Installation

2.1 Standard Packing Contents

When you receive our products, please check carefully to make sure that all of the products arrived in a good condition without defects. If something went wrong during shipping, please contact the carrier; for other damage or missing parts, please contact the dealer.

Contents	Description
4 GE + 2 POTS + WiFi + CATV Home Gateway	1 pc
Power Adapter	1 pc
User Manual	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 6 cm. 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. Keep a minimum 10 cm clearance on all sides of the unit 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 (refer to Figure 1-5) and two flat-head wood screws.

a. Insert the screws into the wall. The screw positions must be on the same horizontal line and the distance between them must be 165 mm. Reserve at least 6 mm 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 GPON HGU Ethernet port using an RJ45 Cat 5 cable.

Set up Wireless Connection

Choose the wireless network name (SSID) “Broadcom1”, there is no password by default.

Chapter 3. Configuration

After finishing the basic connection configuration, basic functions are available for use. In order to satisfy individuation service requirements, this chapter provides you with parameter modifications and individual configuration descriptions.

3.1 Login

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

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

Note The default administrator login User Name “admin”, and the default login Password is “vsONU101”.

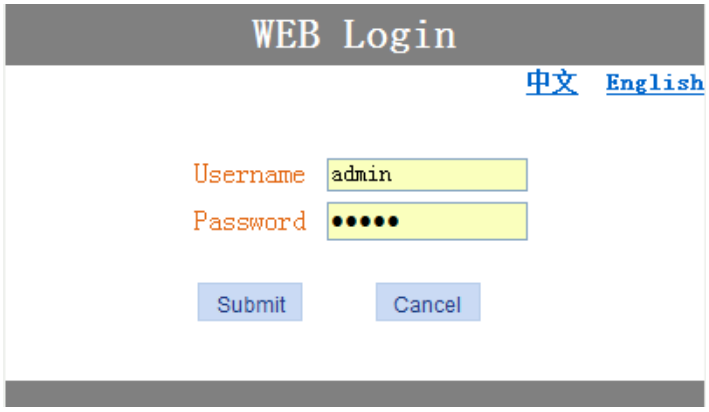

Figure 3-1: Login

3.2 Status

This tab displays basic product information.

3.2.1 Device Info

This page shows basic information for the device such as model, mark no., hardware version, software version, and CFE version.

Figure 3-2: Device Info

3.2.2 Network Info

3.2.2.1 WAN Info

This page shows the WAN connection information you have configured. The WAN connection's protocol can be configured to IPv4, IPv6, or both of them.

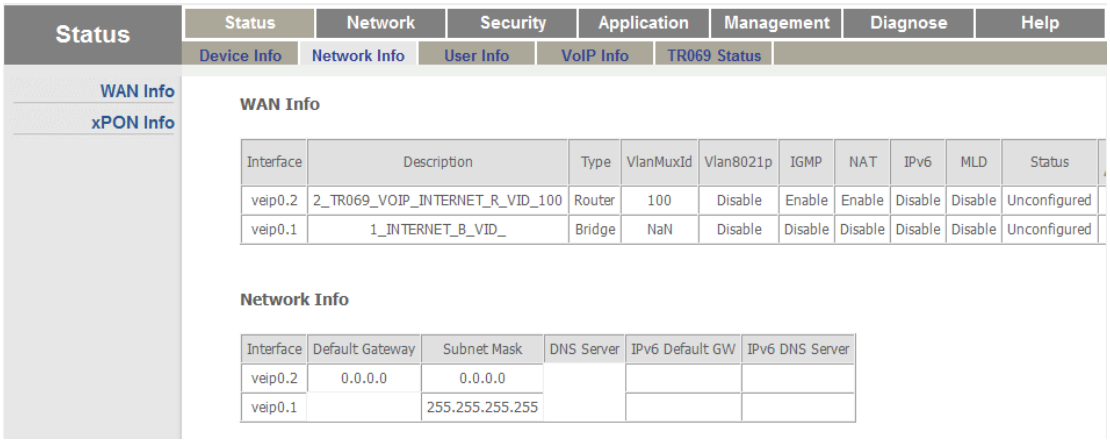

Figure 3-3: WAN Info

3.2.2.2 xPON Info

This page shows the PON information, such as temperature, voltage, current, power, and packet traffic statistics.

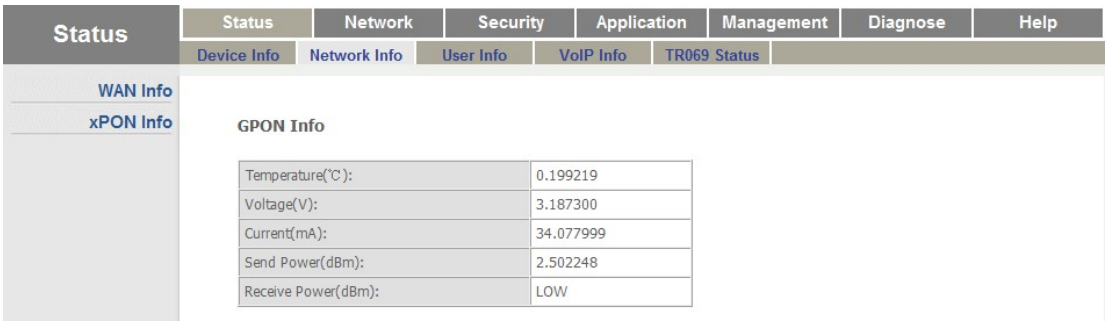

Figure 3-4: xPON Info

3.2.3 User Info

3.2.3.1 WLAN Interface

This page shows WLAN information such as SSID name, whether security is enabled, and packet traffic statistics.

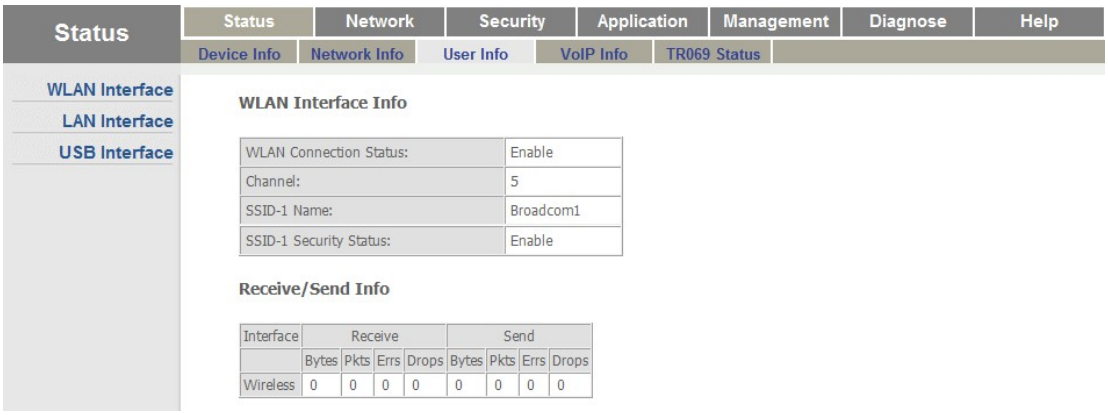

Figure 3-5: WLAN Interface

3.2.3.2 LAN Interface

This page shows LAN information such as LAN gateway information, LAN interface packet traffic statistics, and a list of connected clients.

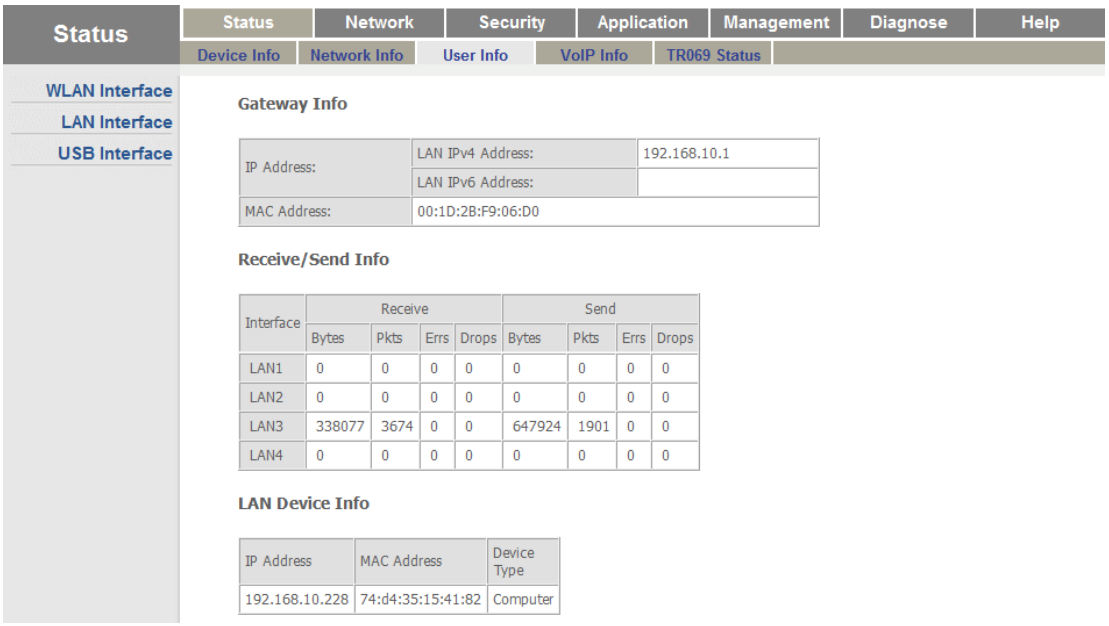

Figure 3-6: Ethernet Interface

3.2.4 VoIP Info

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

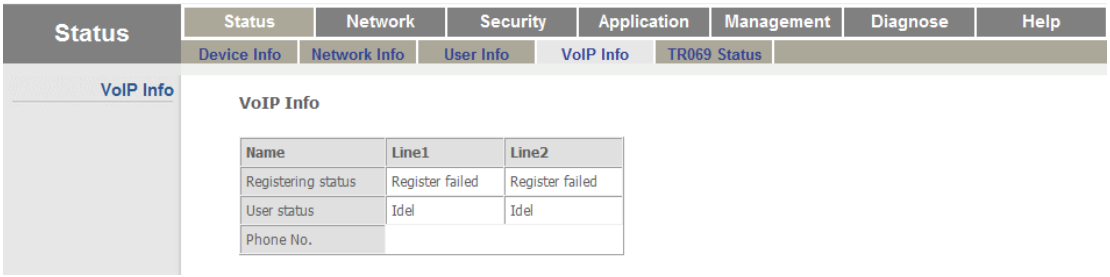

Figure 3-7: VoIP Info

3.2.5 TR069 Status

This page shows the request status of ITMS connections.

Figure 3-8: TR069 Status

3.3 Network

3.3.1 Internet

This page allows you to configure WAN connections. You can't add a WAN connection if you have eight connections configured because the maximum number of WAN connections is eight.

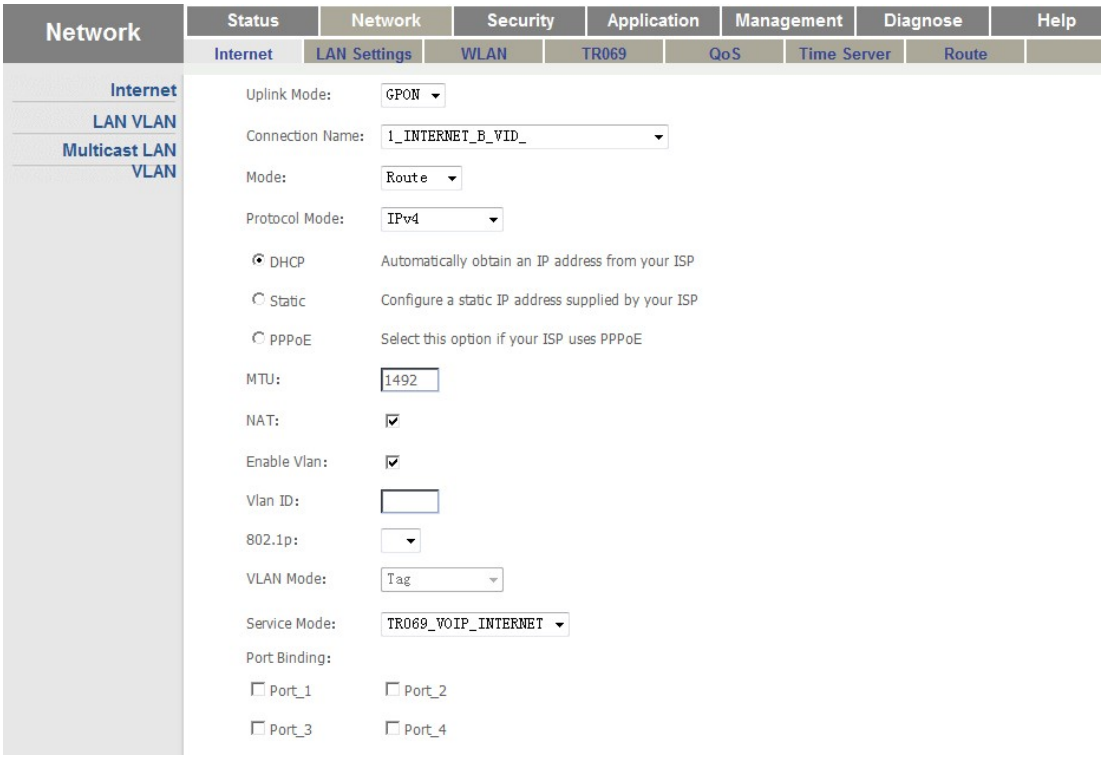

Figure 3-9: Internet

Parameters	Description
Uplink Mode	The uplink mode is set to GPON for this product. It cannot be changed.

Connection Name	This is the list table of WAN connection names. If you want to create a new WAN connection, please select “Add WAN Connection” and input other parameters and then click the “Save/Apply” button. If you want to edit a WAN connection, please select the WAN connection name you want to edit and change the parameters and then click the “Save/Apply” button. If you want to delete a connection, please select the WAN connection you want to delete and then click the “Del” button.
Mode	Bridge: The LAN ports you have selected in this WAN connection and PON port are in bridge mode. Route: The LAN ports you have selected in this WAN connection and PON port are in route mode.
Protocol Mode	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.
MTU	MTU: Max transfer unit. Default Value: 1500 in bridge mode, 1492 in route mode.
NAT	Enable: Open NAT function. Disable: Close NAT function.
Enable VLAN	Disable: In this WAN connection, the packets transmitted by the PON port aren’t given a VLAN tag. Enable: In this WAN connection, the packets transmitted by the PON port are given a VLAN tag. VLAN ID: Input the VLAN ID you want to set. 802.1p: Select the port priority you want to set. VLAN Mode: Tag or Transparent. If you select route mode, the VLAN mode is set to tag mode and it can’t be changed.
IPv4 Static IP Settings	IP Address: Please input WAN IP address. Subnet Mask: Please input WAN IP address mask. Default Gateway: Please input gateway. Primary DNS: Please input primary DNS. Secondary DNS: Please input secondary DNS.
IPv6 Static IP Settings	WAN IPv6 gateway address: Please input WAN IP gateway. WAN IPv6 address: Please input WAN IP address. Primary IPv6 DNS server: Please input primary DNS. Secondary IPv6 DNS server: Please input secondary DNS.
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 a service mode which includes VoIP such as TR069_VoIP_INTERNET, TR069_VoIP, VoIP, or VoIP_INTERNET.
Port Binding	Shows which LAN port or SSID the WAN connection has included.

Port binding is only effective to OTHER mode WAN connections.

Note

If a port isn't bound to an OTHER mode WAN, it will give preference to OTHER mode WAN connections for upstream when there is no LAN VLAN rule and give preference to INTERNET mode WAN connections for upstream when there is a LAN VLAN rule.

DHCP HGU servers will not affect the LAN port which is bound to OTHER mode WAN for upstream. You can't visit webpages from this port.

3.3.2 LAN VLAN

This page allows you to configure LAN interface VLAN.

3.3.2.1 Basic Mode Settings

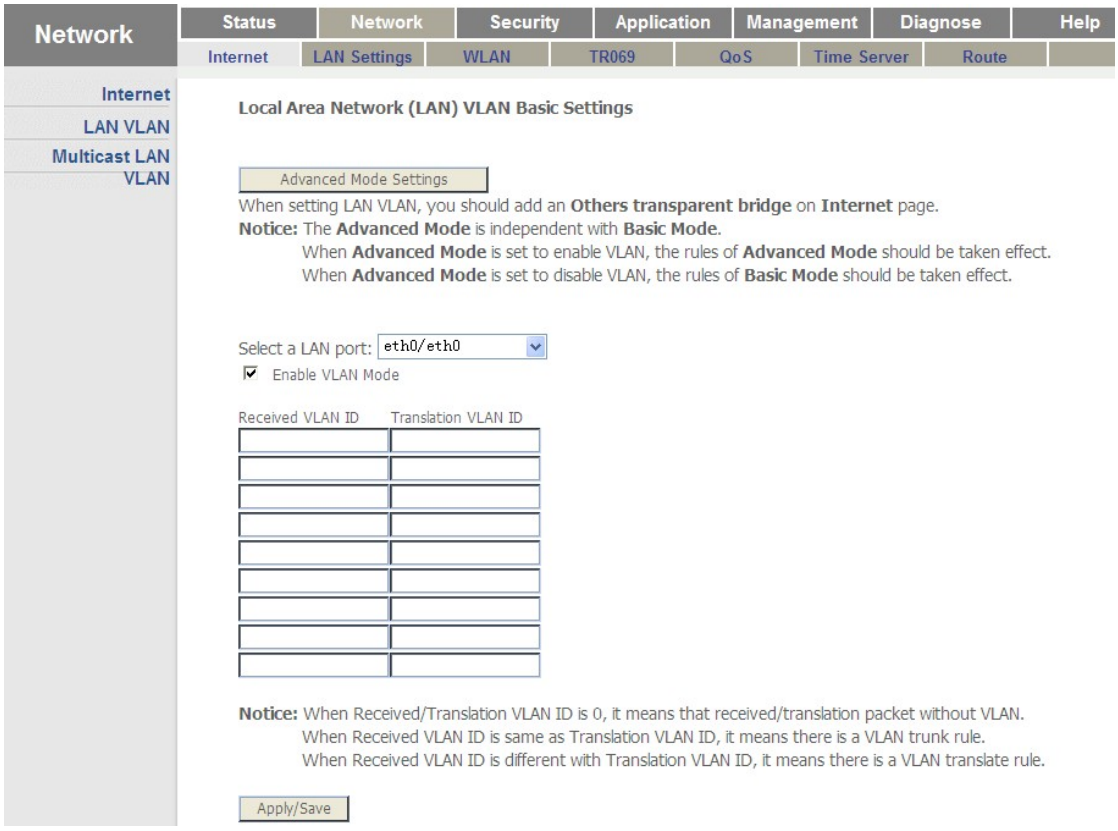

Figure 3-10: LAN VLAN basic mode settings

Parameter	Description
Enable VLAN Mode	VLAN mode toggle.
Received VLAN ID	LAN port received VLAN.
Translation VLAN ID	LAN port translated VLAN. LAN port sends messages to PON port with this VLAN.

For example,

1. Received VLAN ID is 0, translation VLAN ID is 99.

   The port is in tag mode, VLAN ID is 99.

2. Received VLAN ID is 99, translation VLAN ID is 99.

   The port is in trunk mode, VLAN ID is 99.

3. Received VLAN ID is 77, translation VLAN ID is 99.

   The port is in translation mode. The port receives messages with VLAN 77, then translates to VLAN 99 and sends to PON port.

4. Received VLAN ID is 0, translation VLAN ID is 0.

   The port is in transparent mode.

Advanced Mode Settings

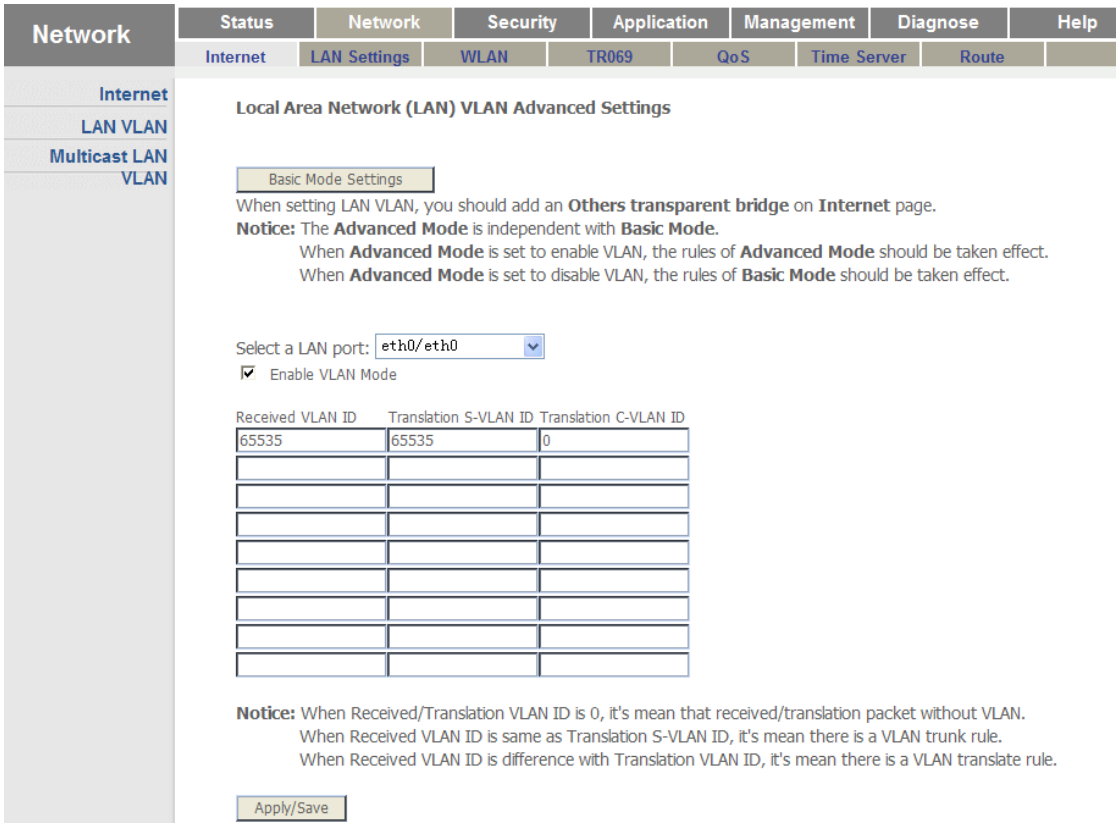

Figure 3-11: LAN VLAN advanced mode settings

Parameters	Description
Enable VLAN mode	VLAN mode toggle.
Received VLAN ID	LAN port received VLAN.

Translation S-VLAN ID	LAN port translated service VLAN.
Translation C-VLAN ID	LAN port translated custom VLAN.

For example,

1. Received VLAN ID is 0, translation S-VLAN ID is 99.

   The port is in tag mode, VLAN is 99.

2. Received VLAN ID is 99, translation S-VLAN ID is 99.

   The port is in trunk mode, VLAN is 99.

3. Received VLAN ID is 77, translation S-VLAN ID is 99.

   The port is in translation mode. The port receives messages with VLAN 77, then translates to VLAN 99 and sends to PON port.

4. Received VLAN ID is 65535, translation S-VLAN ID is 65535.

   The port is in transparent mode.

5. Received VLAN ID is 22, translation S-VLAN ID is 33 and translation C-VLAN ID is 44.

   The port is in QinQ mode. The port receives messages with VLAN 22, sends to PON port with double VLAN where the inner VLAN is 44 and outer VLAN is 33.

3.3.3 Multicast LAN VLAN

This page allows you to configure multicast VLAN of LAN ports.

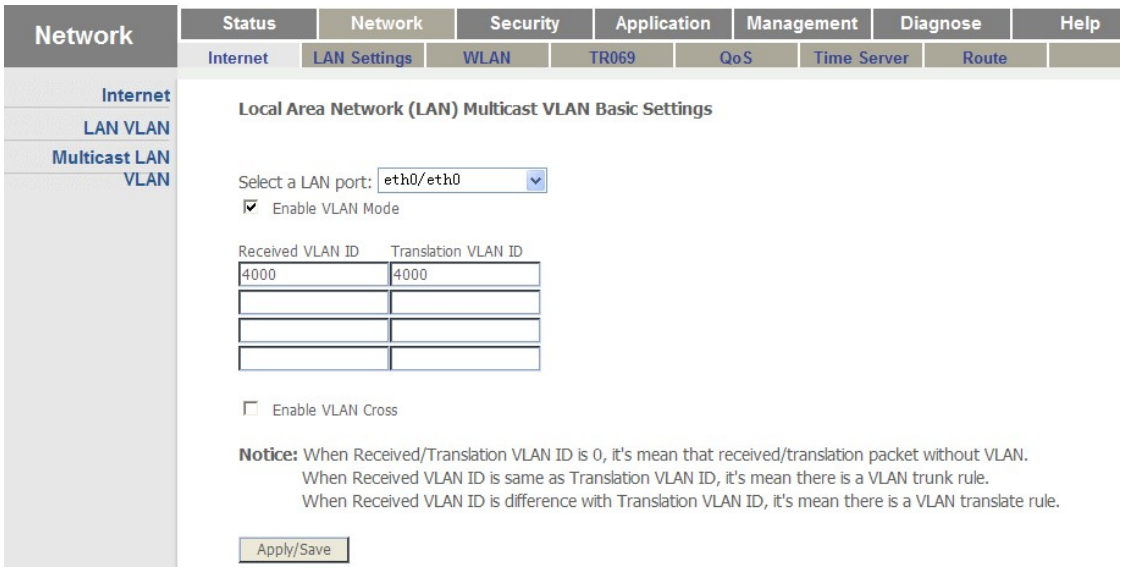

Figure 3-12: LAN multicast VLAN

Parameter	Description
Enable VLAN Mode	Multicast VLAN mode switch.
Received VLAN ID	LAN port received VLAN.
Translation VLAN ID	LAN port translated VLAN.
Enable VLAN Cross	Multicast VLAN cross switch. Join or leave messages do not need to carry the same VLAN as the multicast VLAN when VLAN cross is enabled; but it must be the same as the multicast VLAN when it is disabled.

For example,

1. Received VLAN ID is 0, translation VLAN ID is 10.

   The multicast VLAN of the port is in tag mode, VLAN is 10.

2. Received VLAN ID is 10, translation VLAN ID is 10.

   The multicast VLAN of the port is in trunk mode, VLAN is 10.

3. Received VLAN ID is 10, translation VLAN ID is 20.

   The multicast VLAN mode of the port is in translation mode. The LAN port translates multicast VLAN 20 to VLAN 10 before sending multicast streams to customers.

3.3.4 LAN Settings

3.3.4.1 IPv4

This page allows you to set LAN settings such as LAN IP settings and DHCP server settings.

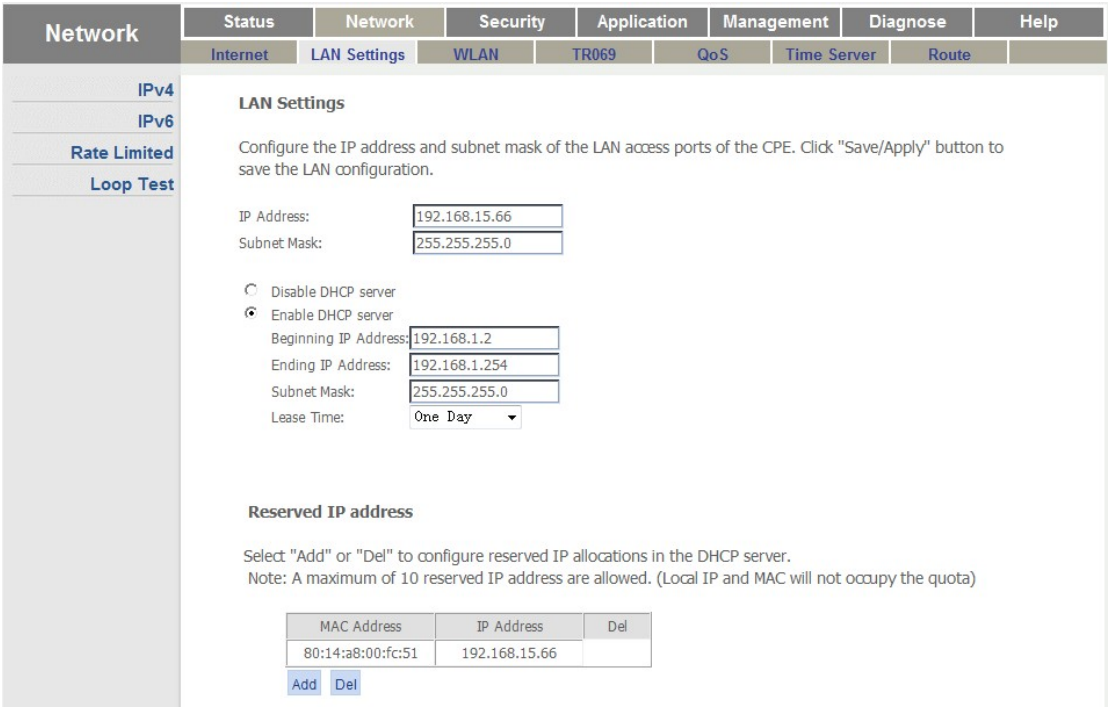

Figure 3-13: IPv4 Settings

Parameters	Description
IP Address	LAN IP address.
Subnet Mask	LAN IP mask.
Disable DHCP Server	DHCP server is disabled.
Enable DHCP Server	Enable HGU DHCP server. Beginning IP Address: The first IP address of the IP pool. Ending IP Address: The last IP address of the IP pool. Subnet Mask: The subnet mask of the IP pool. Lease Time: The lease time of an IP address.
Reserved IP Address	Click the “Add” button to configure IP addresses you want to reserve. If you want to delete a reserved IP configuration, select the “Del” checkbox and then click the “Del” button.

3.3.4.2 IPv6

This page allows you to configure the IPv6 DHCP server.

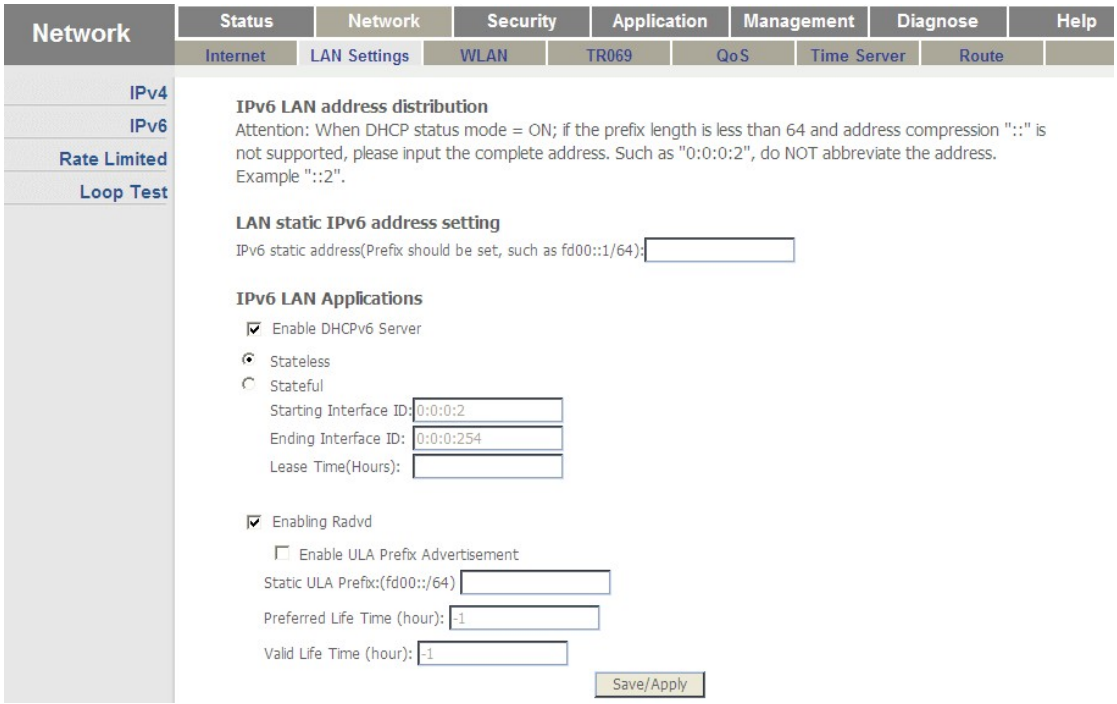

Figure 3-14: IPv6 Settings

Parameter	Description
LAN Static IPv6 Address setting	LAN IPv6 address.
Enable DHCPv6 Server	Enable or disable DHCPv6 server.
Stateless	In this mode, the terminal host gets a gatherable unicast IP address according to the global address prefix which the router declared, and its interface ID.

Stateful	In this mode, DHCP is used to configure the host. You should set up a DHCP server according to your requirements.
Enable RADVD	Enable RADVD to monitor automatic configuration requests from the IPv6 host and responses in the local area network.
Enable ULA Prefix Advertisement	Enable or disable ULA prefix advertisement.
Static ULA Prefix	Input static ULA prefix.
Preferred Lift Time	Used to restrain lease time and re-bind time. By default, lease time is 50% of preferred life time and re-bind time is 80% of preferred life time.
Valid Life Time	Lease period of IPv6 addresses. After a valid life time expires, the server will take back the IPv6 address

3.3.4.3 Rate Limited

This page allows you to configure LAN port rate limiting.

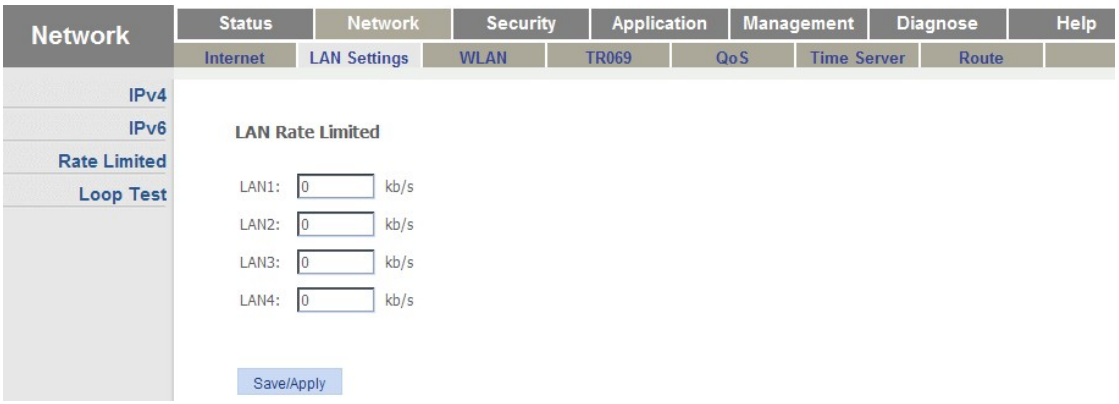

Figure 3-15: Rate Limited

Parameter	**Description**
LAN Rate Limited	Input the value you want to limit and then click “Save/Apply” button to save. 0 means no limit. This is only effective for downstream data rates.

3.3.4.4 Loop Test

This page allows you to enable the loop test function.

Figure 3-16: Enable Loop Test

3.3.5 WLAN

This tab is used to configure WIFI parameters. Click the “Save/Apply” button to save any changes you make.

3.3.5.1 WLAN Basic

This page allows you to configure basic wireless settings. Basic settings include wireless switch settings, SSID name, country, max clients, and so on for each SSID. You can enable each AP and decide whether you want the SSID hidden or not.

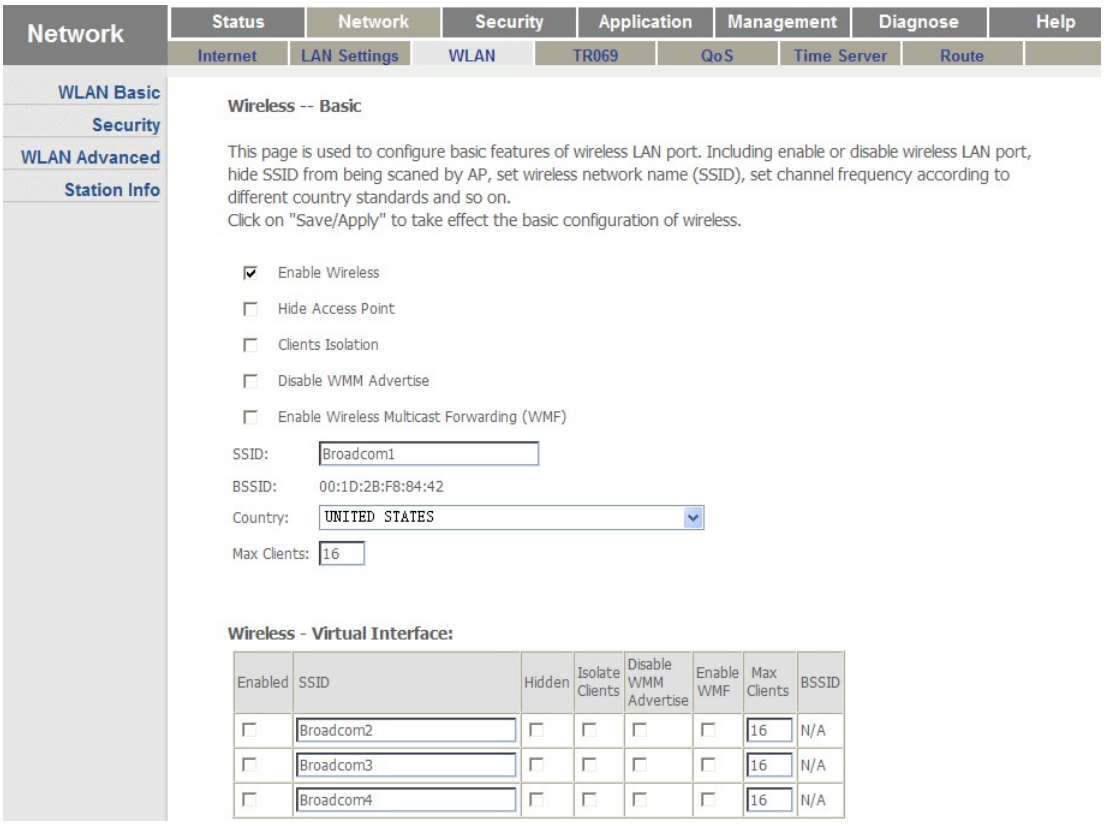

Figure 3-17: WLAN Basic

Parameter	Description
Enable Wireless	Enable or disable WLAN.
Hide Access Point	Select it to hide SSID.
Clients Isolation	Isolate each WIFI clients.
Disable WMM Advertise	Disable wireless QoS.
Enable Wireless Multicast Forwarding	Whether to enable wireless multicast or not.
SSID	SSID name.
Country	Country or region.
Max Clients	Max. clients for this SSID.

3.3.5.2 Security

This page is used to configure wireless security.

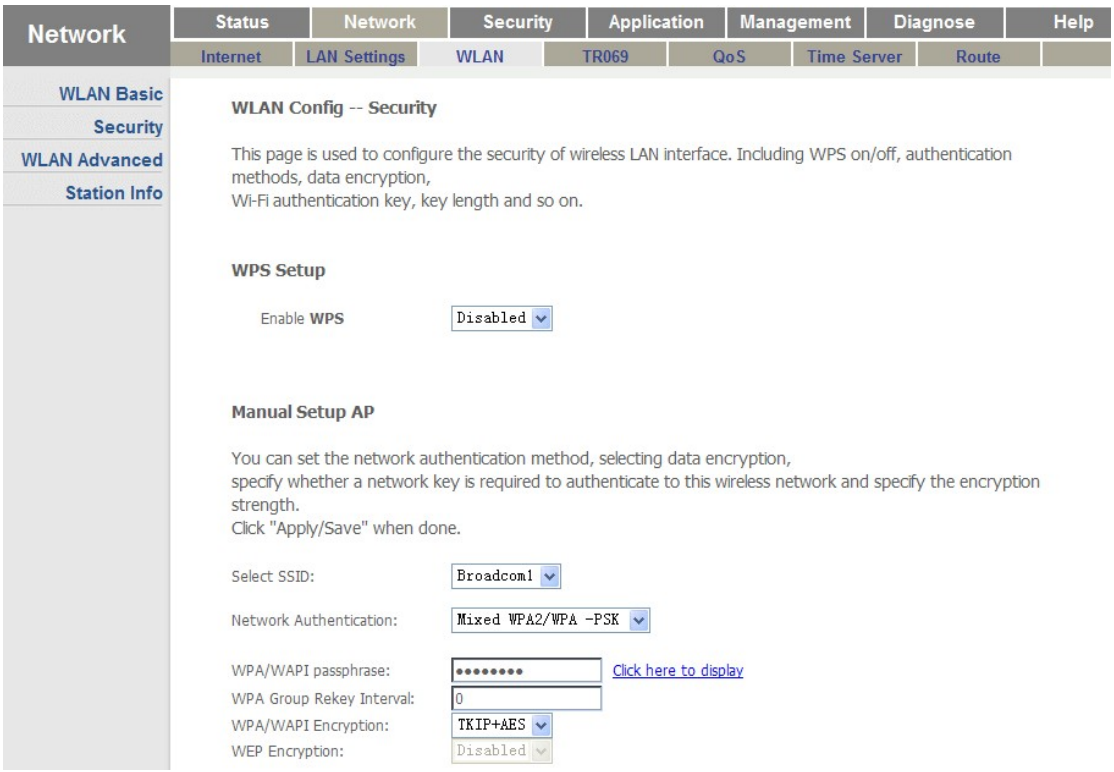

Figure 3-18: WLAN Security

In “WPS Setup” you can select whether to enable the WPS (Wi-Fi Protected Setup) function and add WPS client method: by Push Button or PIN.

In “Manual Setup AP”, select your SSID name. Take WPA-PSK for example, select “Mixed WPA2/WPA-PSK” in 【Network Authentication】, and set up a WPA-PSK password in【WPA/WAPI passphrase】.

3.3.5.3 WLAN Advanced

This page shows more detailed settings for your wireless network.

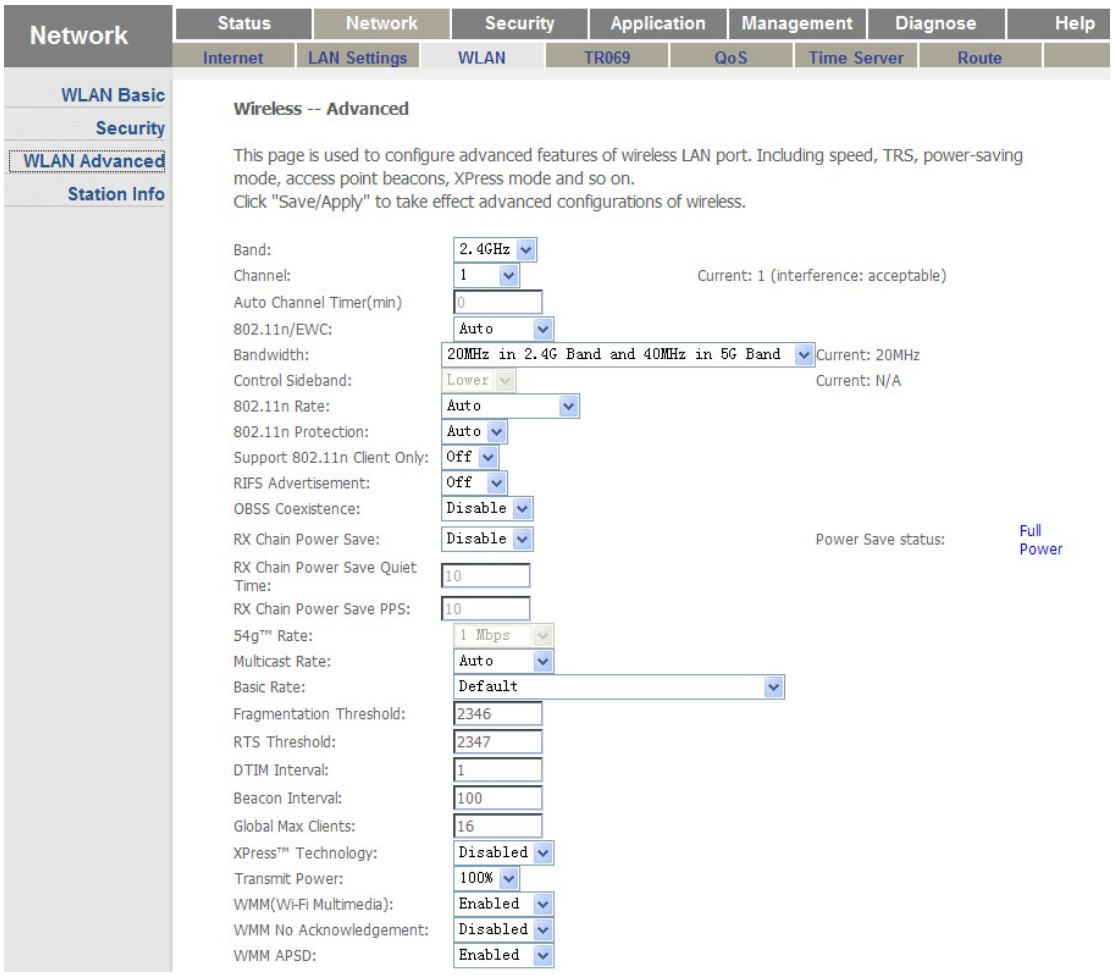

Figure 3-19: WLAN Advanced

Parameter	**Description**
Band	2.4 GHz or 5.8 GHz
Channel	Wireless channel, different bandwidths have different channel ranges.
802.11n/EWC	802.11n/EWC switch. There are other parameters for 802.11n/EWC when it is enabled.
54g™ Rate	54g™ rate
Multicast Rate	Wireless multicast rate
Basic Rate	Wireless basic rate
Fragmentation Threshold	Messages will be segmented if their length is higher than the threshold. When a fragmented transmission is interrupted, only the part that failed needs to be re-sent. The range is 256 ~ 2346 bytes, default is 2346 bytes.
RTS Threshold	RTS (Request To Send) threshold is used to avoid transmission conflicts in the WLAN.

	The smaller the value is, the faster the frequency of sending RTS messages and the less time it takes for the system to recover from interruptions or conflicts. This also costs more bandwidth and affects throughput. The range is 1 ~ 2347 bytes, default is 2347 bytes.
DTIM Interval	DTIM (Delivery Traffic Indication Map) interval. The range is 1 ~ 125, default is 1.
Beacon Interval	Beacon interval, default is 100.
Global Max Clients	The maximum number of clients for the equipment.
XPress™ Technology	Xpress technology is based on IEEE802.11e wireless multimedia extension standards. In a single network, using Xpress technology can improve the total rate of AP by 27%.
Transmit Power	Wireless transmit power. Value is 20%, 40%, 60%, 80% or 100%. The bigger the value is, the better the coverage area is.
WMM(Wi-Fi Multimedia)	Enable or disable wireless QoS function. This will improve video and voice quality of wireless terminal.
WMM No Acknowledgement	WMM No Acknowledgement switch
WMM APSD	WMM APSD switch

3.3.5.4 Station Info

This page shows the information of clients connected to your wireless network.

Figure 3-20: Station Info

3.3.6 TR069

3.3.6.1 ITMS server

This page allows you to configure ITMS server parameters.

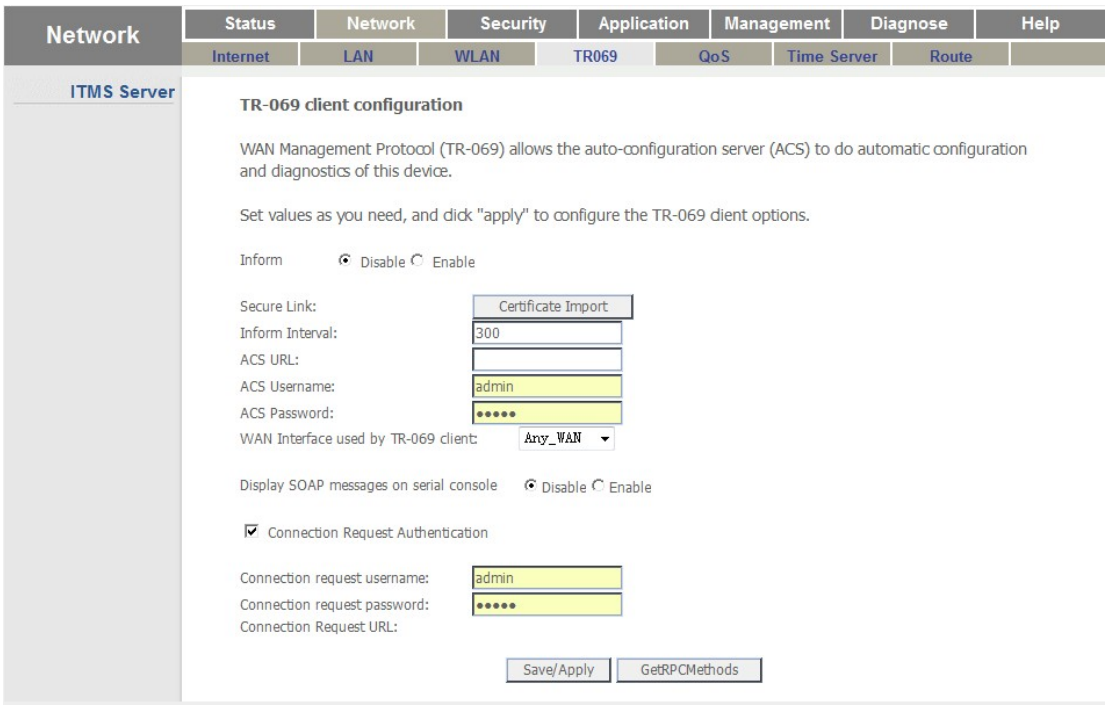

Figure 3-21: ITMS server parameters

Parameter	Description
Inform	Enable or disable HGU sending information to the server.
Inform Interval	Reconnection interval. HGU will verify connection with ITMS server at inform interval times.
ACS URL	Server provider's network management server.
ACS Username	Authentication username for HGU connecting to ITMS server.
ACS Password	Authentication password for HGU connecting to ITMS server.
WAN interface	Choose a WAN interface for TR069.
Connection request username	Authentication username for ITMS connecting to HGU.
Connection request password	Authentication password for ITMS connecting to HGU.

3.3.6.2 LOID

This page shows the LOID settings. After inputting the LOID and password you can click the "save/effect" button to save them.

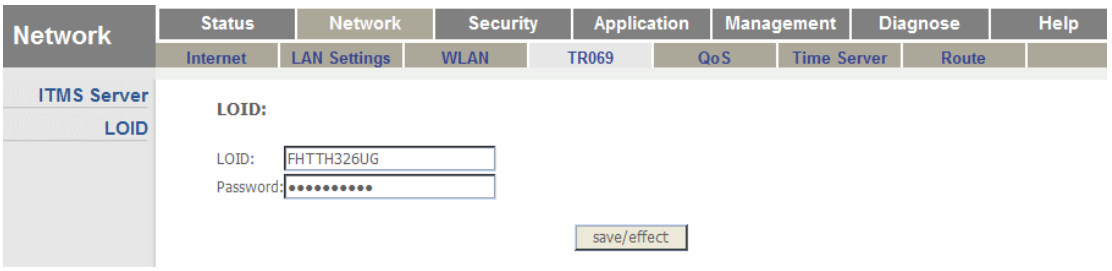

Figure 3-22: LOID settings

3.3.7 QoS

This page shows the QoS settings. Once the data stream is matched to the rule and the rule has bound to a specifical queue, the data stream's rate will be in schedule depending on the queue settings.

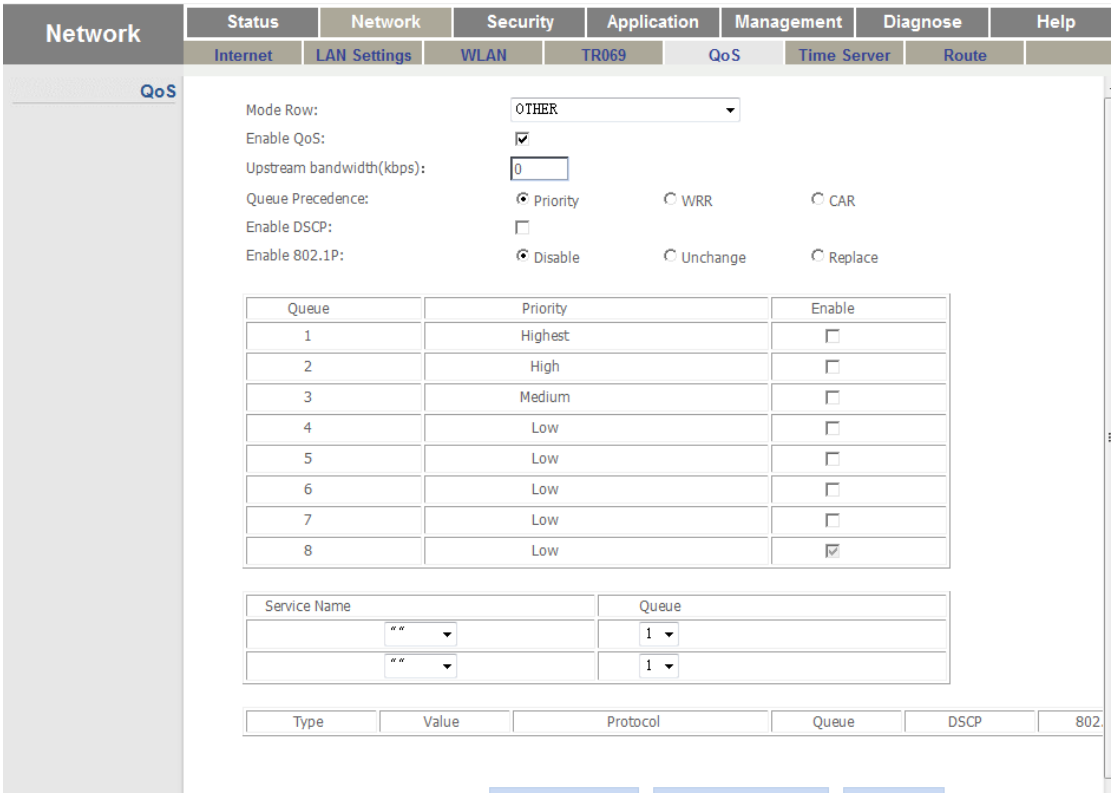

Figure 3-23: QoS Configuration

Parameter	Description
Mode Row	QoS template. There are several templates to choose from.
Enable QoS	Enable QoS
Upstream Bandwidth	Set up upstream bandwidth. 0 means no limit.
Queue Precedence	Set up the scheduling policy.
Enable DSCP	Enable DSCP
Enable 802.1P	Enable 802.1P

3.3.8 Time Server

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 “Save/Apply” button to save.

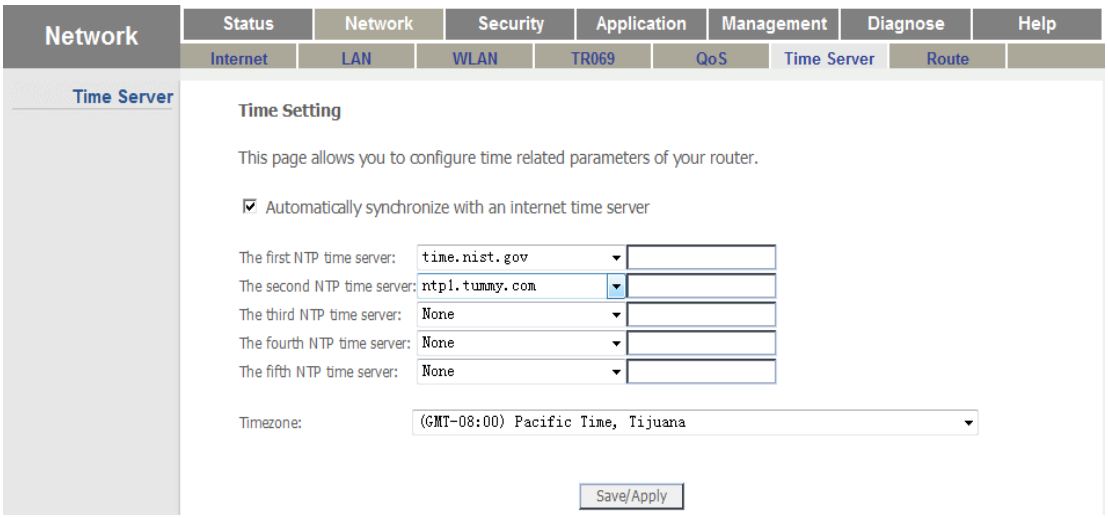

Figure 3-24: Time server

3.3.9 Route

This page allows you to configure static routing.

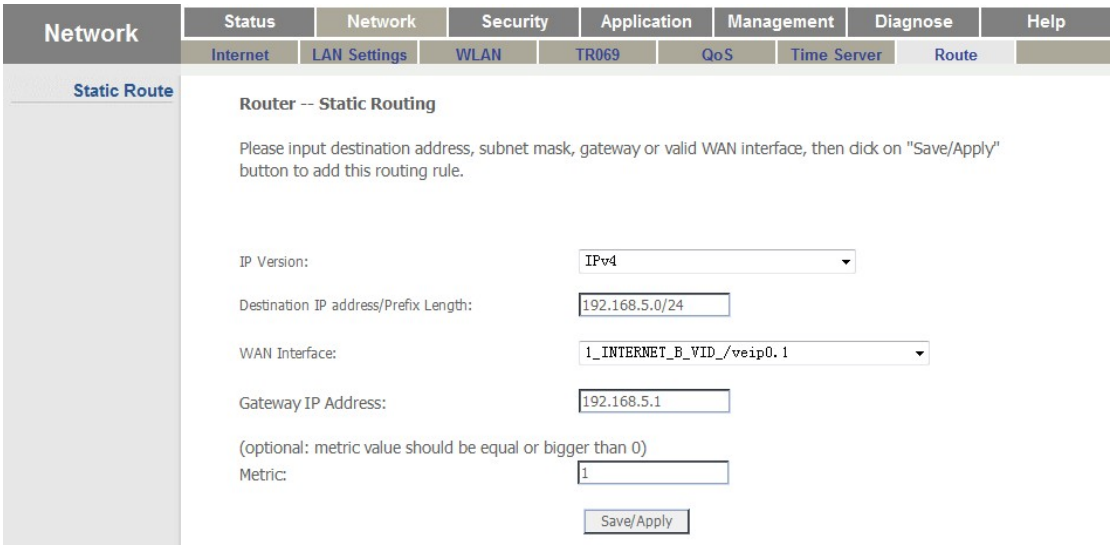

Figure 3-25: Configure Static Route

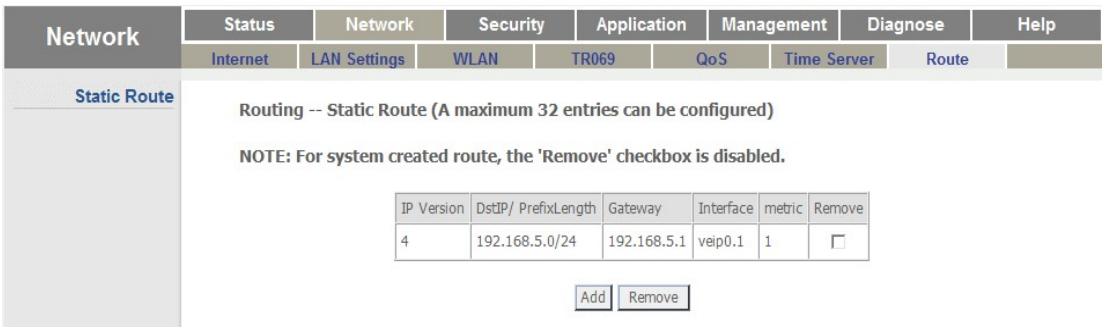

Figure 3-26: Static Route List

Parameter	Description
IP Version	IPv4: Static route for IPv4. IPv6: Static route for IPv6.
Destination IP Address	Destination IP address format: the last several bits should be zero, such as 192.168.5.0/24, 192.168.0.0/16.
WAN Interface	Select the WAN interface you want to add static route.
Gateway IP Address	Please input the gateway IP address.
Metric	Please input the metric value.

3.4 Security

3.4.1 URL Filter

This page allows you to configure the URL filter. The URL filter takes effect when the WAN connection is in router mode. When the WAN connection is in bridge mode, the URL filter cannot take effect.

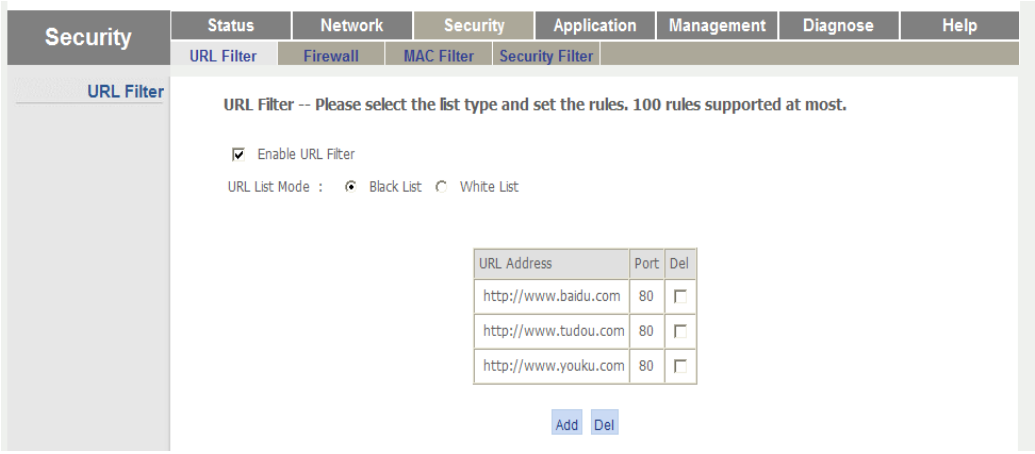

Figure 3-27: URL Filter

Parameter	Description
Enable URL Filter	Enable or Disable URL Filter
URL List Mode	Black List: URLs in the list will be forbidden, all others can be accessed. White List: URLs in the list can be accessed, all others are forbidden.
URL List	URL list you want to deal with (Drop or Access). Click the “Add” button to add a URL item to the list. Select the “Del” checkbox and then click the “Del” button to remove URL items from the list.

3.4.2 Firewall

3.4.2.1 Security Level

This page allows you to configure the firewall level. The firewall has three levels: Low, Medium and High.

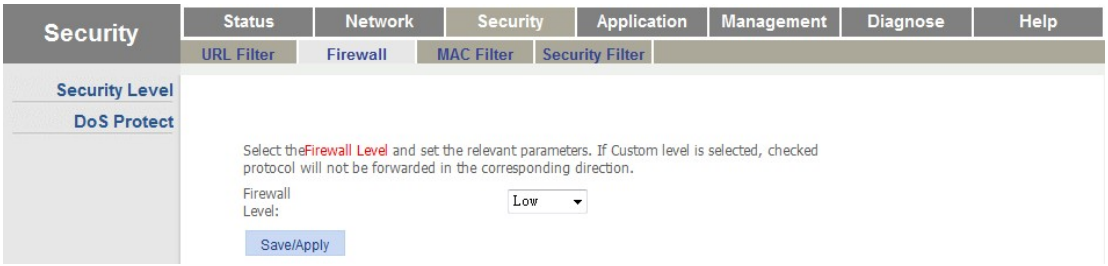

Figure 3-28: Security Level

Parameter	Description
Firewall Level	**Low**: Protects nothing. **Medium**: Denial of Service protections. **High**: Forbid ICMP Input, Forbid Port Scan, and Denial of Service protections.

3.4.2.2 DoS Protection

This page allows you to enable/disable the DoS protection function

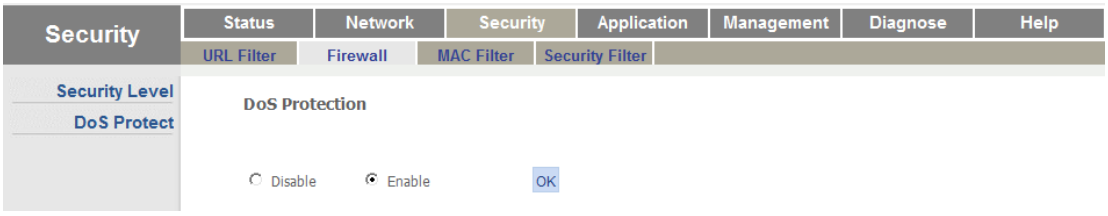

Figure 3-29: DoS Protection

3.4.3 MAC Filter

This page allows you to configure the MAC filter. The MAC filter is different from the URL filter in that it is nothing to do with the WAN connection mode. When packets are input into the LAN port, the packets will be dropped or accessed depending on the MAC filter rules.

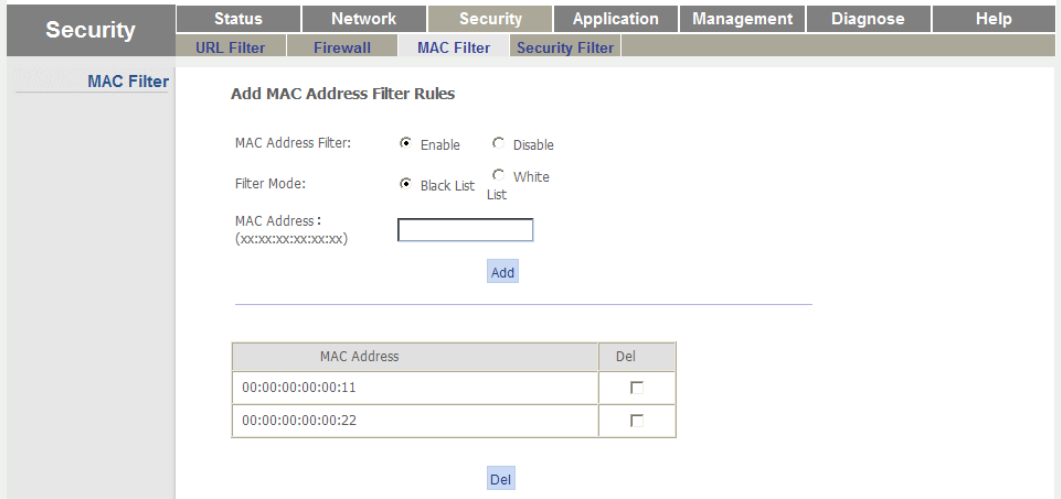

Figure 3-30: MAC Filter

Parameter	Description
MACAddress Filter	Disable: Disable MACFilter Enable: Enable MACFilter
Filter Mode	Black List: MAC Addresses in the list are forbidden, all others can be accessed. White List: MAC Addresses in the list can be accessed, all others are forbidden.
MAC Address	Input the MAC address and click the “Add” button to add a MAC address to the table. Select the “Del” checkbox and then click “Del” button to remove a MAC address from the table.

3.4.4 Port Filter

This page is used to configure port filters. Port filters include many kind of filters such as the MAC filter, IP filter, protocol filter, and port filter.

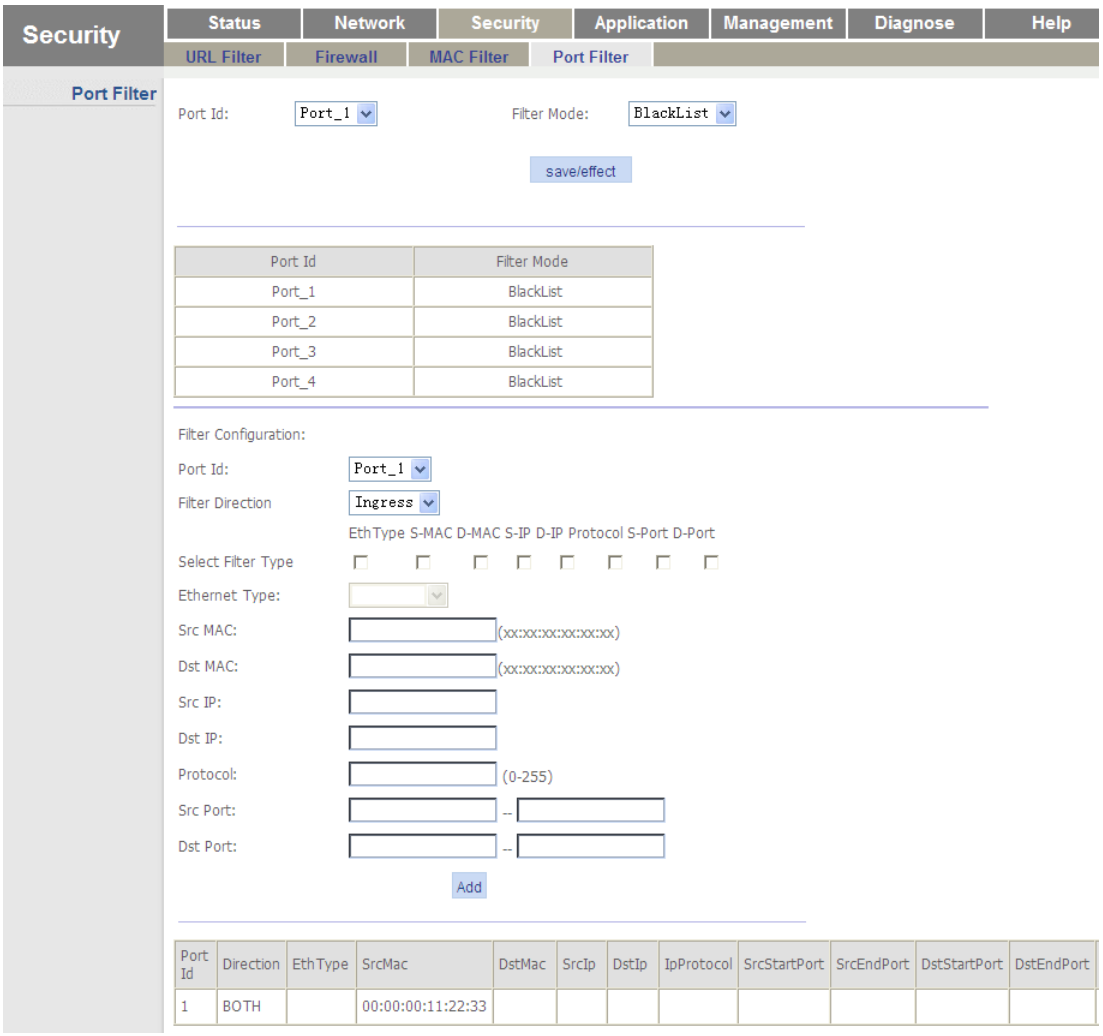

Figure 3-31: Port Filter

Parameter	Description
Filter Global Settings	
Port ID	Select the port you want to configure
Filter Mode	Black List: Items in the list are forbidden, all others can be accessed. White List: Items in the list can be accessed, all others are forbidden.
Filter Rule Settings	
Port ID	Select the port you want to configure rules for.
Filter Direction	Ingress: Packet ingress for the port will be filtered by the rule. Egress: Packet egress for the port will be filtered by the rule. BOTH: Packets of both directions will be filtered by the rule.
Select Filter Type	Select the items you want to configure a rule for.
Ethernet Type	Select which Ethernet type you want to configure in the rule.
Src MAC	Input the source MAC address you want to configure in the rule.
Dst MAC	Input the destination MAC address you want to configure in the rule.

Src IP	Input the source IP address you want to configure in the rule.
Dst IP	Input the destination IP address you want to configure in the rule.
Protocol	Input the protocol you want to configure in the rule.
Src Port	Input the source port you want to configure in the rule.
Dst Port	Input the destination port you want to configure in the rule.

Notice: When port filter mode changes to white list, you should configure two rules: One rule for ingress direction and one rule for egress direction.

Eg: Port_1 filter mode has changed into white list.

Port Id	Filter Mode
Port_1	WhiteList
Port_2	WhiteList
Port_3	BlackList
Port_4	BlackList

Here two rules have been configured (one for ingress and one for egress). The MAC address is the computer's MAC address. In this way, the computer can access the equipment via port 1.

Port Id	Direction	EthType	SrcMac	DstMac	SrcIp
1	Ingress		00:30:18:ae:ef:35		
1	Egress			00:30:18:ae:ef:35	

3.5 Application

3.5.1 NAT

3.5.1.1 ALG

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

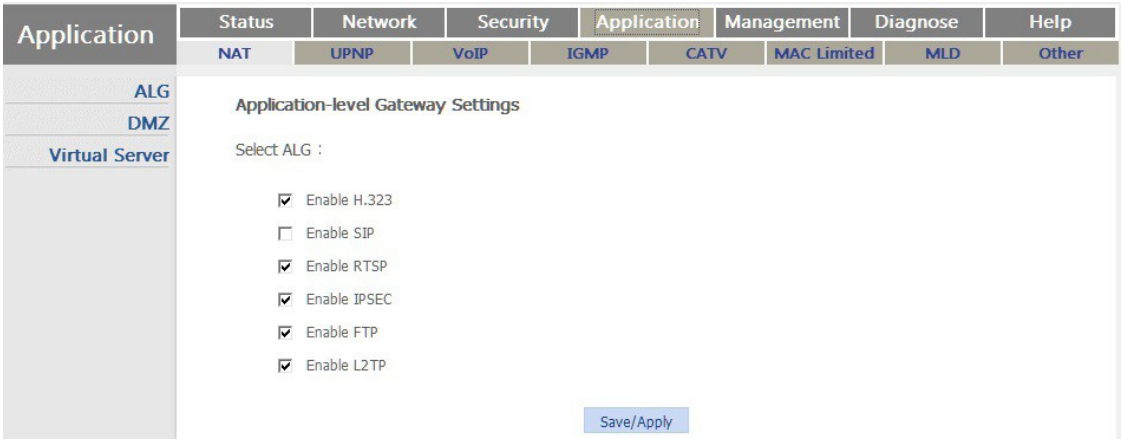

Figure 3-32: ALG

3.5.1.2 DMZ

This page allows you to configure the DMZ server.

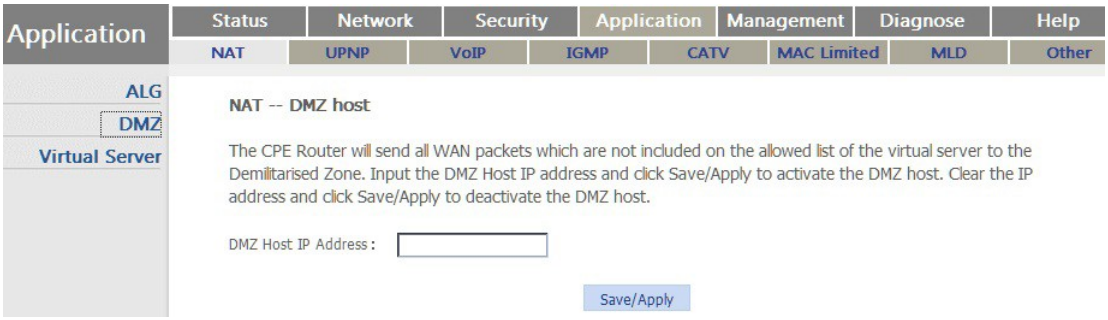

Figure 3-33: DMZ

3.5.1.3 Virtual Server

This page allows you to configure a 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 shown in Figure 3-32.

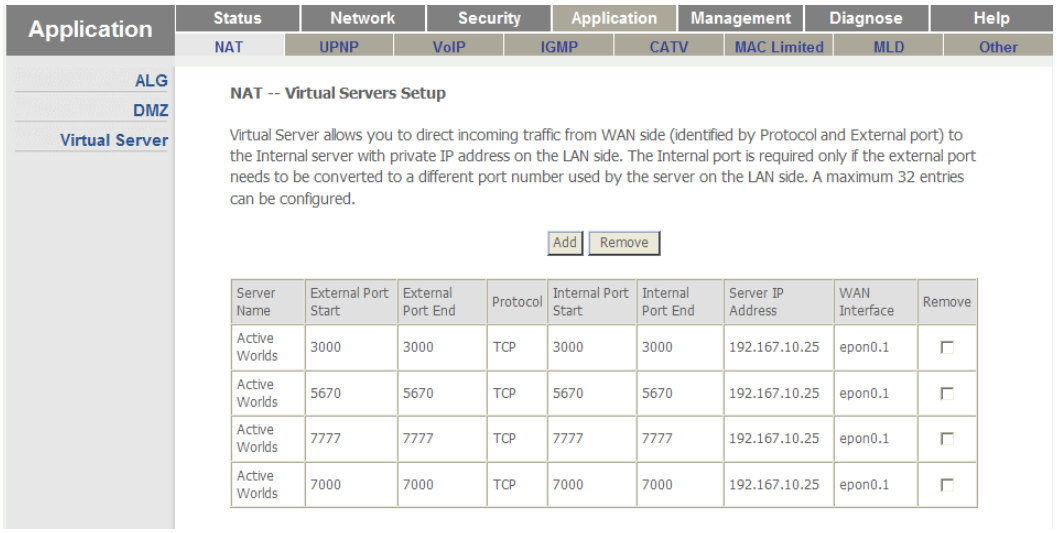

Figure 3-34: Virtual Server

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

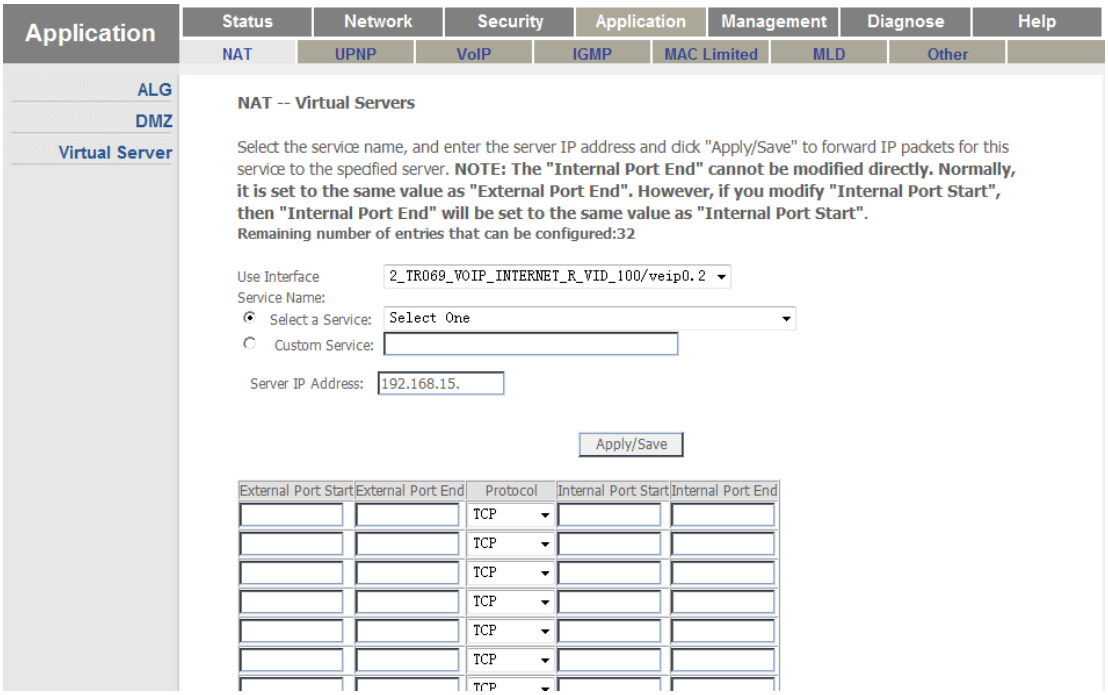

Figure 3-35: Virtual Server

Parameter	Description
Use Interface	Select a WAN connection with NAT function enabled.
Service Name	Select a service you want to add to the virtual server.
Server IP Address	Input an internal server IP address.

3.5.2 UPNP

This page is used to enable UPNP.

Figure 3-36: UPNP Settings

3.5.3 VoIP

3.5.3.1 General Settings

This page allows you to configure VoIP general settings.

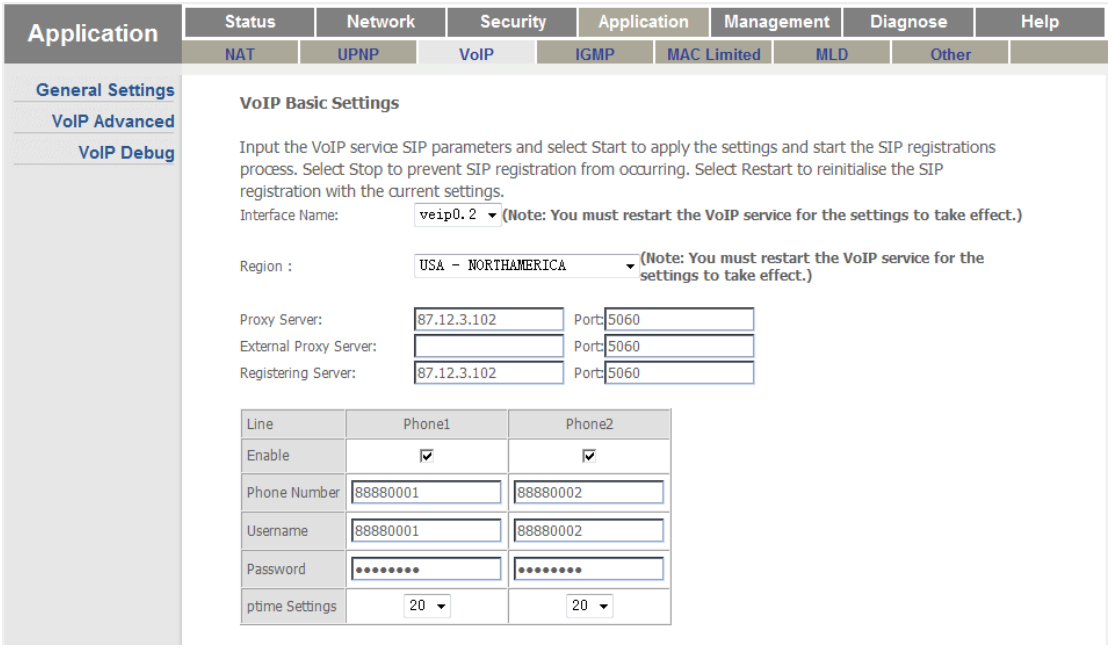

Figure 3-37: VoIP General Setting

Parameter	Description
Interface Name	Select a WAN connection that includes VoIP service.
Region	Select the region.
Proxy Server	Enter the IP address or domain name of the SIP proxy server.
External Proxy Server	Enter external proxy server address. If the main proxy server is down, the equipment will send the signal to an external proxy server.
Registering Server	Enter the IP address or domain name of the SIP server address.

Port	Enter the signal port of the server. The range is 1 to 65535. The default port is 5060.
Enable	Enable: Enable phone 1 or phone 2 VoIP function. Disable: Disable phone 1 or phone 2 VoIP function.
Phone Number	Enter the display name as it should appear on caller ID.
Username	Enter the registration ID of the user with the registrar.
Password	Enter the password used for authentication with the registrar.
ptime Settings	Select the packing time you want to set.

This page shows the VoIP WAN connection. Service mode must contain VoIP.

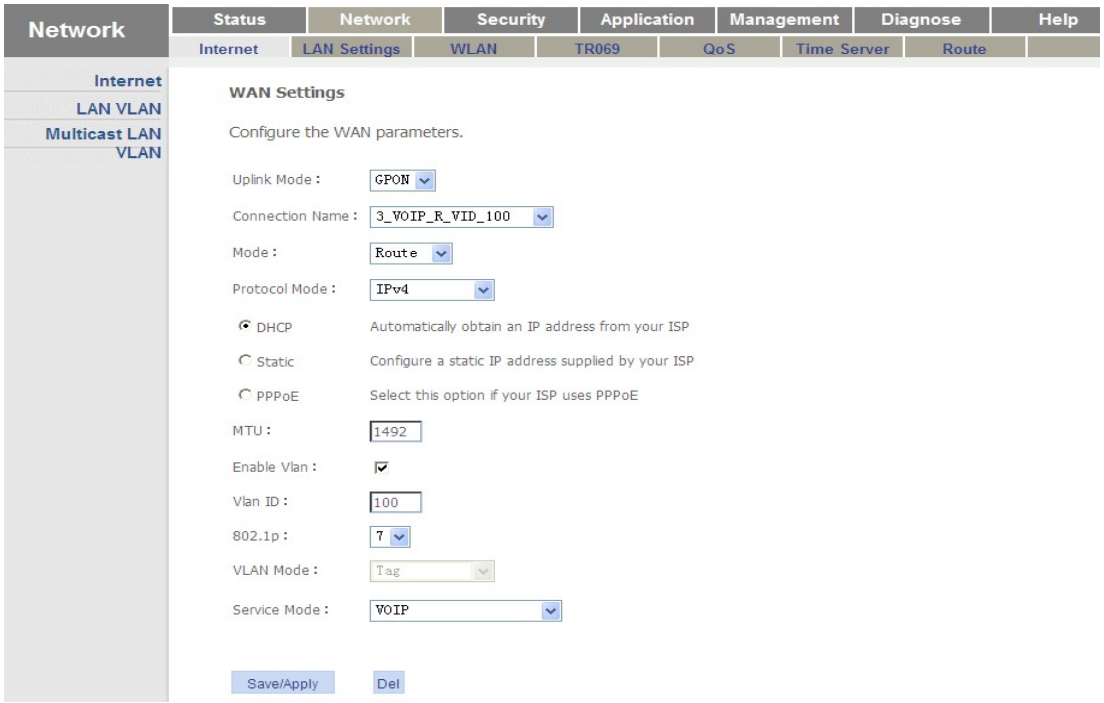

Figure 3-38: VoIP WAN Connection Setting

3.5.3.2 VoIP Advanced

This page shows advanced VoIP settings.

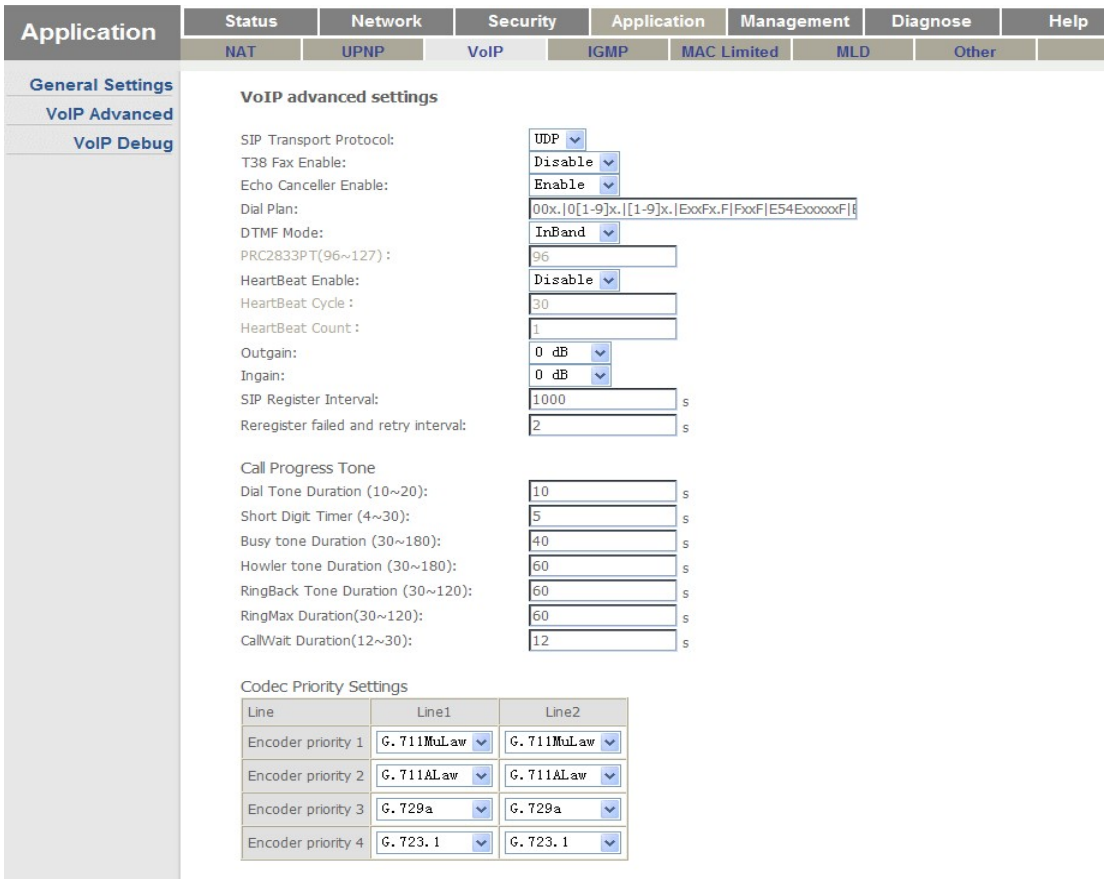

Figure 3-39: VoIP Advanced Settings (1)

Parameter	**Description**
SIP Transport Protocol	Select the SIP transport protocol: UDP or TCP.
Enable T38 Fax	Enable T38 mode.
Enable Echo Canceller	Enable echo canceller.
Dial Plan	Default is: 00x.|0[1-9]x.|[1-9]x.|ExxFx.F|FxxF|E54ExxxxxF|ExxExxsxxxxxsx .F|ExxExxExxxxxxxxF|FxxF|EExx|FxxExxF|ExxF|EExxExxxxEx xxxxxxxF|FExxExxxxExxxxxxxxF|FF|ExxExxxxF|FExx|ExxEx.F| ExxEx.Ex.F|E98x.|E5s.|F54ExxxxxF
DTMF Mode	DTMF type: Refers to the transfer mode of users pressing buttons while a voice call is active. It can be set as 3 modes: In-Band, RFC2833, and INFO message. If the mode is set as In-band transport, the signal from pressing buttons will be transferred along with the voice signal. If the mode is set as INFO message, the signal from pressing buttons will be transferred in the signaling. Note that the INFO message mode only supports nonfast-connections.
Outgain	Select outgain value.
Ingain	Select ingain value.
SIP Register Interval	Set the SIP register internal value, default value is 1000.
Register Interval	Set the register internal value, default value is 2.
Dial Tone Duration	Set the off-hook dialing expire time, default value is 10 (range: 10 s to 20 s).

Short Digit Timer	Set the short digit timer value, default value is 5 (range: 4 s to 30 s).
Busy Tone Duration	Set the busy tone duration, default value is 40 (range: 30 s to 180 s).
Howler Tone Duration	Set the howler tone duration, default value is 60 (range: 30 s to 180 s).
Ring Back Tone Duration	Set the ring back tone duration, default value is 60 (range: 30 s to 120 s).
Ring Max Duration	Set the ringing duration, default value is 60 (range: 30 s to 120 s).
Call Wait Duration	Set the call wait duration, default value is 12 (range: 12 s to 30 s).
Codec Priority Settings	This parameter sets the ITU-T coding standard of voice calls. The coding technology supported by this equipment is G.711 A law, G.711 Mu law, G.723.1, G.729, and so on. Users can choose one of several coding modes, but one of those modes must be chosen as the priority.

Call Addition Functions

Line	Line1	Line2
Call Wait	☐	☐
Call Conference	☐	☐
Warm Line	☐	☐
Warm Line Timeout	0	0
Warm Line Number		
CfwdUncond	☐	☐
CfwdUncond Number		
CfwdBusy	☐	☐
CfwdBusy Number		
CfwdNoAns	☐	☐
CfwdNoAns Timeout	30	30
CfwdNoAns Number		
Call Transfer	☑	☑
Unattended(E/F/0~9)	E77	E77
Attended(E/F/0~9)	E78	E78

RTP Transfer Setting

Line	Line1	Line2
Audio port	4000	4010
T.38 port	5000	5010

Figure 3-40: VoIP Advanced Settings (2)

Parameter	Description
Call Addition Functions	Set call wait, call conference, warm line, and several call forward modes.
RTP Transfer Setting	Set audio port and T38 port for the two lines.

3.5.4 IGMP

3.5.4.1 IGMP SNOOPING

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

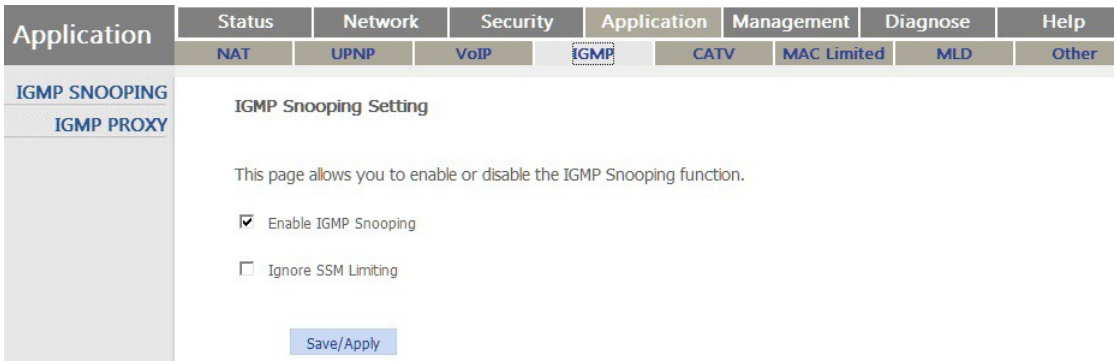

Figure 3-41: IGMP Snooping Setting

3.5.4.2 IGMP PROXY

This page allows you to enable IGMP proxies for a specified WAN connection.

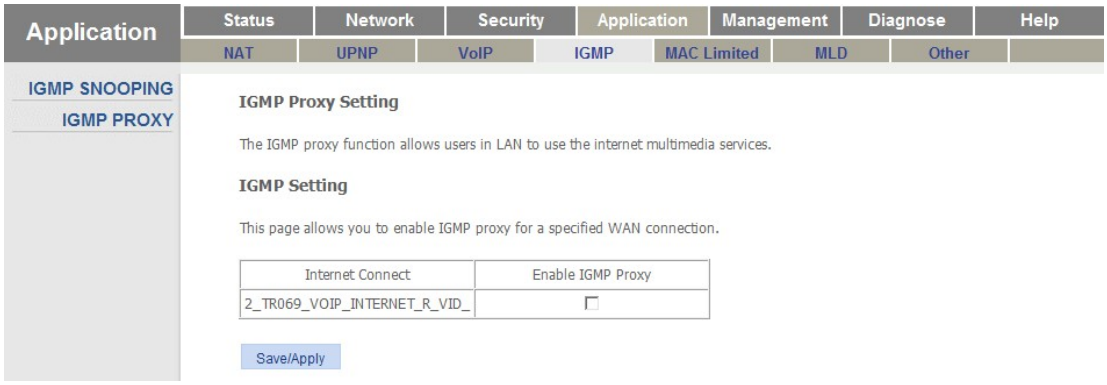

Figure 3-42: IGMP PROXY Setting

3.5.5 CATV

This page allows you to enable IGMP proxies for a specified WAN connection.

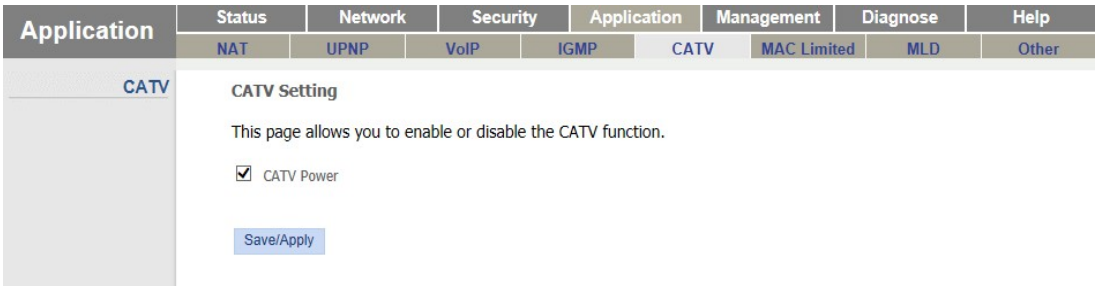

Figure 3-43: CATV Setting

3.5.6 MAC Limited

This page allows you to configure MAC aging time as well as the MAC address limited.

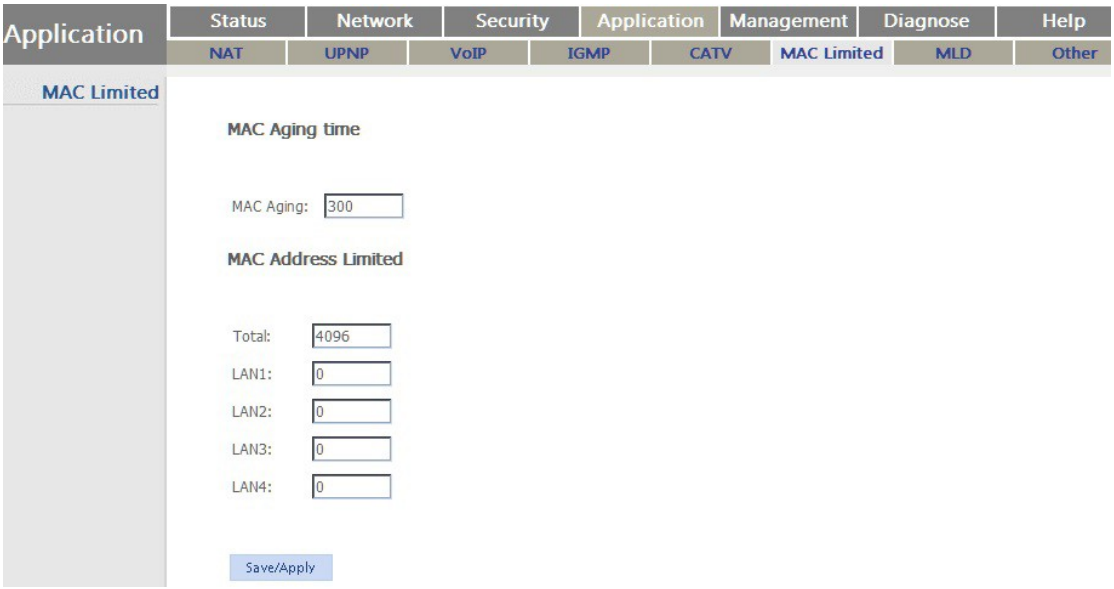

Figure 3-44: MAC Limited Setting

3.5.7 MLD

3.5.7.1 MLD SNOOPING

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

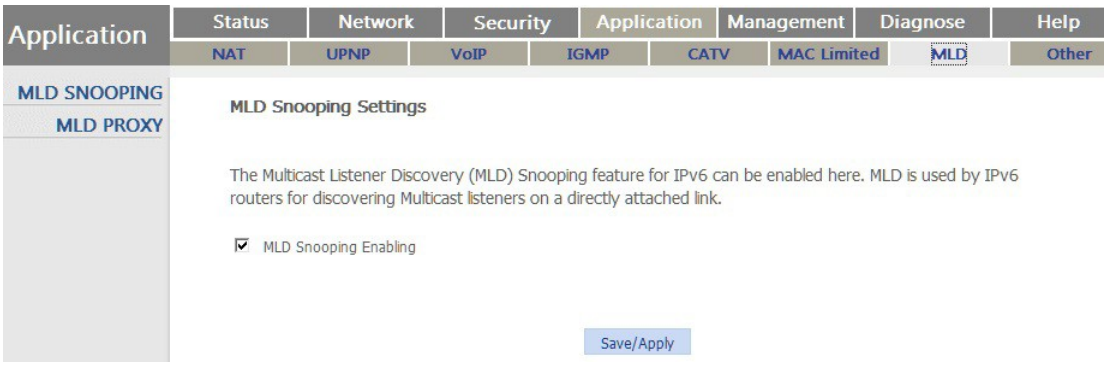

Figure 3-45: MLD SNOOPING Setting

3.5.7.2 MLD PROXY

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

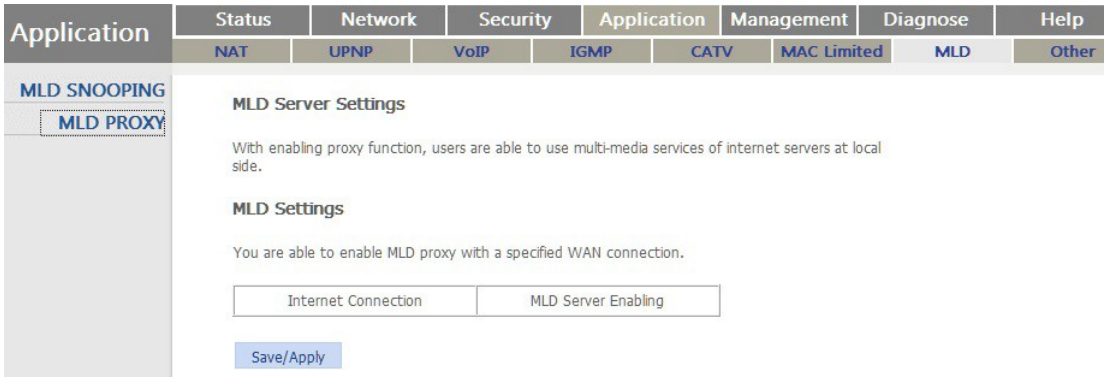

Figure 3-46: MLD PROXY Setting

3.5.8 Other

3.5.8.1 Family Storage

This page allows you to build a FTP server.

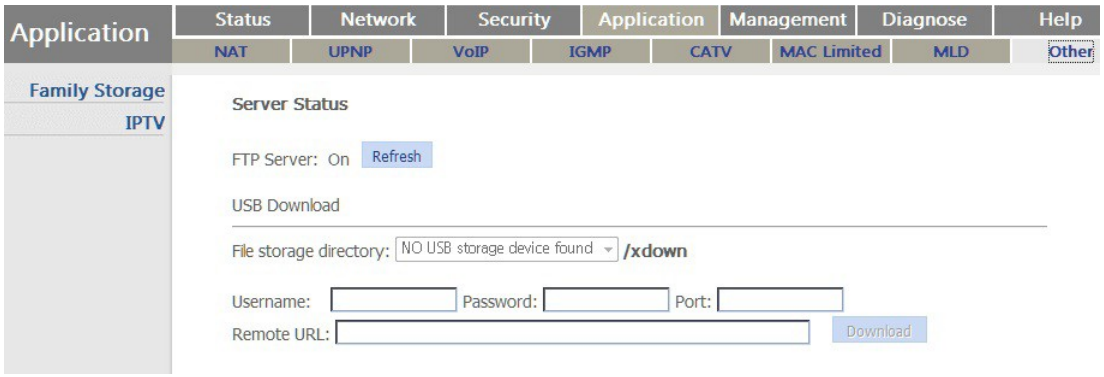

Figure 3-47: Family Storage

3.5.8.2 IPTV

This page allows you to configure IPTV settings for route mode WAN connections.

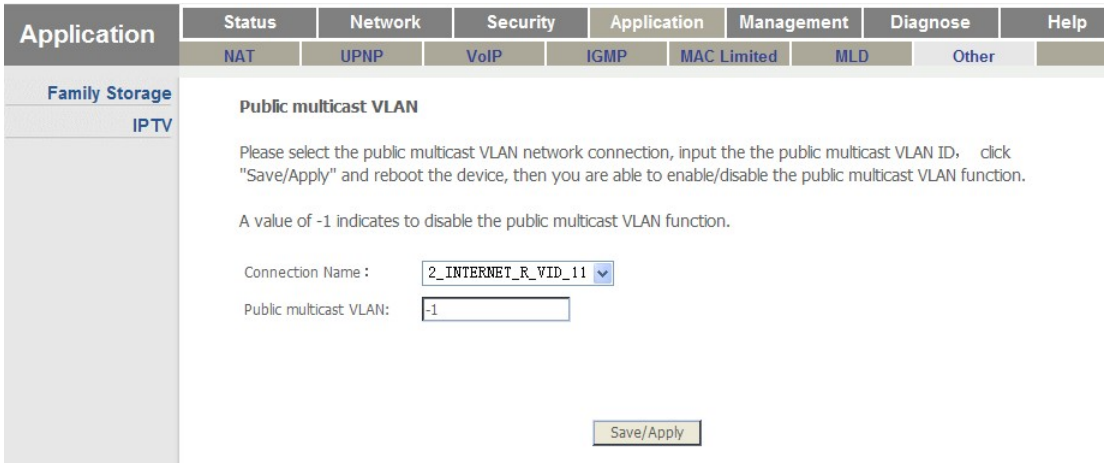

Figure 3-48: IPTV Setting

3.6 Management

3.6.1 User Manage

This page allows you to change username or password. There are two levels for accounts: admin and user.

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

The user account can only be used to view configurations, statuses, and configure limited parameters such as enable wireless, modify SSID name, configure filter, firewall, reboot HGU, etc.

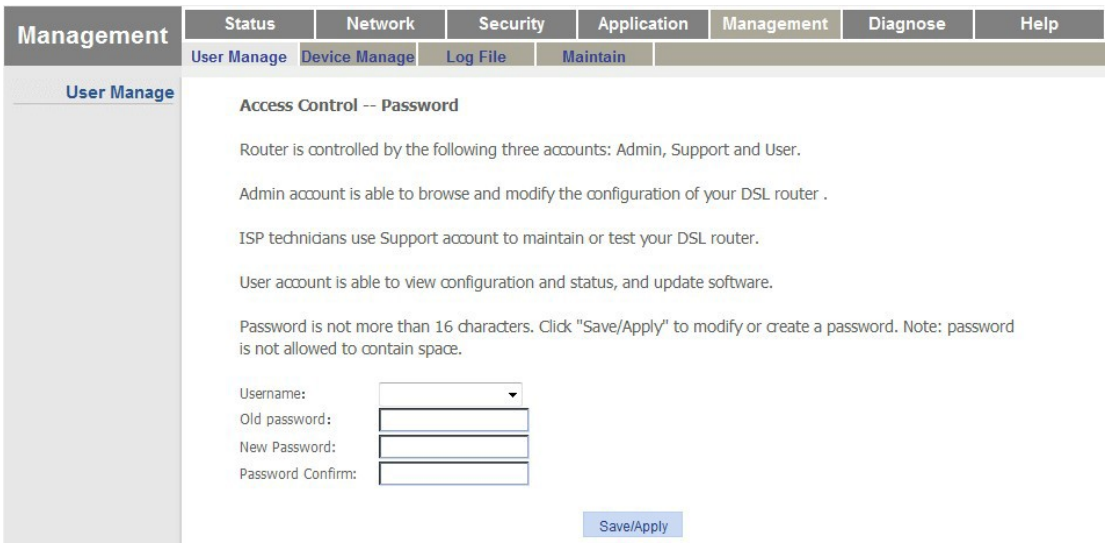

Figure 3-49: User manage

3.6.2 Device Manage

3.6.2.1 Device Reboot

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

Figure 3-50: Device reboot

3.6.2.2 Update Image

This page allows you to update the software of the device. You can click the “browse” button to select the software you want to update and then click the “Update Software” button to update the image.

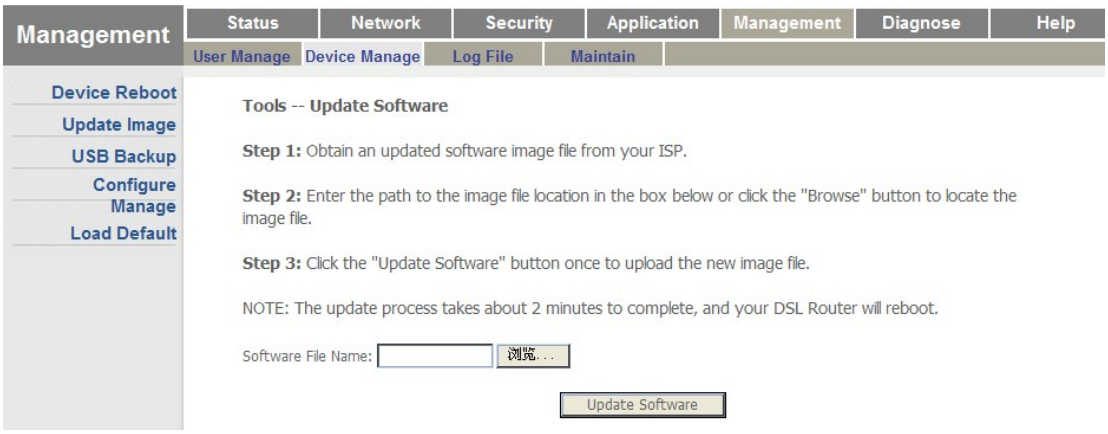

Figure 3-51: Update image

3.6.2.3 USB Backup

This page allows you to back up a configuration file to USB storage.

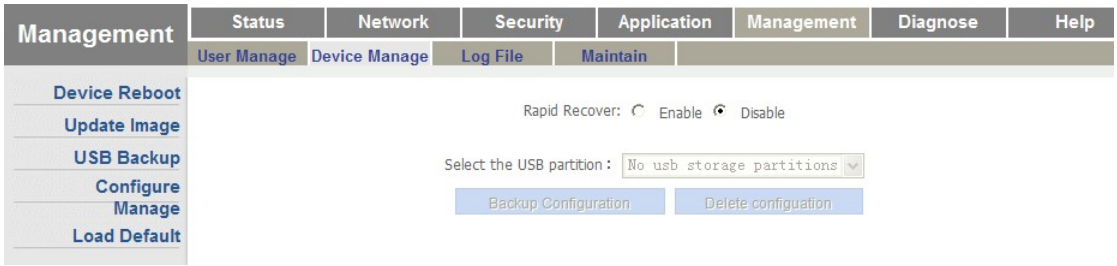

Figure 3-52: USB backup

3.6.2.4 Configure Manage

This page allows you to back up and restore the configuration settings of a router.

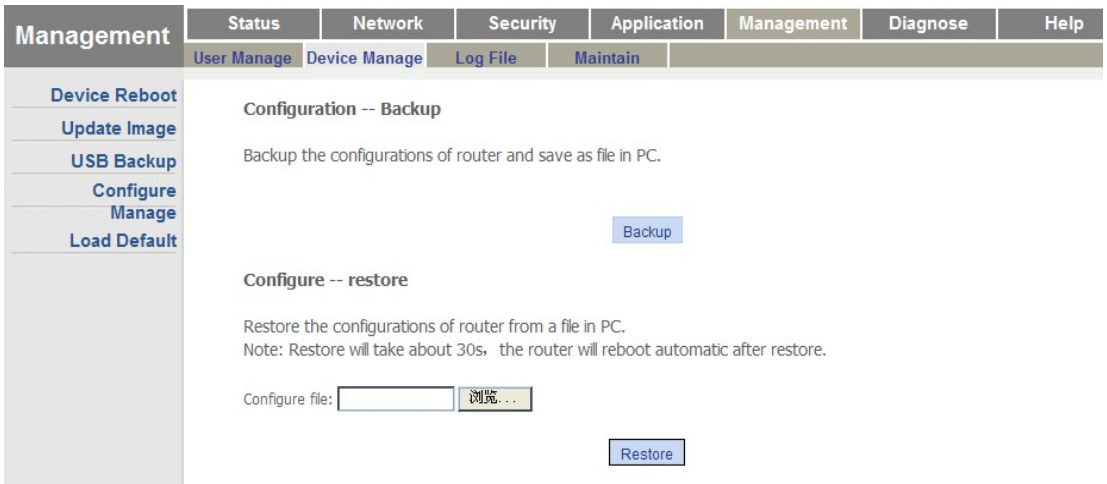

Figure 3-53: Configure manage

3.6.2.5 Load Default

This page allows you to restore the device to default settings. You can click the “Load Default” button to restore the factory settings of the device. After being restored, it will restart automatically.

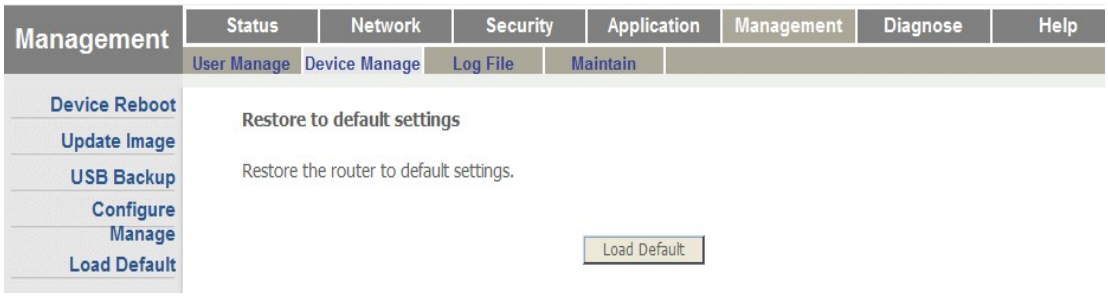

Figure 3-54: Load default

3.6.3 Log File

3.6.3.1 Log

This page allows you to set up log level, display level, etc.

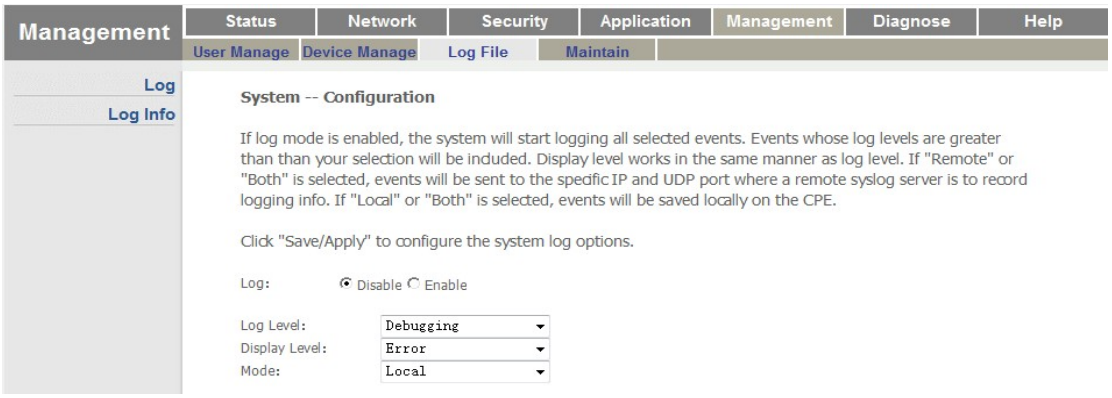

Figure 3-55: Log settings

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

3.6.3.2 Log Info

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

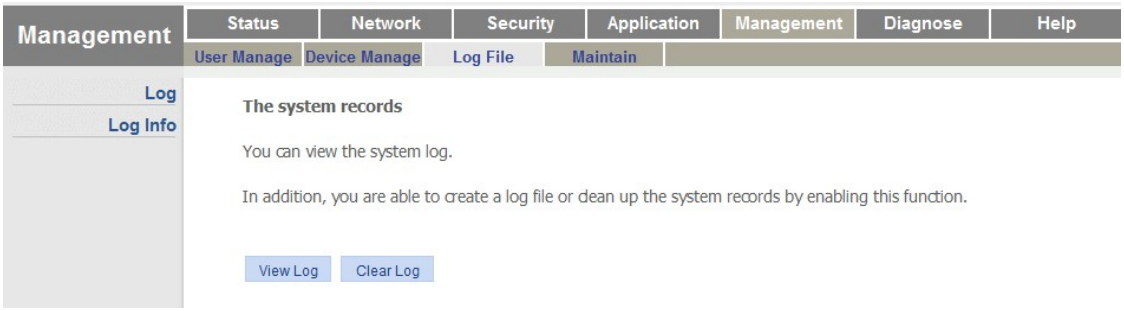

Figure 3-56: Log Info

3.6.4 Maintain

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

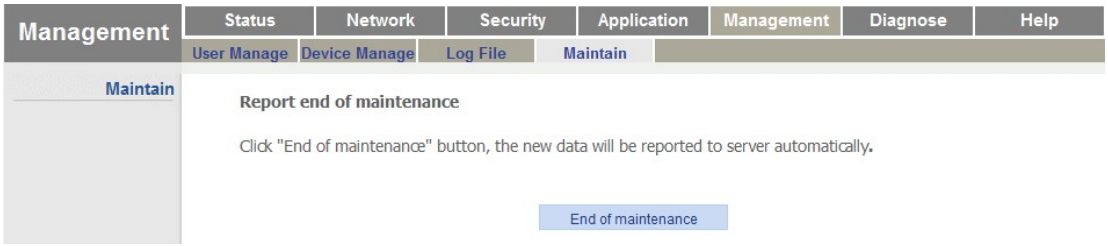

Figure 3-57: Maintain

3.7 Diagnose

3.7.1 Line Diagnose

This page shows information about the line diagnosis. You can click the “Re-diagnose” button to refresh the status.

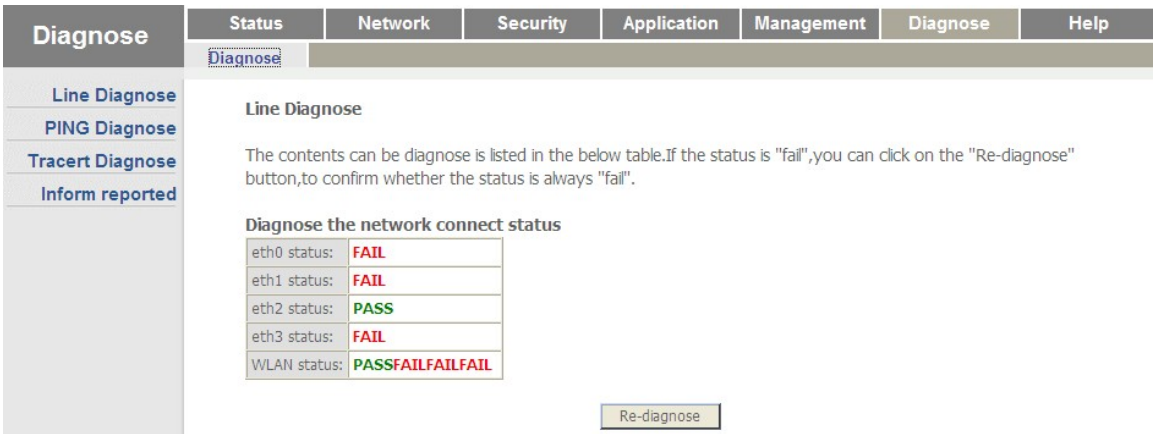

Figure 3-58: Line diagnose

3.7.2 PING Diagnose

This page shows information about the ping test. You can diagnose the connection status between the HGU and other devices.

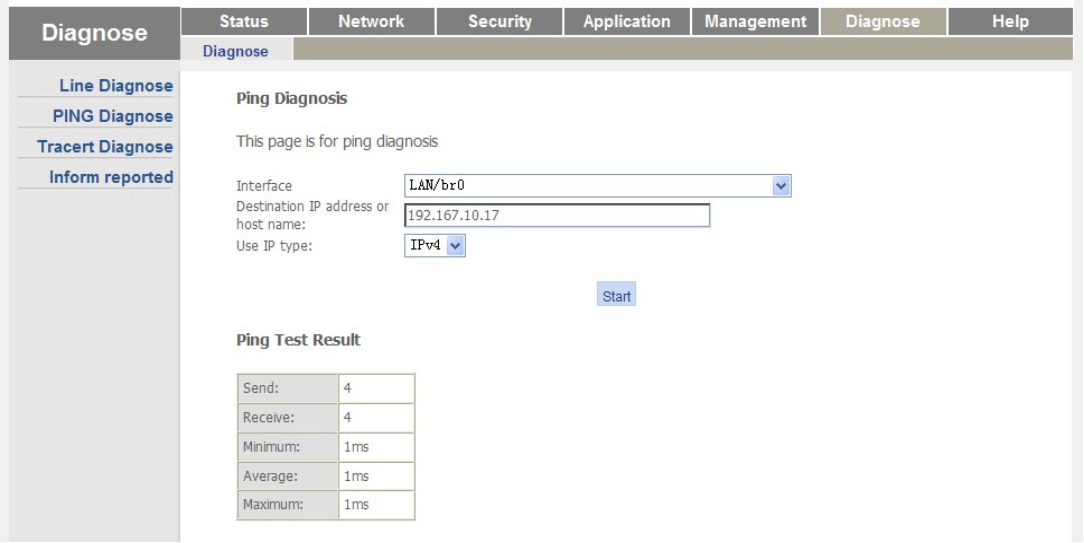

Figure 3-59: PING diagnose

Parameters	**Description**
Interface	Select the interface you want to test.
Destination IP or Host Name	Input the destination IP you want to ping.
Use IP type	IPv4: Use IPv4 protocol. IPv6: Use IPv6 protocol.

3.7.3 Tracert Diagnosis

This page shows information about the tracert diagnosis.

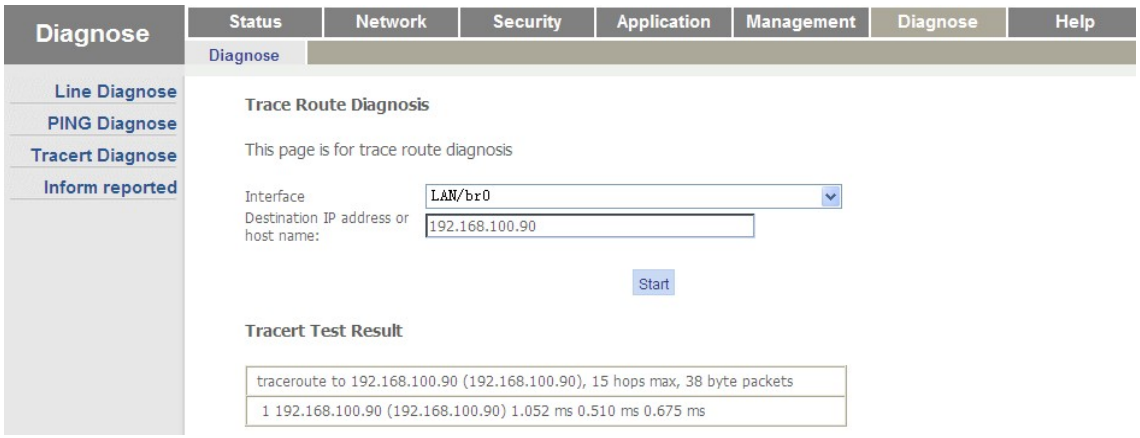

Figure 3-60: Tracert diagnosis

Note Do not start a trace route test when the trace route is in running status.

3.7.4 Inform reported

This page shows information about the manual send inform test.

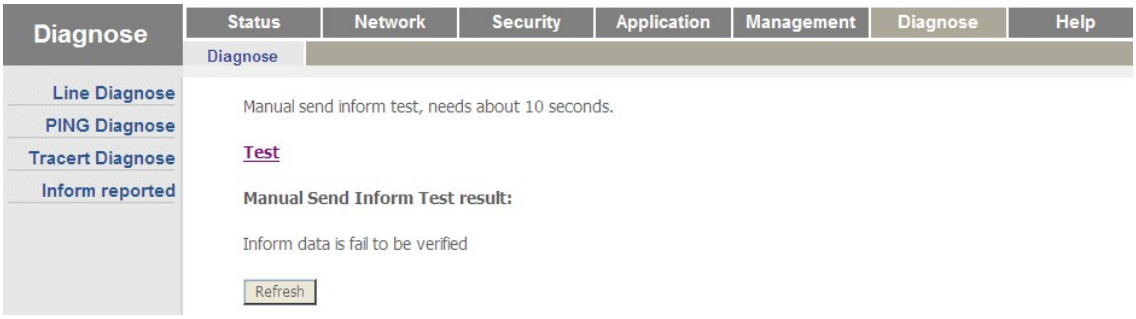

Figure 3-61: Inform reported

3.8 Help

The Help tab displays information for HGU display instructions and prompts in each web UI.

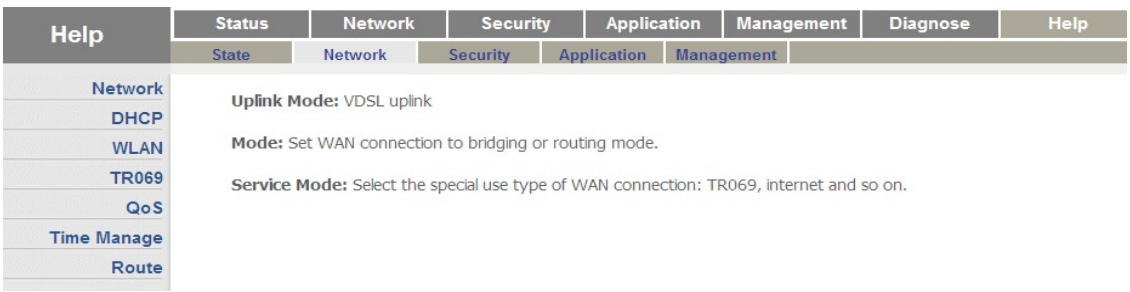

Figure 3-62: Help information

Chapter 4. Examples

4.1 Internet Service

There are two configuration methods for internet service: bridge mode and route mode.

4.1.1 Requirements

1. HGU works on bridge mode, service VLAN is 9. Users access the Internet via LAN port 1.
2. HGU works on route mode, service VLAN is 10. HGU receives IP address via DHCP.

4.1.2 Steps

Before configuring, make sure the HGU has been successfully registered and authorized. Connect PC to one of the HGU's LAN ports with a twisted cable.

4.1.2.1 Bridge Mode for Internet Service

3. Add a WAN connection

Choose "Network > Internet > Internet" in the navigation menu. Add a bridge mode WAN connection with the following parameters:

- Mode is bridge.
- Enable VLAN and VLAN mode is transparent.
- Service mode is OTHER.
- Bind port 1.
- Keep other parameters default.

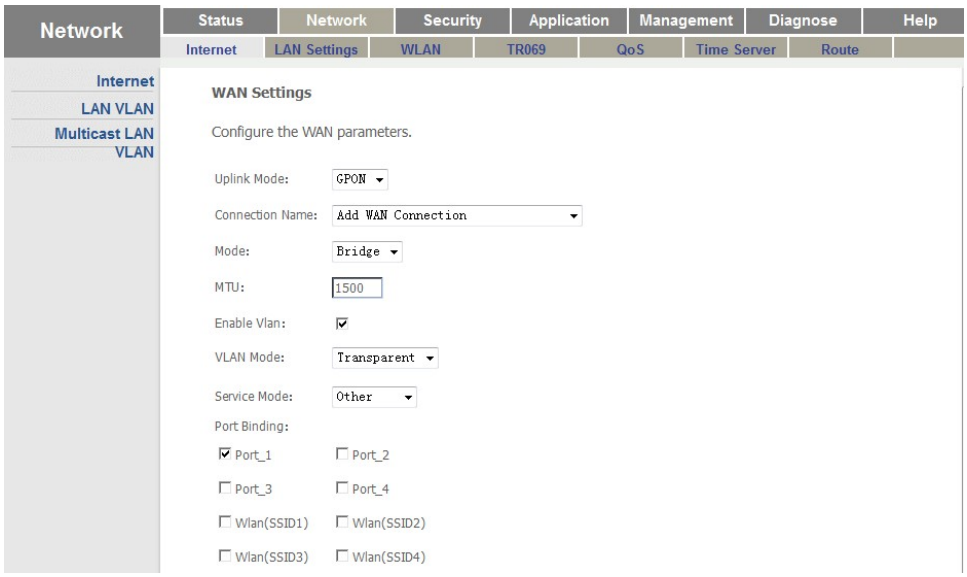

Figure 4-1: Add a bridge WAN connection

1. Configure LAN port

Choose “Network > Internet > LAN VLAN” in the navigation menu. Enable VLAN mode of LAN1, received VLAN is 0 and translation VLAN is 9.

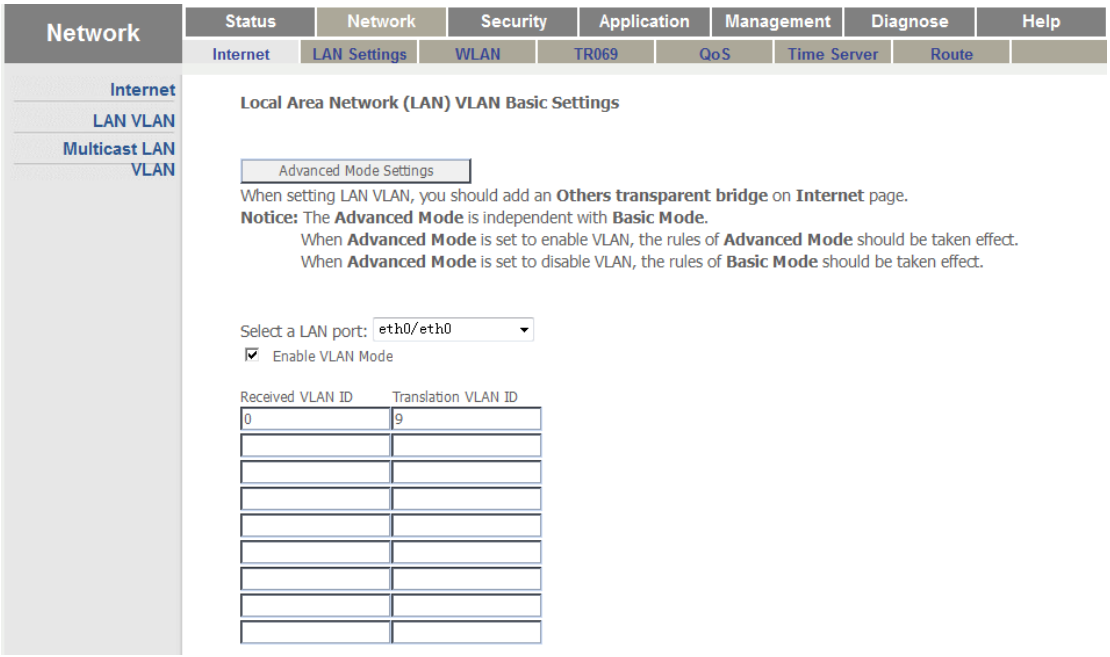

Figure 4-2: LAN VLAN settings

2. Access the internet

Connect PC to LAN 1 port. After receiving an IP address from a DHCP server in the network, the PC can access the Internet.

4.1.2.2 Route Mode for Internet Service

1. Add a WAN connection

Choose “Network > Internet > Internet” in the navigation menu. Add a route mode WAN connection using the following parameters:

- Protocol mode is IPv4.
- Choose DHCP.
- NAT function is checked.
- Enable VLAN with VLAN ID as 10.
- Service mode is INTERNET.
- Bind port 1.
- Keep other parameters default.

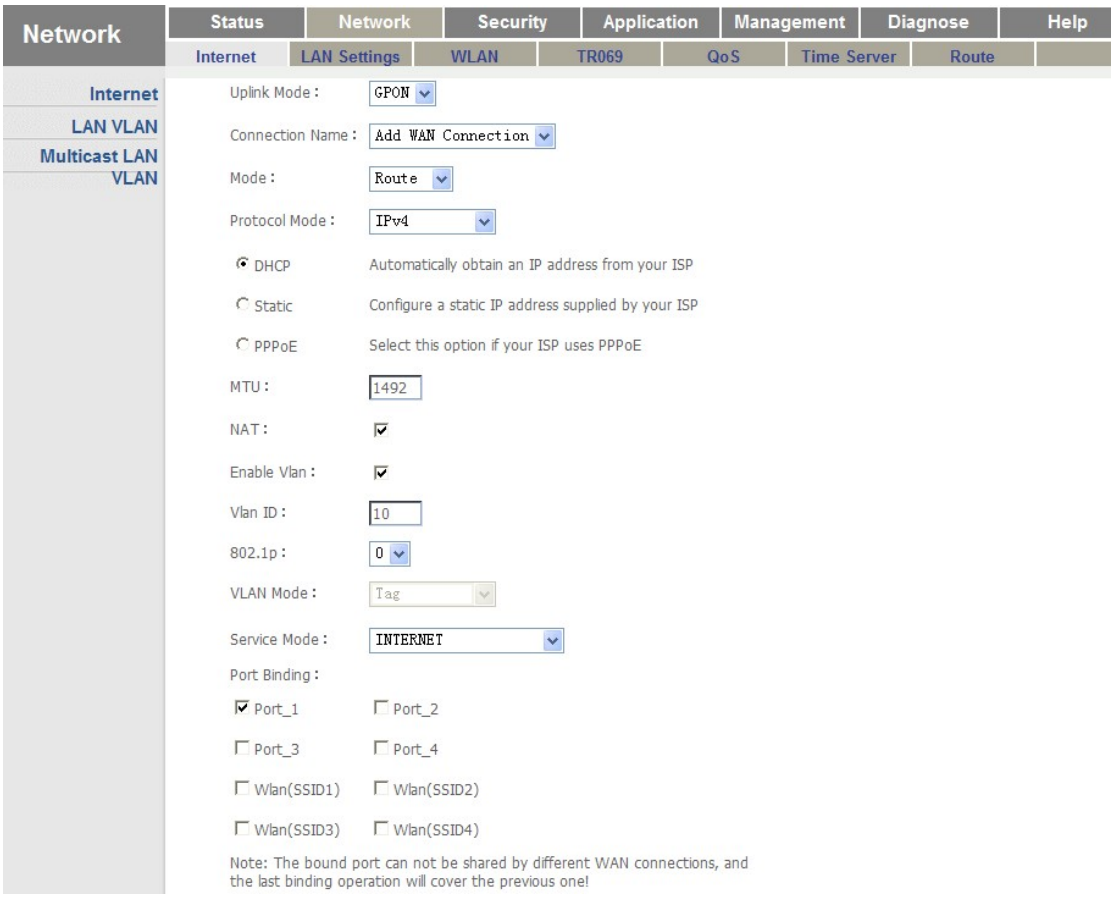

Figure 4-3: Add a route WAN connection

2. Configure LAN port

You should disable the VLAN mode of port 1.

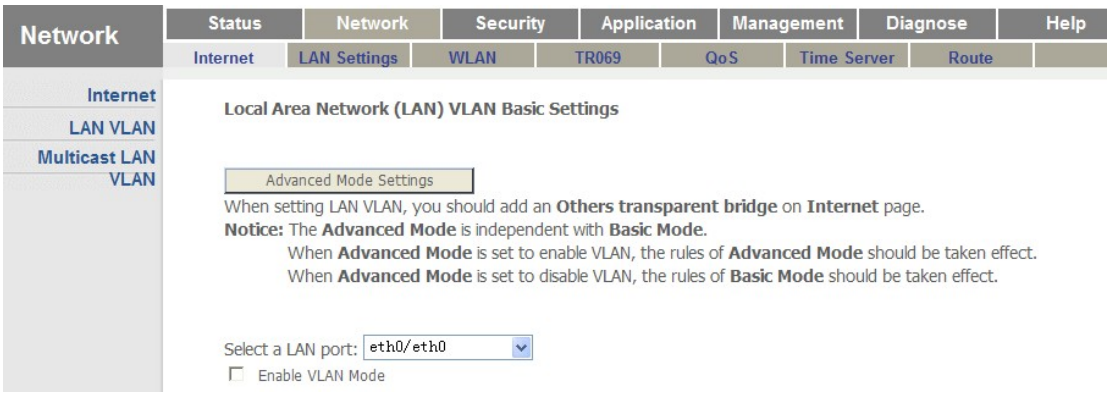

Figure 4-4: LAN VLAN settings

3. Access the Internet

Connect PC to LAN port 1. The PC receives an IP address from the HGU and the HGU receives an IP address from a DHCP server in the network. The PC can then access the internet.

Note

Usually, VLAN mode for bridge WAN connections is transparent.

4.2 IPTV Service

There are two methods for IPTV service, IGMP snooping and IGMP proxy. You must enable IGMP proxy when the HGU is working in route mode.

4.2.1 Requirements

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

4.2.2 Steps

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

Connect PC to one of the HGU's LAN ports with a twisted cable.

4.2.2.1 Bridge mode for IGMP

1. Add a WAN connection

Choose "Network > Internet > Internet" in the navigation menu. Add a bridge mode WAN connection using the following parameters:

- Enable VLAN with VLAN mode as transparent.
- Service mode is OTHER.
- Bind port 2.
- Keep other parameters default.

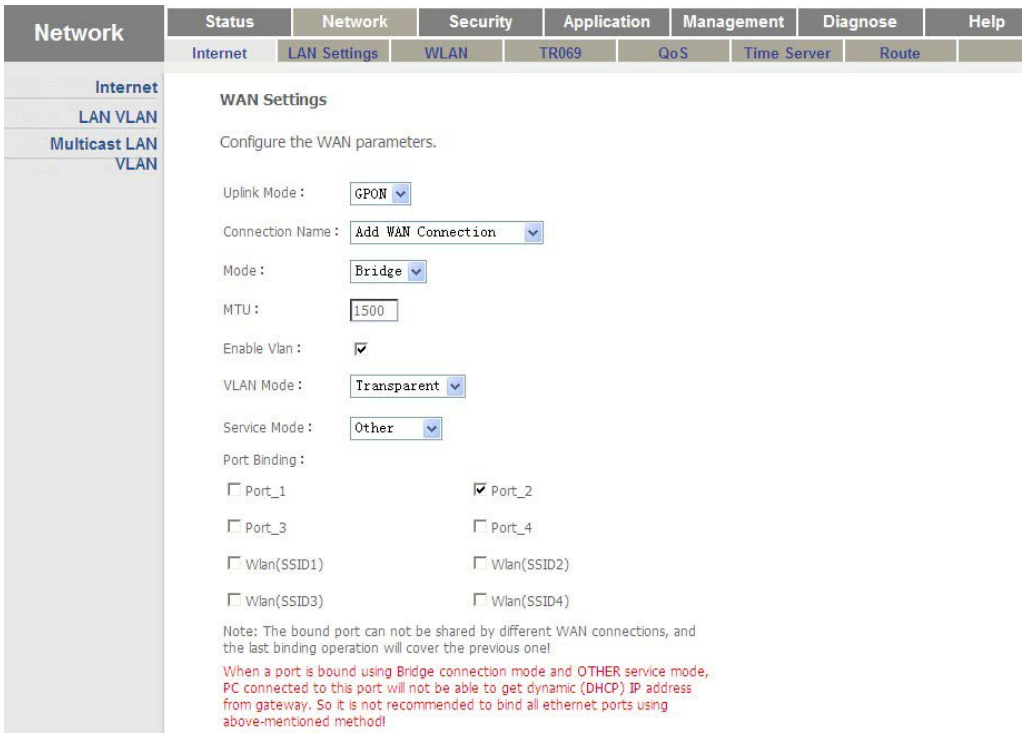

Figure 4-5: Add a bridge WAN connection

2. Configure LAN port

Choose “Network > Internet > LAN VLAN” in the navigation menu. Enable VLAN mode of port 2. Received VLAN ID is 0 and translation VLAN ID is 0.

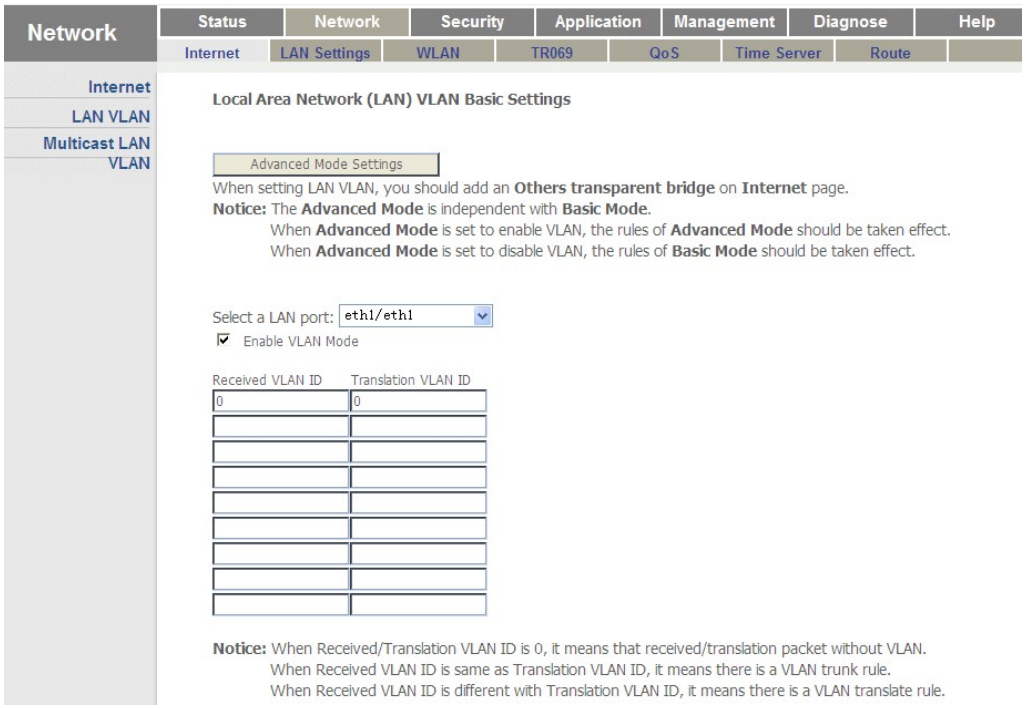

Figure 4-6: Enable LAN VLAN

Choose “Network > Internet > Multicast LAN VLAN” in the navigation menu. Enable VLAN mode of LAN 2. Received VLAN is 0 and translation VLAN is 20.

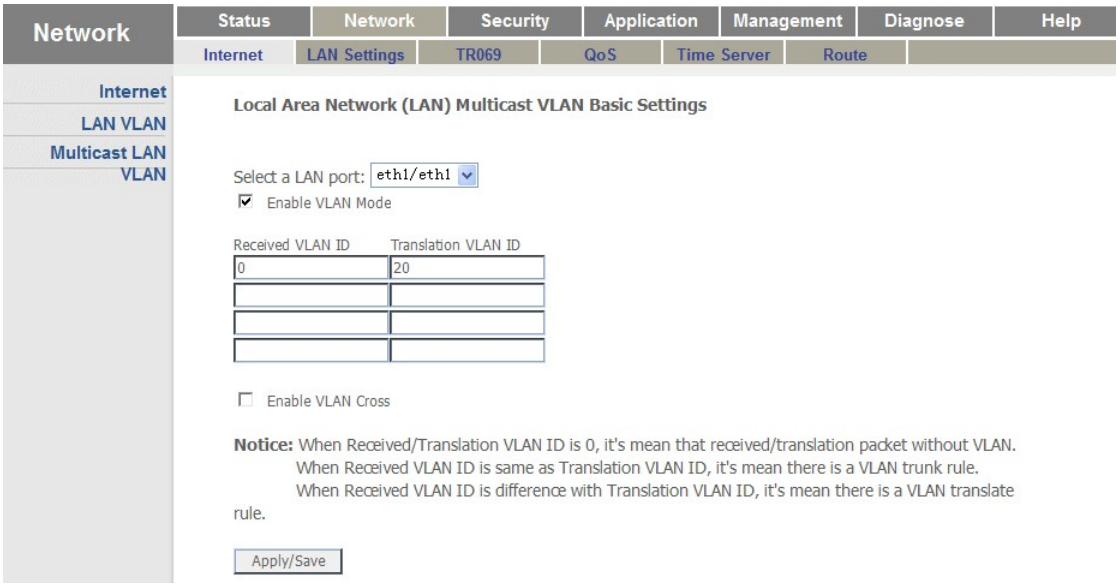

Figure 4-7: Configure multicast VLAN

3. Enable IGMP snooping

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

Figure 4-8: Enable IGMP snooping

4. Join multicast group

User sends an IGMP report message through LAN port 2. Report messages don’t have a VLAN tag.

4.2.2.2 Route Mode for IGMP

5. Add a WAN connection

Choose “Network > Internet > Internet” in the navigation menu. Add a route mode WAN connection using 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 3.
- Keep other parameters default.

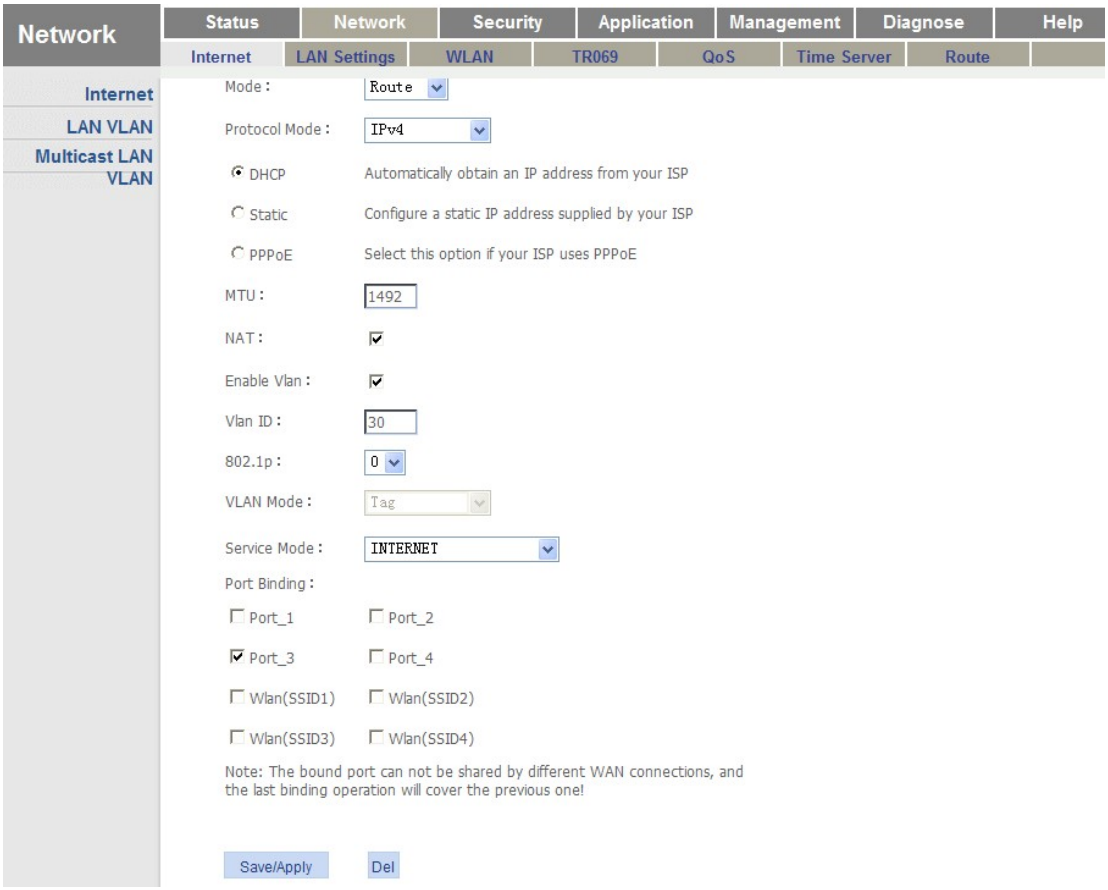

Figure 4-9: Add a route WAN connection

6. Enable IGMP proxy

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

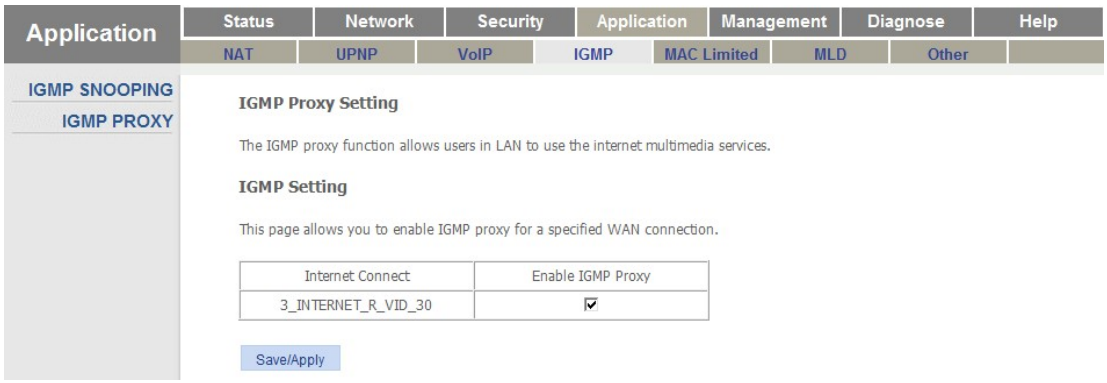

Figure 4-10: Enable IGMP proxy

7. Configure LAN port

It is not necessary to configure any VLANs for LAN ports when the HGU works in route mode for IGMP, so you should disable the VLAN mode of LAN 3.

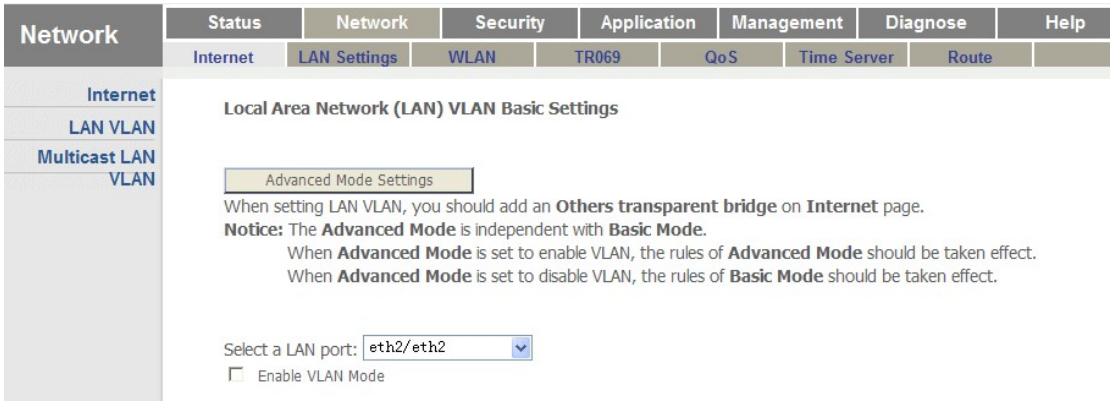

Figure 4-11: LAN VLAN settings

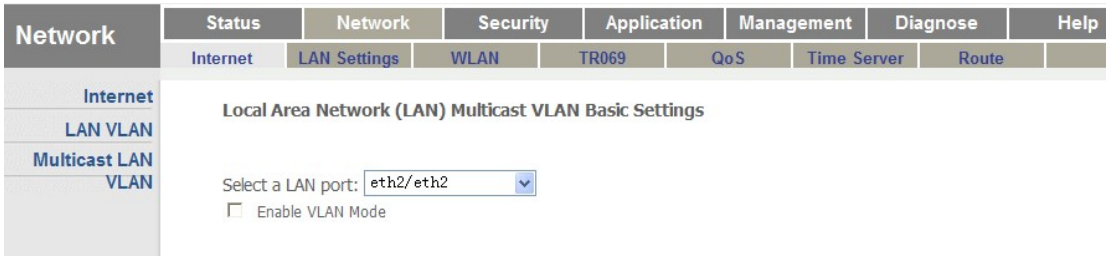

Figure 4-12: Multicast LAN VLAN settings

8. Join multicast group

User sends an IGMP report message through LAN port 3 after they receive an IP address from the HGU.

4.3 VoIP Service

HGU supports the SIP protocol for VoIP service. This example introduces how to configure VoIP service through the web interface.

4.3.1 Requirements

HGU works in route mode. Its IP address is 192.168.3.199, VLAN ID is 100. The SIP server is 192.168.3.19, proxy server is 192.168.3.19.

Phone numbers are 88880001 and 88880002. Usernames and their passwords are the same as the phone numbers.

4.3.2 Steps

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

Connect PC to one of the HGU's LAN ports with a twisted cable.

1. Add a WAN connection

Choose "Network > Internet > Internet" in the navigation menu. Add a route mode WAN connection using the following parameters:

- Protocol mode is IPv4.
- Static IP address.
- Enable VLAN with VLAN ID as 100.
- IP address is 192.168.3.199.
- Subnet mask is 255.255.255.0.
- Default gateway is 192.168.3.1.
- DNS is 192.168.1.1.
- Service mode is VoIP.
- Keep other parameters default.

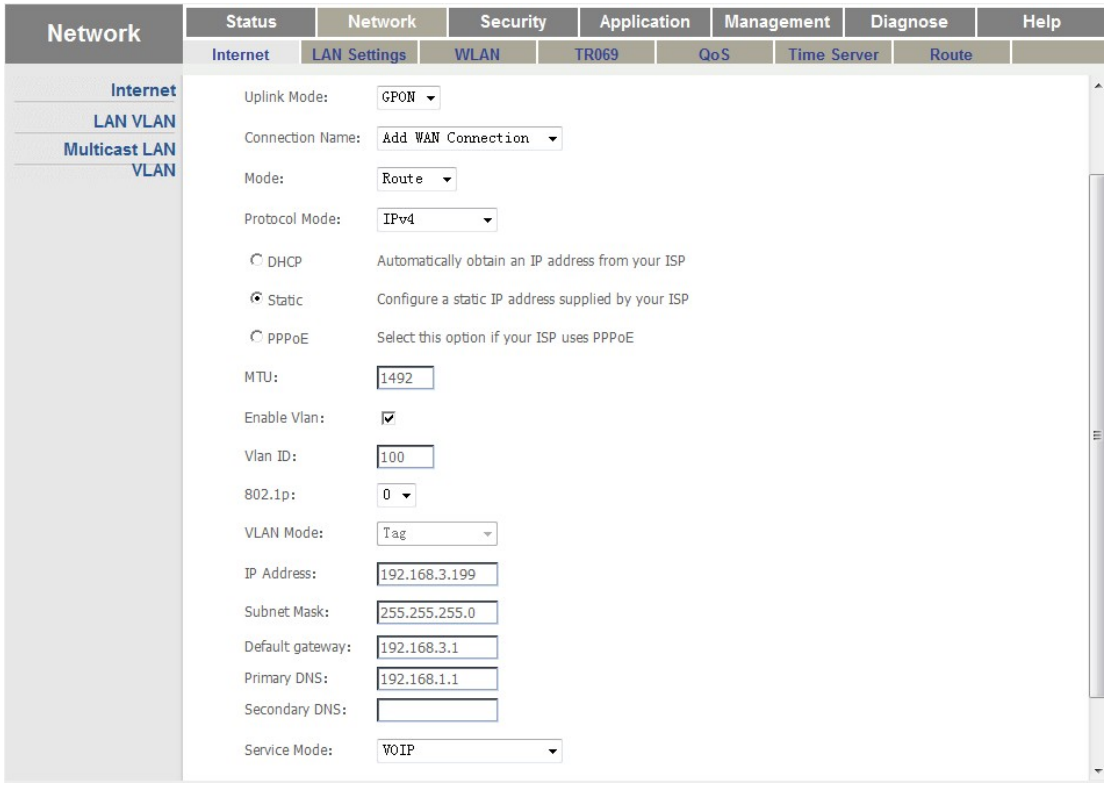

Figure 4-13: Add a route WAN connection

2. Configure VoIP general parameters

Choose “Application > VoIP > General settings” in the navigation menu. Set up VoIP using the following parameters:

- Interface Name is the WAN connection for the VoIP you have added.
- Choose which region the VoIP service is used for. Different regions have different dial tones, ring tones, etc.
- Proxy server and registering server are both 192.168.3.19. Protocol ports are both 5060.
- Enable phone 1 and phone 2. Input phone numbers, usernames, and passwords.
- Select a suitable packing time, default value is 20 ms.

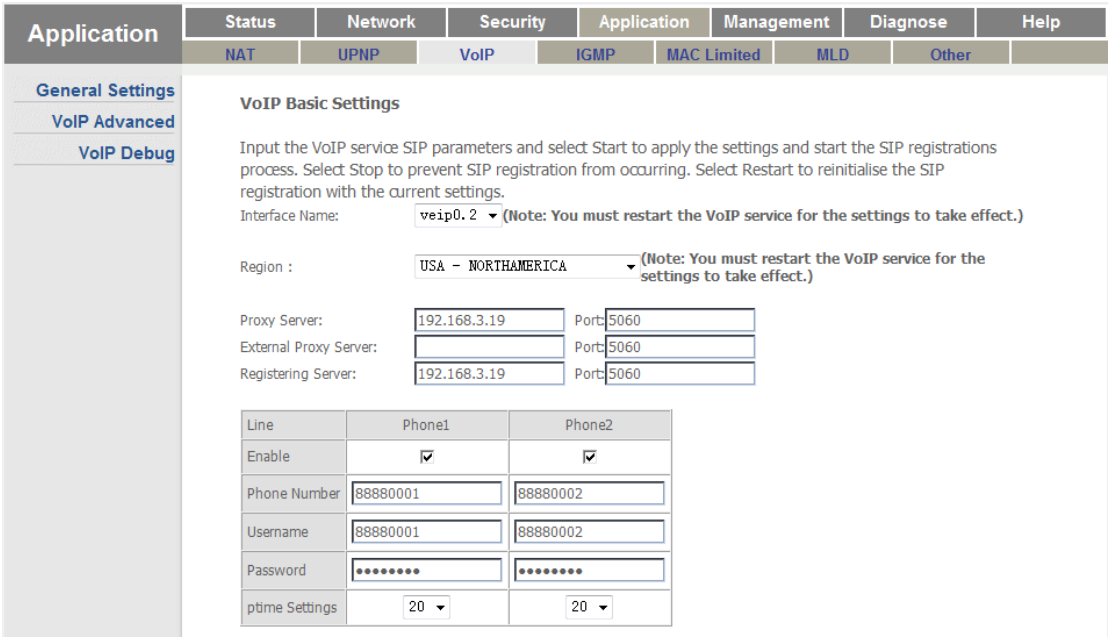

Figure 4-14: VoIP general settings

3. Look up register status

Choose “Status > VoIP Info > VoIP Info” in the navigation menu. You can use the VoIP service once the Registering status is successful.

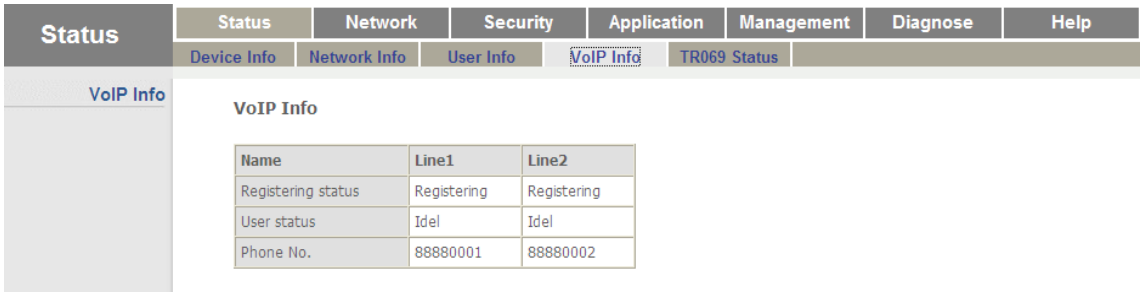

Figure 4-15: VoIP registering status

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 Requirements

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, including

VOD (unicast) and multicast. VOD VLAN is 1000 and multicast VLAN is 1100.

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, including VOD (unicast) and multicast. VOD VLAN is 11 and multicast VLAN is 22.

4.4.2 Steps

Before configuring, make sure the HGU has ben successfully registered and authorized.

Connect PC to one of the HGU's LAN ports with a twisted cable.

4.4.2.1 Route and Bridge Mode for Mixed Service

1. Add WAN connections

Choose "Network > Internet > internet" in the navigation menu. Add a route mode WAN connection using the following parameters:

- Protocol mode is IPv4.
- Choose DHCP. (Provided by ISP)
- Enable VLAN with VLAN ID as 10.
- Service mode is INTERNET.
- Bind port 1.
- Keep other parameters default.

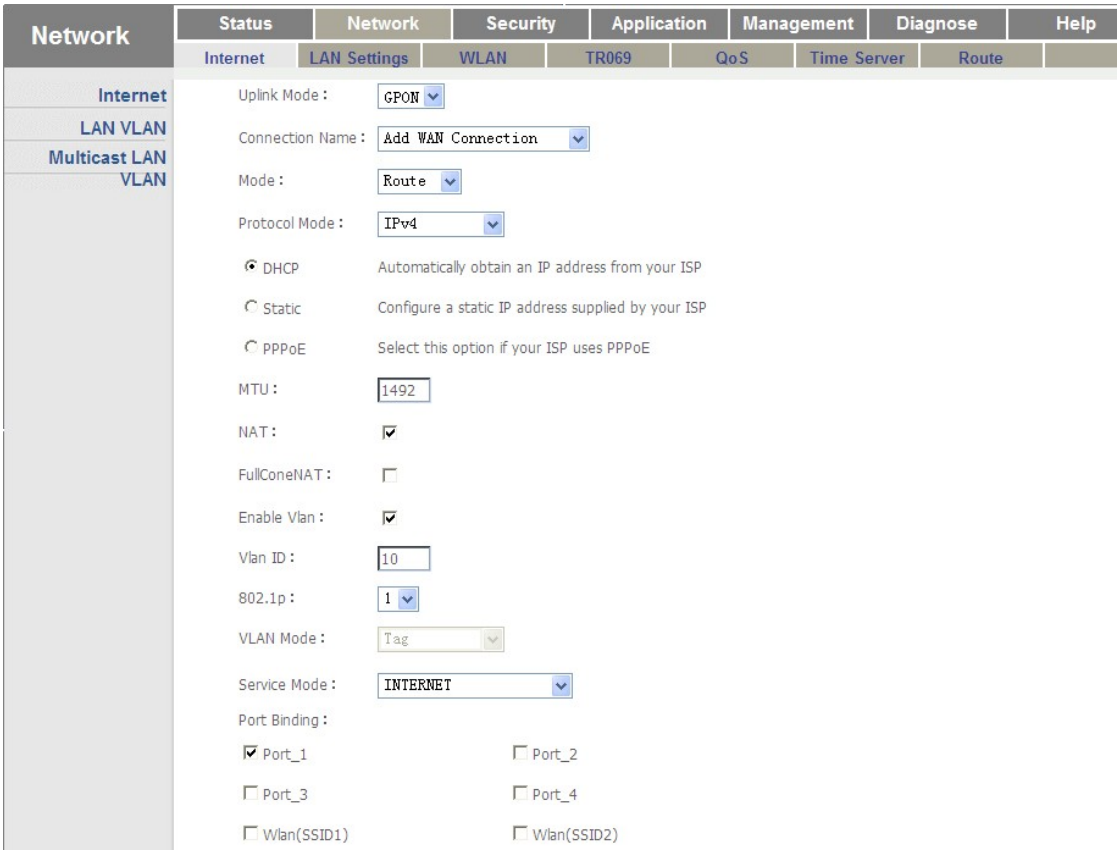

Figure 4-16: Add a route mode WAN

Add a bridge mode WAN connection. Enable VLAN with transparent mode. Service mode is OTHER. Bind port 2.

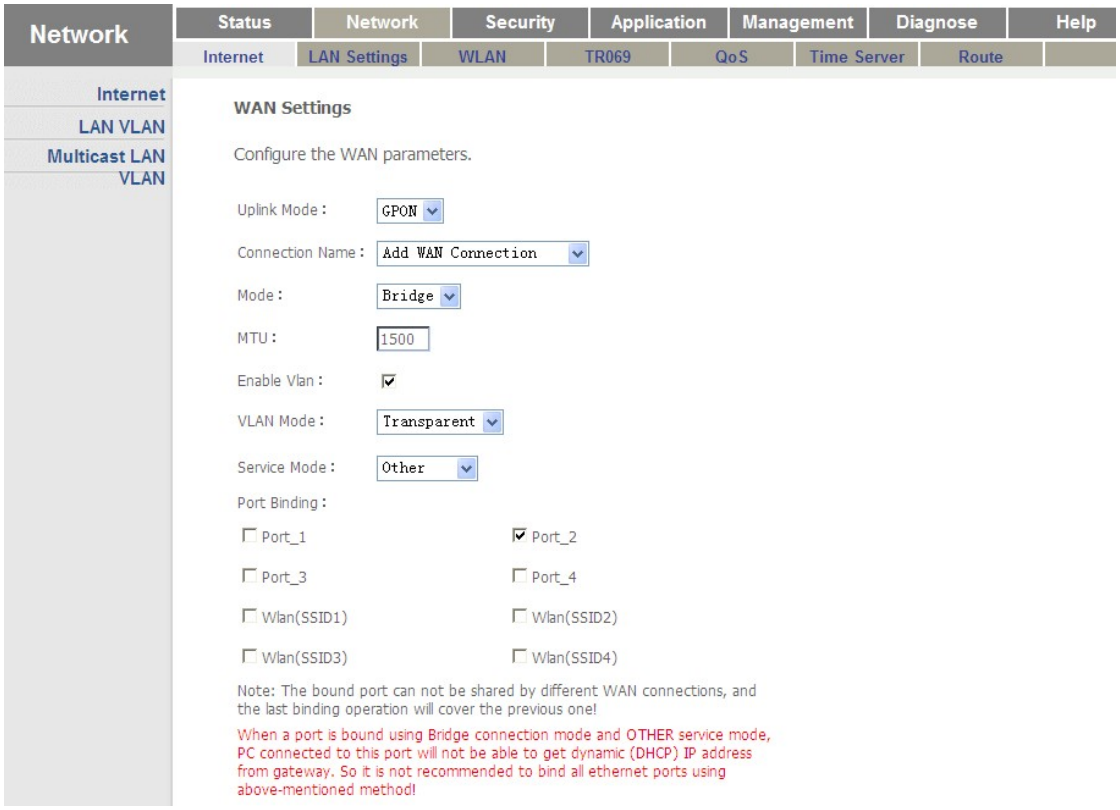

Figure 4-17: Add a bridge mode WAN

2. Configure LAN VLAN

Choose “Network > Internet > LAN VLAN” in the navigation menu. Disable VLAN mode of LAN 1.

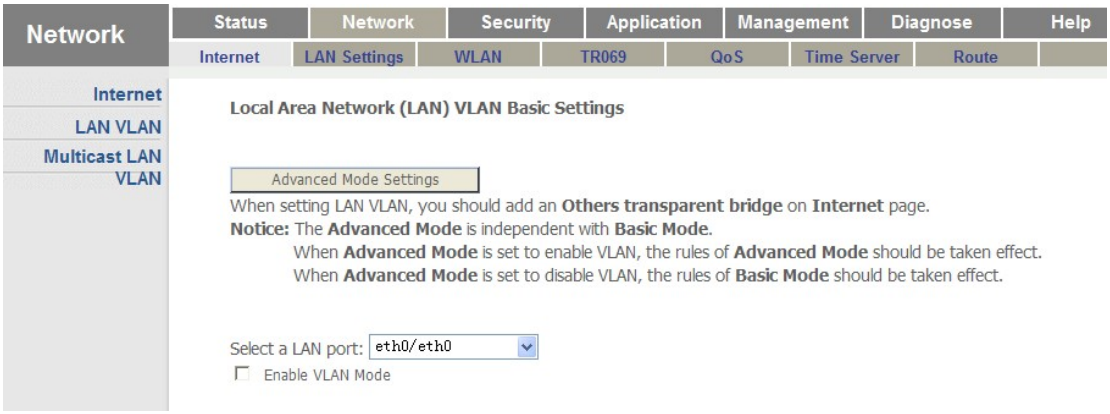

Figure 4-18: Set VLAN for LAN1

Set VLAN as 1000 for VOD service in LAN 2. Received VLAN is 0 and translation VLAN is 1000.

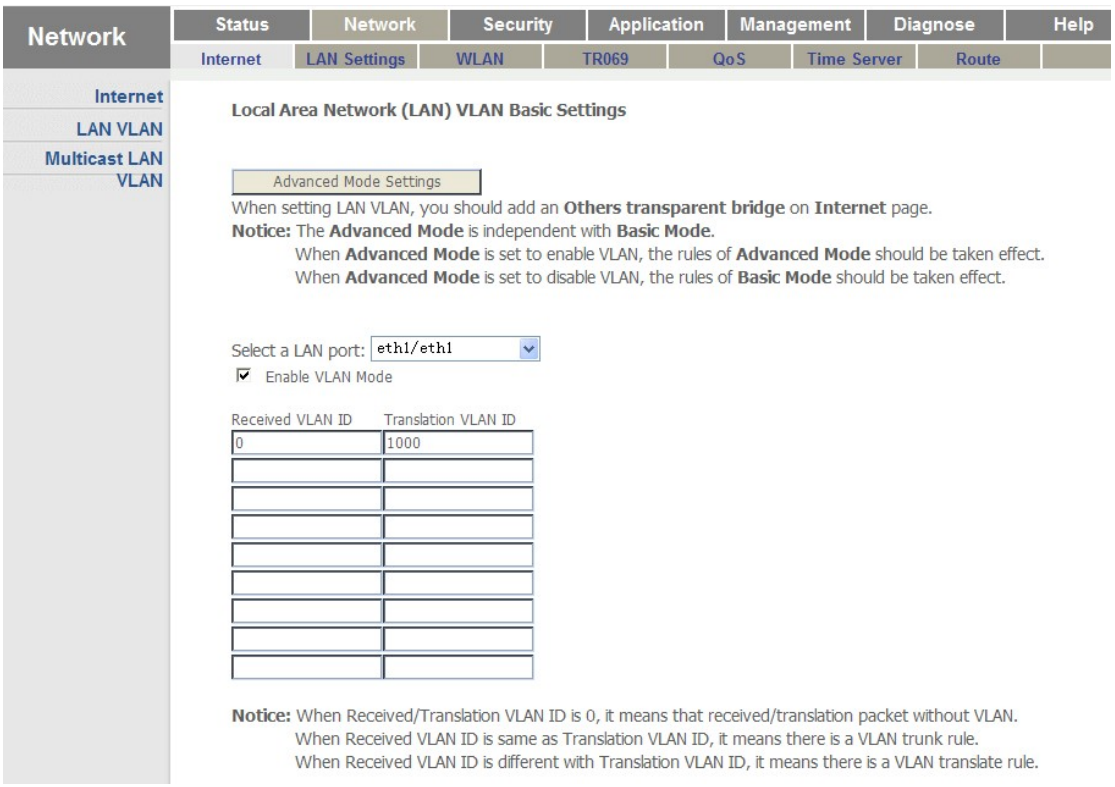

Figure 4-19: Set VLAN for LAN2

3. Configure LAN multicast VLAN.

Choose “Network > Internet > Multicast LAN VLAN” in the navigation menu. Set multicast VLAN as 1100 for LAN2. Received VLAN is 0 and translation VLAN is 1100.

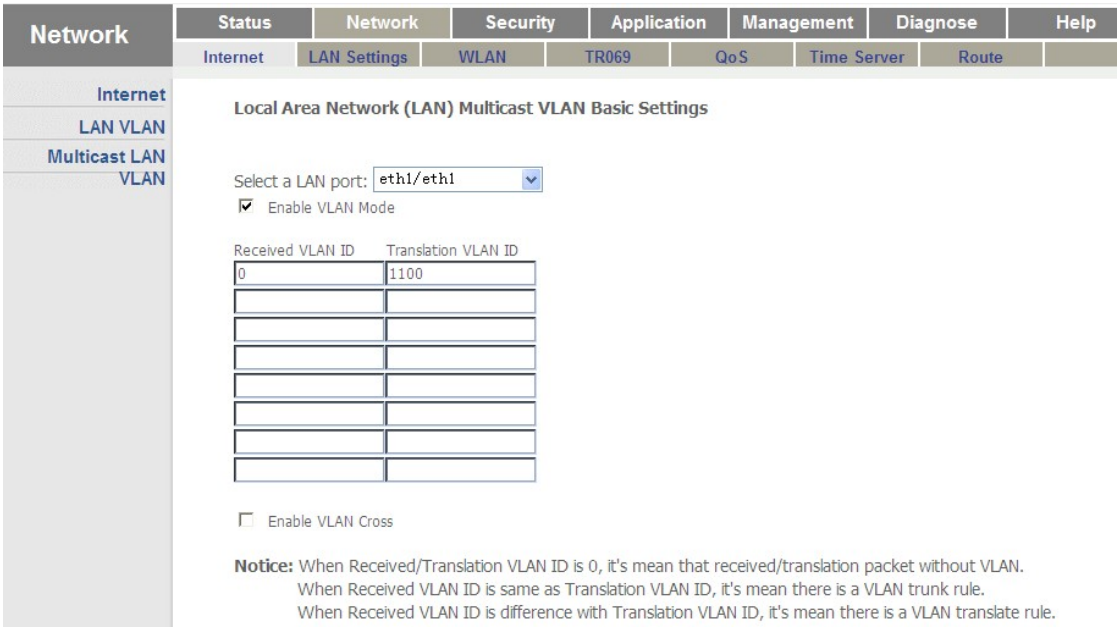

Figure 4-20: Set multicast VLAN for LAN2

4. Access the Internet

Connect PC to LAN port 1. The PC receives an IP address from the HGU and the HGU receives an IP address from a DHCP server in the network. The PC can then access the internet.

5. Watch IPTV

After the STB receives an IP address from your 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 the navigation menu. Add a route mode WAN connection using 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.
- Keep other parameters default.

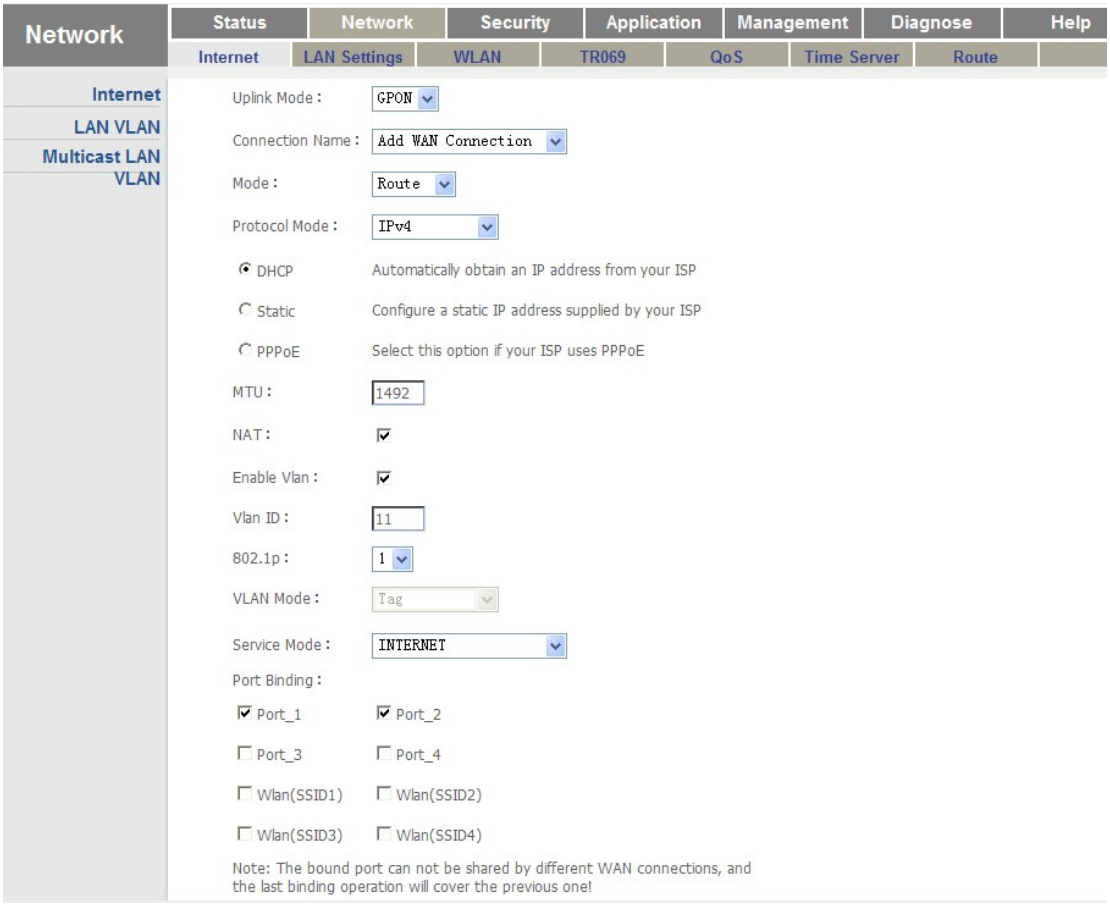

Figure 4-21: Add a route mode WAN connection

2. Enable IGMP proxy

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

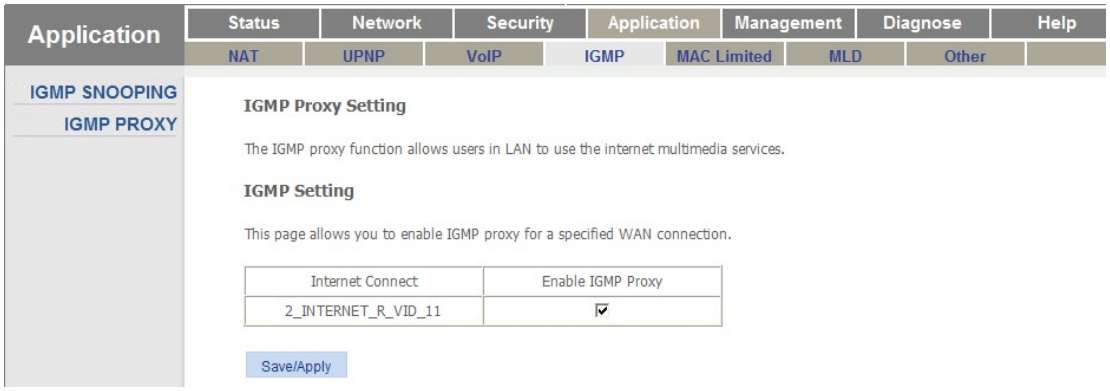

Figure 4-22: Enable IGMP proxy

3. Configure public multicast VLAN

Choose “Application > Other > IPTV” in the navigation menu. Choose the relevant WAN connection and set public multicast VLAN as 22.

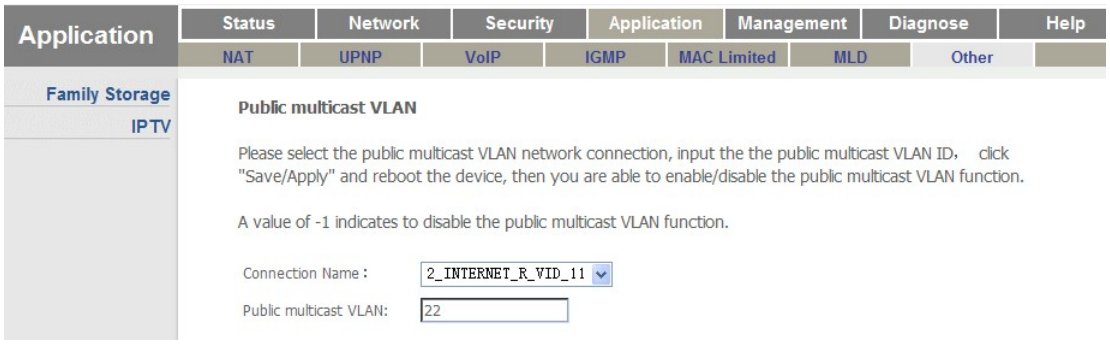

Figure 4-23: Configure public multicast VLAN

4. Configure LAN VLAN

Choose “Network > Internet > LAN VLAN” in the navigation menu. Disable VLAN mode of LAN 1.

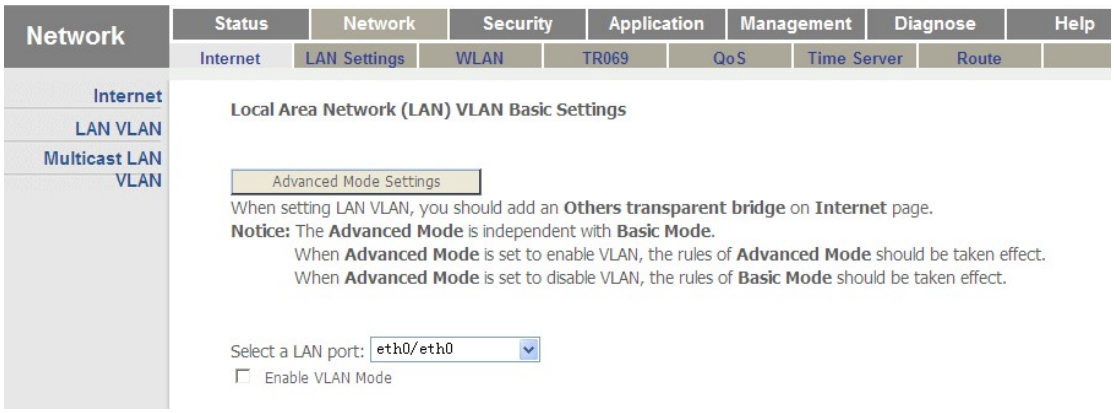

Figure 4-24: Configure VLAN of LAN 1

Disable VLAN mode of LAN 2.

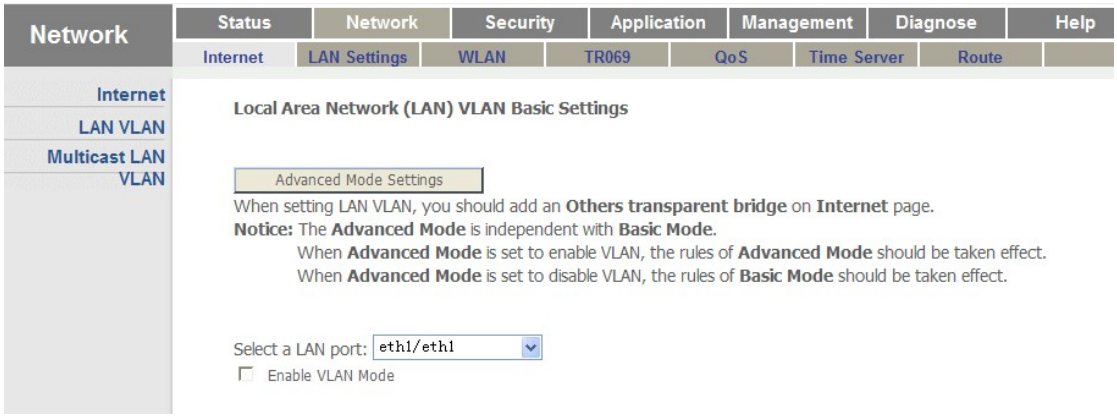

Figure 4-25: Configure VLAN of LAN 2

5. Configure LAN multicast VLAN

Choose “Network > Internet > Multicast LAN VLAN” in the navigation menu. Disable multicast VLAN of LAN 2.

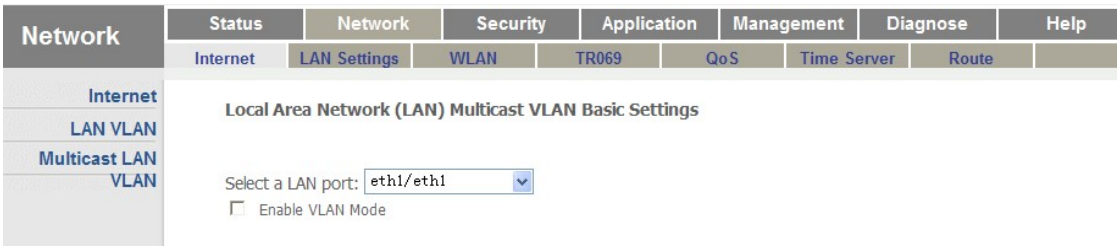

Figure 4-26: Configure multicast VLAN of LAN 2

6. Access the internet

Connect PC to LAN port 1. The PC receives an IP address from the HGU and the HGU receives an IP address from a DHCP server in the network. The PC can then access the internet.

7. Watch IPTV

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

4.5 Internet, IPTV and VoIP Service Mixed

4.5.1 Requirements

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 100, VoIP IP address is 192.168.3.199, and SIP server is 192.168.3.19. The proxy server is 192.168.3.19 as well.

Username and password of SIP account 1: 88880001, 88880001; Account 2: 88880002, 88880002.

4.5.2 Steps

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

Connect PC to one of the HGU's LAN ports with a twisted cable.

1. Add WAN connection

Choose "Network > Internet > Internet" in the navigation menu. Add a route mode WAN connection for internet service using 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.
- Keep other parameters default.

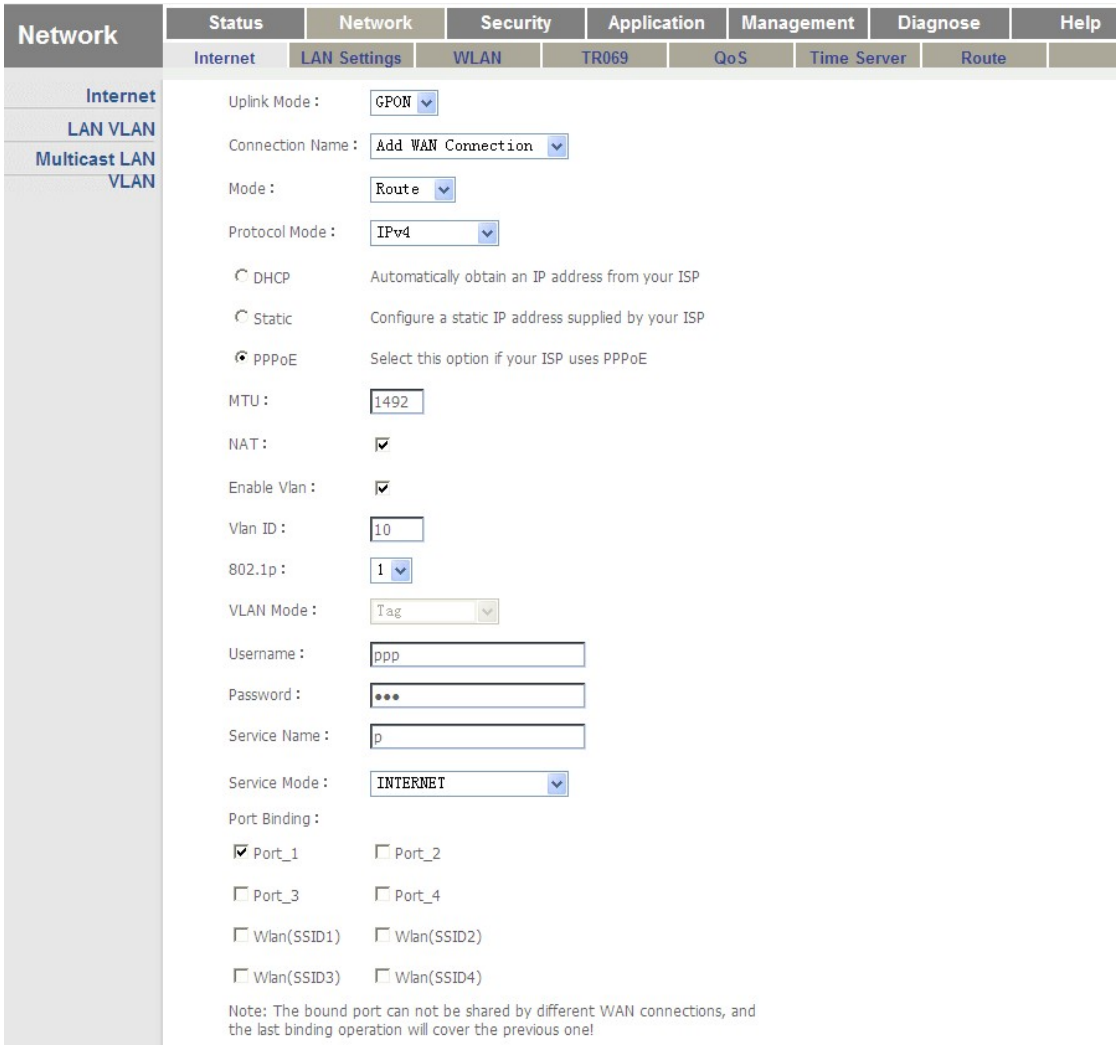

Figure 4-27: Add a WAN connection for Internet service

Add a bridge mode WAN connection for IPTV service. Enable VLAN with transparent mode. Service mode is other. Bind LAN 2.

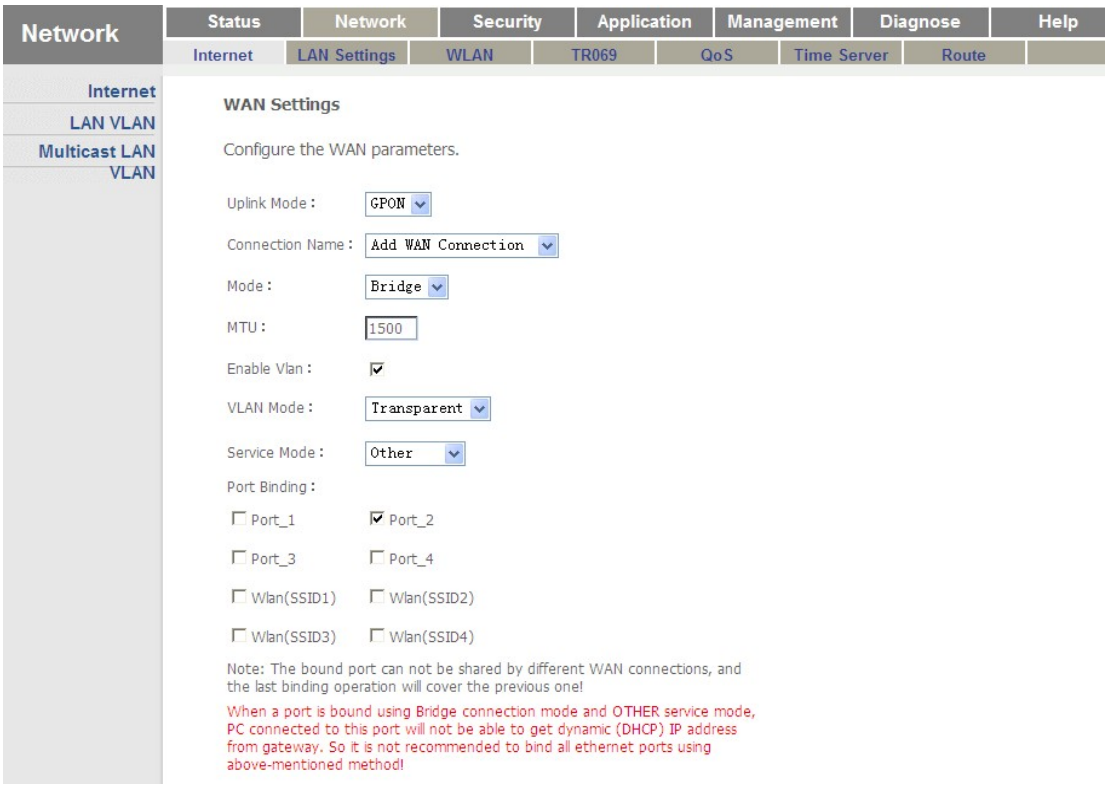

Figure 4-28: Add a WAN connection for IPTV service

Add a route mode WAN connection for VoIP service. Choose IPv4 and static. Input the IP address, mask, gateway, DNS etc. Enable VLAN, VLAN ID is 100. Service mode is VoIP.

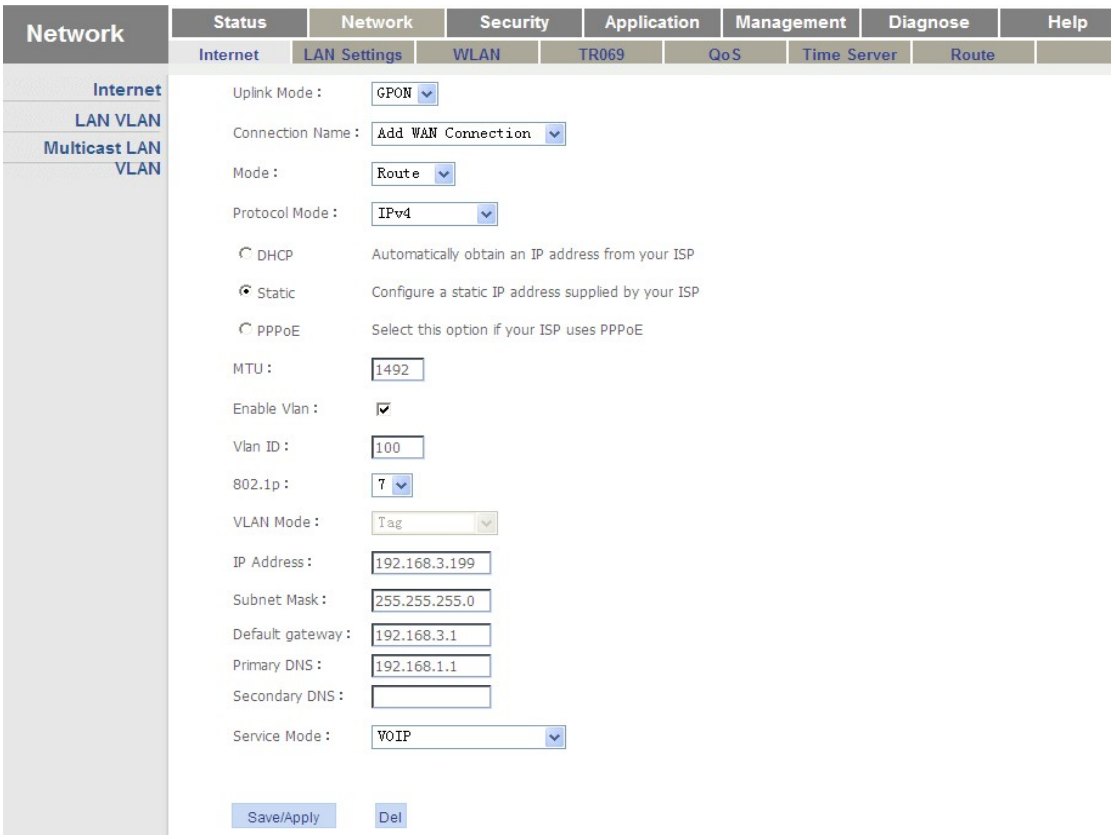

Figure 4-29: Add a WAN connection for VoIP service

2. Configure LAN VLAN

Choose “Network > Internet > LAN VLAN” in the navigation menu. Disable VLAN mode of LAN 1.

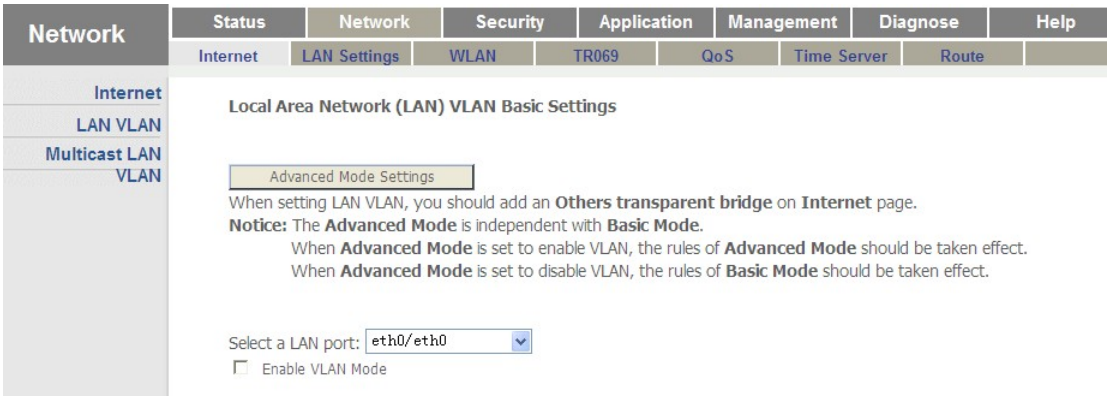

Figure 4-30: Configure VLAN of LAN 1

Configure VLAN of LAN 2. VLAN ID is 1100, for VOD service.

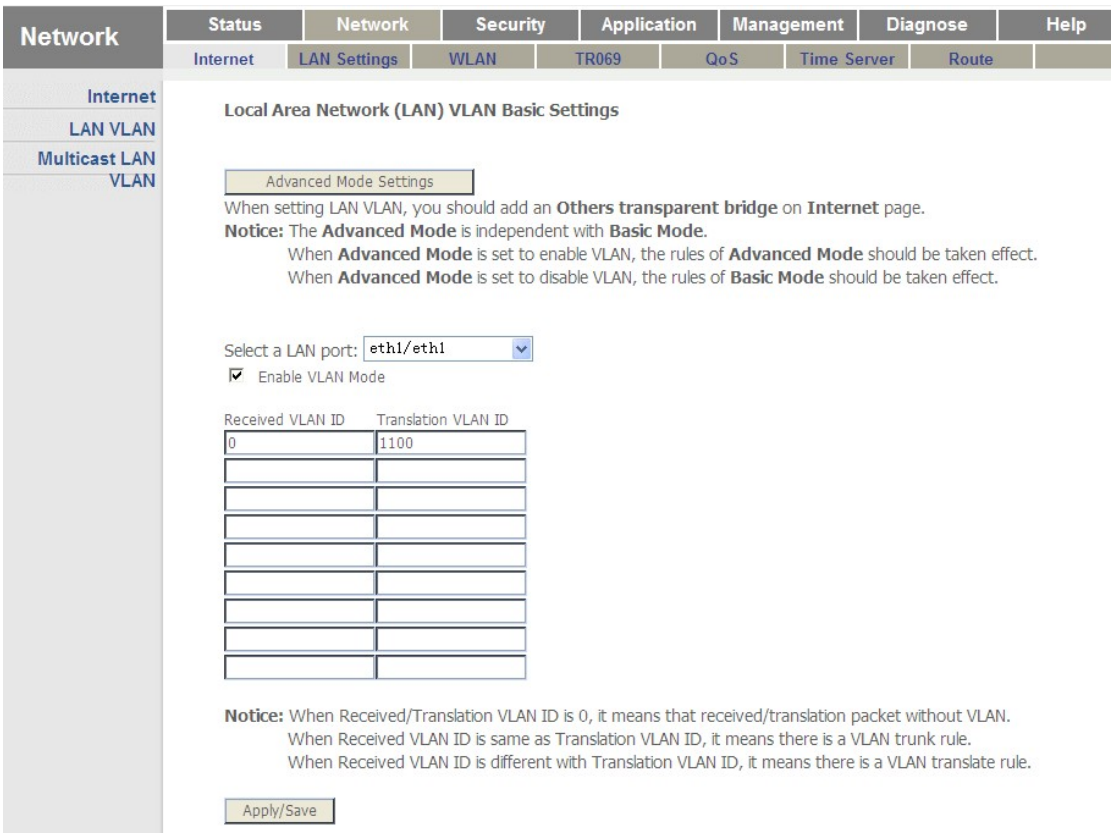

Figure 4-31: Configure VLAN of LAN 2

3. Configure LAN multicast VLAN

Choose “Network > Internet > Multicast LAN VLAN” in the navigation menu. Enable VLAN of LAN 2. Input received VLAN ID with 0 and translation VLAN ID with 1100.

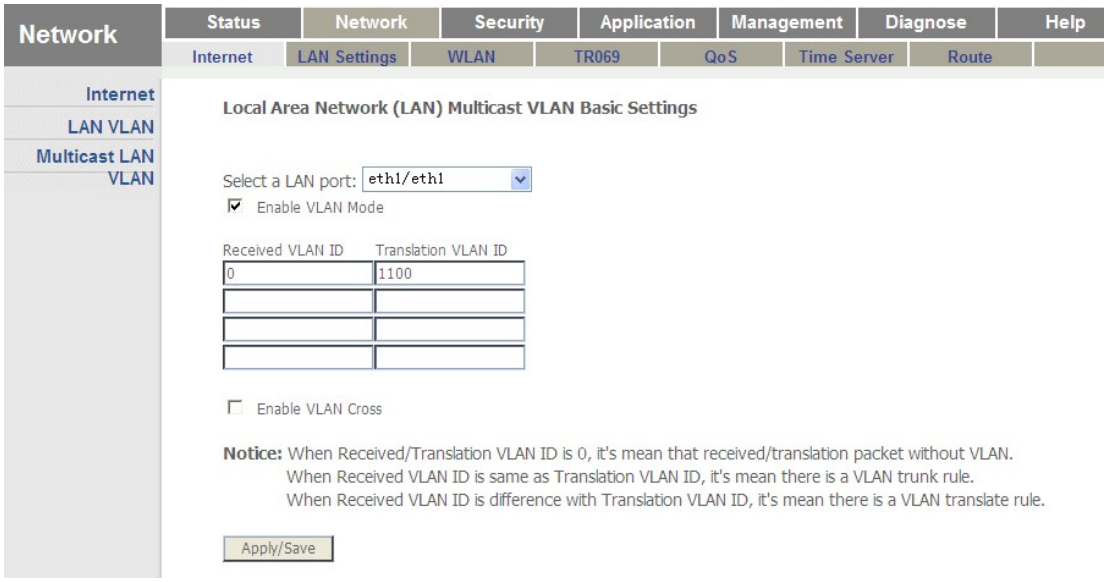

Figure 4-32: Configure multicast VLAN of LAN 2

4. Configure VoIP general parameters

Choose “Application > VoIP > General Settings” in the navigation menu. Configure VoIP using the following parameters:

- “Interface Name” is the WAN connection that you have added for VoIP in step 1.
- “Region” contains many countries or regions. Different regions have their own dial tones, ring tones, etc.
- “Proxy server” and “Registering server” are both 192.168.3.19, port is 5060.
- Input phone number, username, and password of each line.
- Choose packing time, default is 20ms.

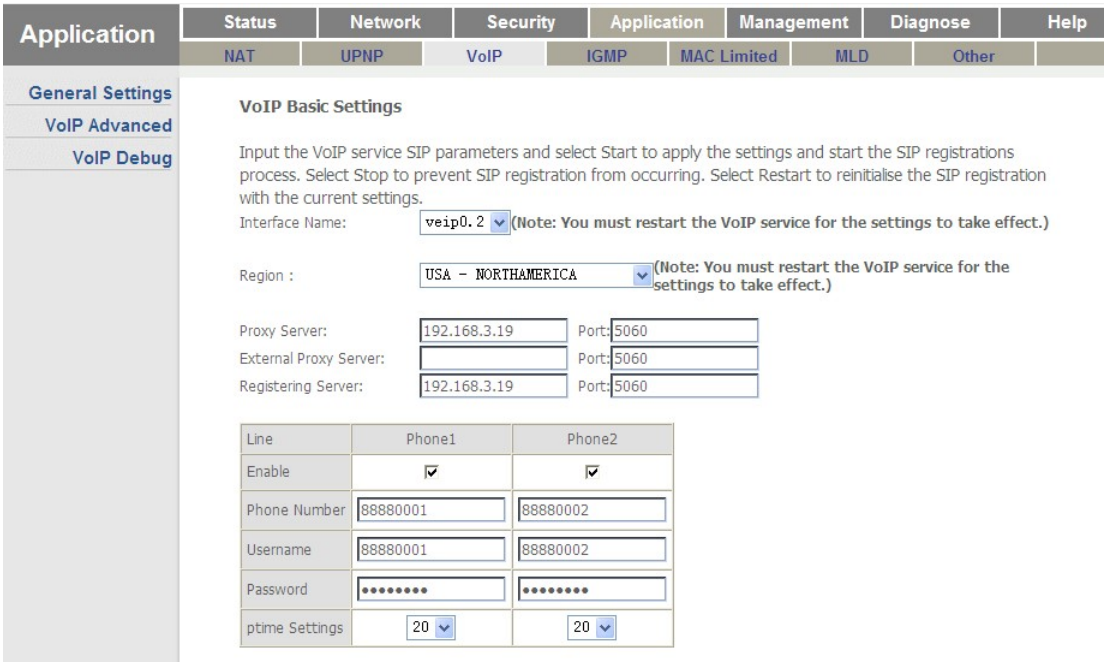

Figure 4-33: VoIP general settings

5. Access the internet

Connect PC to LAN port 1. The PC receives an IP address from the HGU and the HGU receives an IP address from a DHCP server in the network. The PC can then access the internet.

6. Watch IPTV

After the STB receives an IP address from your ISP via DHCP, you can watch IPTV.

7. Look up register status

Choose “Status > VoIP Info > VoIP Info” in the navigation menu. You can use the VoIP service once Registering status is successful.

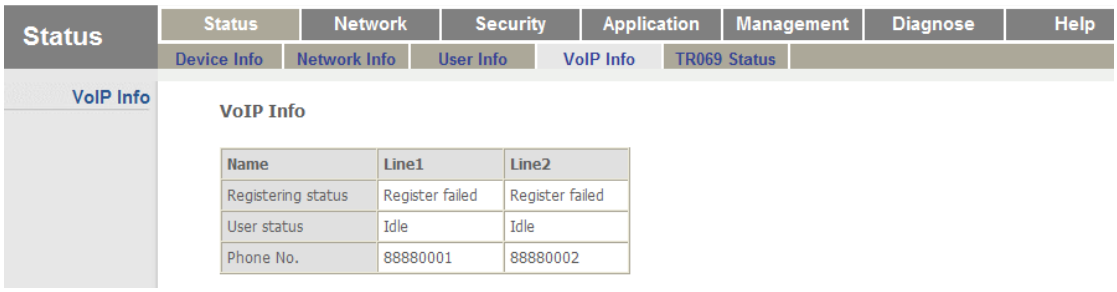

Figure 4-34: VoIP information

4.6 WLAN Service

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

4.6.1 Requirements

1. HGU works in Route mode, HGU receives 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 been successfully registered and authorized.

Connect PC to one of the HGU’s LAN ports with a twisted cable.

1. Add a WAN connection

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

- Obtain IP address by DHCP.
- Enable VLAN with VLAN ID as 11.
- Service mode is INTERNET and bind SSID1.
- Keep other parameters default.

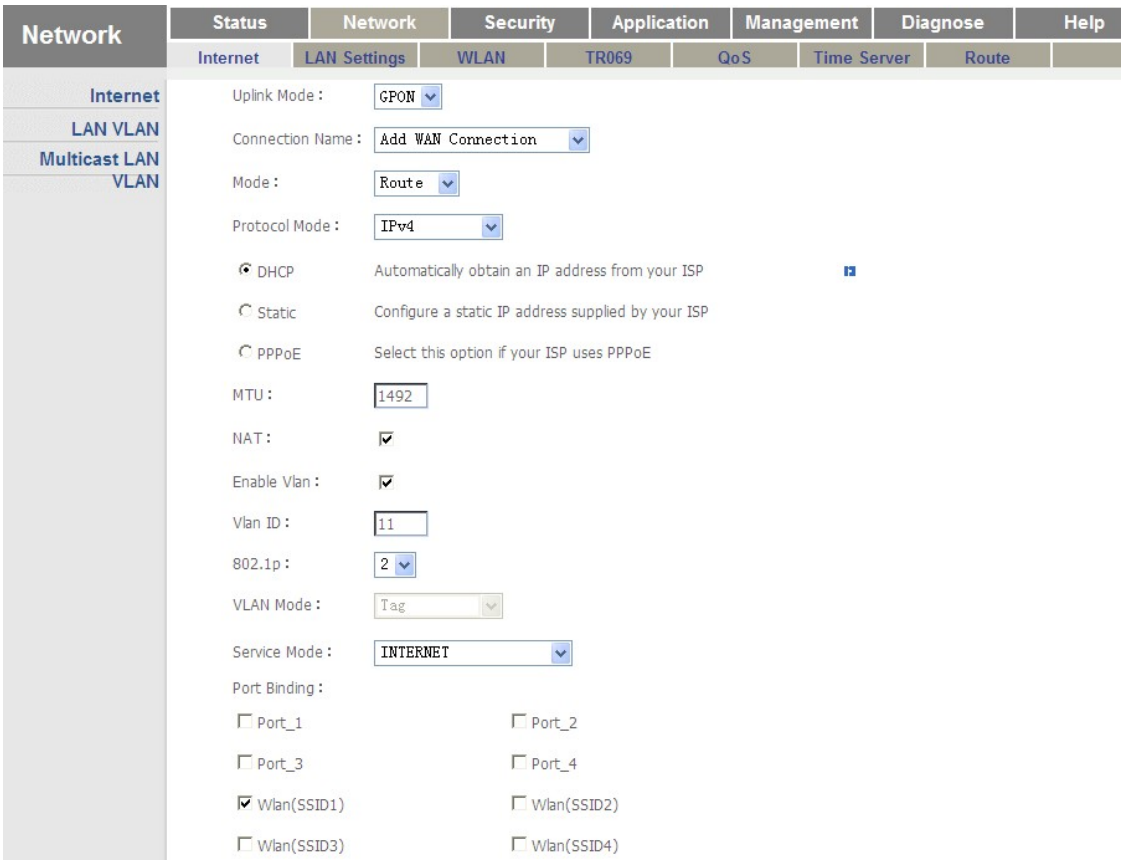

Figure 4-35: Add a route WAN connection

2. Configure WLAN basic parameters

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

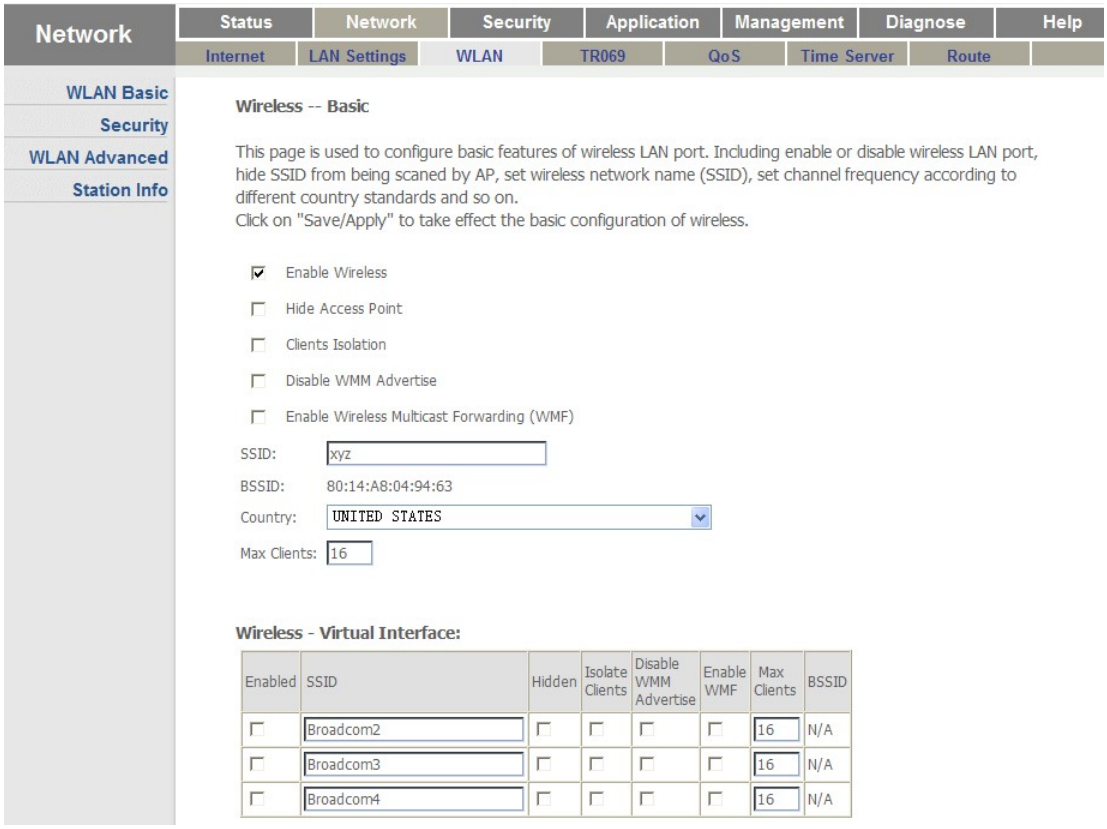

Figure 4-36: WLAN basic settings

3. Configure network authentication

Choose “Network > WLAN > Security” in the navigation menu. Select the SSID, and set up WPA-PSK for its network authentication method and TKIP+AES for its encryption method. Enter a password in the passphrase textbox.

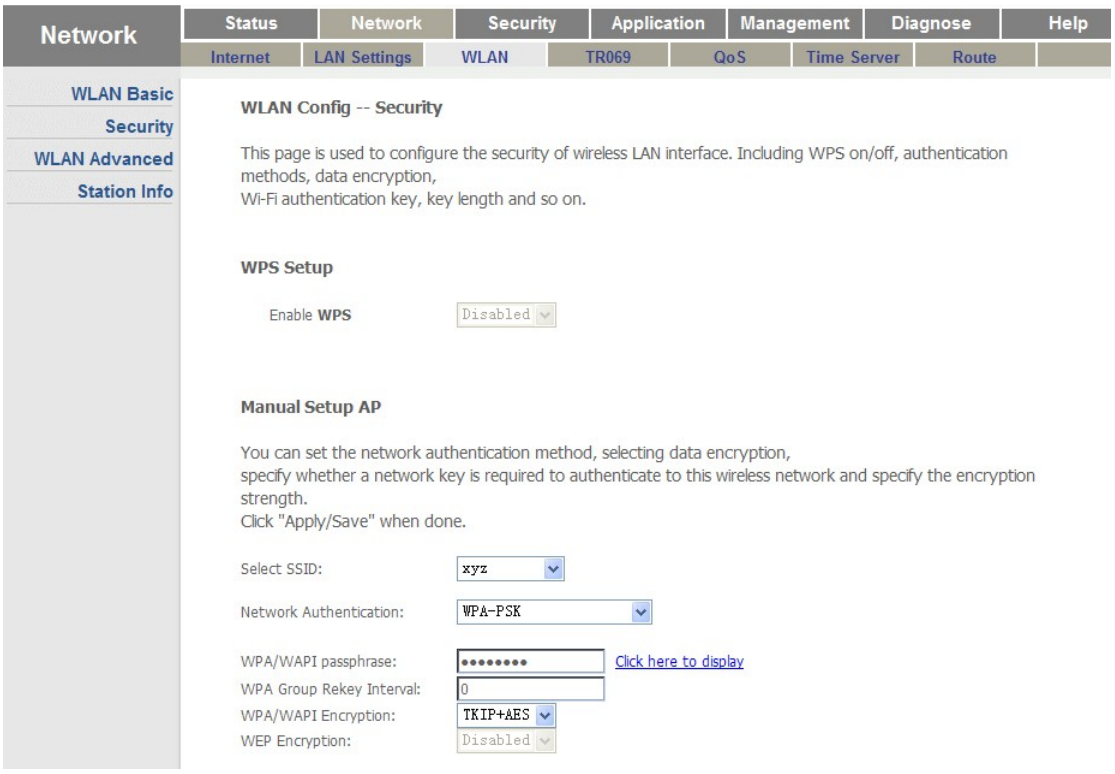

Figure 4-37: WLAN security settings

4. Configure WPS

Choose “Network > WLAN > Security” in the navigation menu. Enable WPS and select Push-Button for both client and AP.

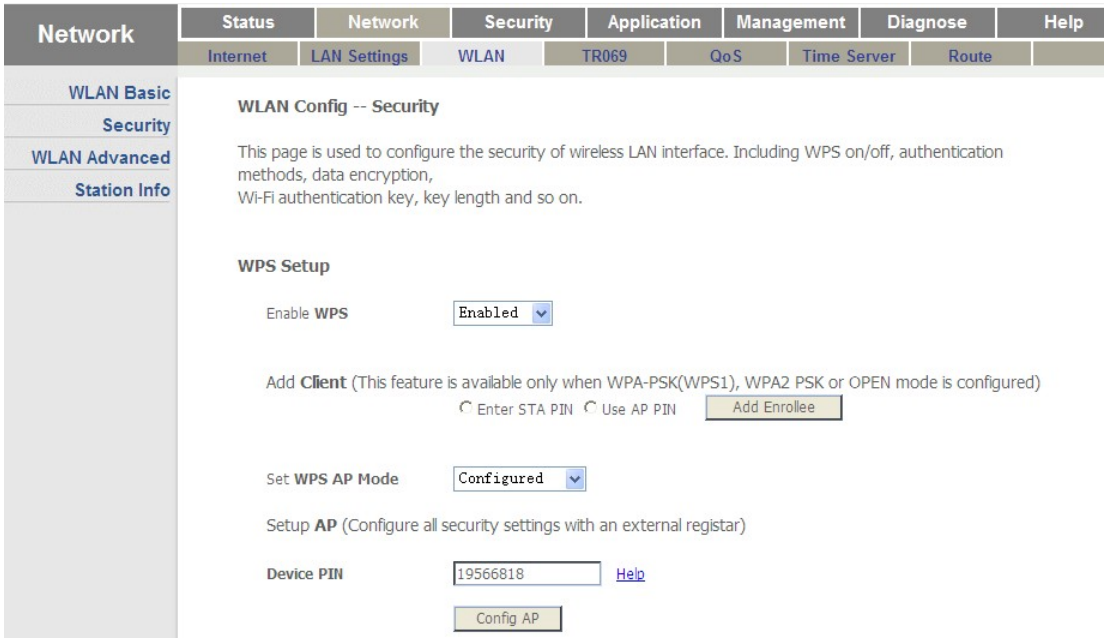

Figure 4-38: WPS settings

5. Access the Internet

Search for an SSID named xyz with a laptop. Double-click to connect and enter the correct password.

If client has WPS function, you can connect the client to AP by pressing the Pair button on the HGU. When the WPS indicator blinks, press the WPS button on the 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 the navigation menu. Select the software image file with .w as a suffix, and click the “Update Software” button. The HGU will restart automatically once it’s been updated. The whole process takes about 2 minutes.

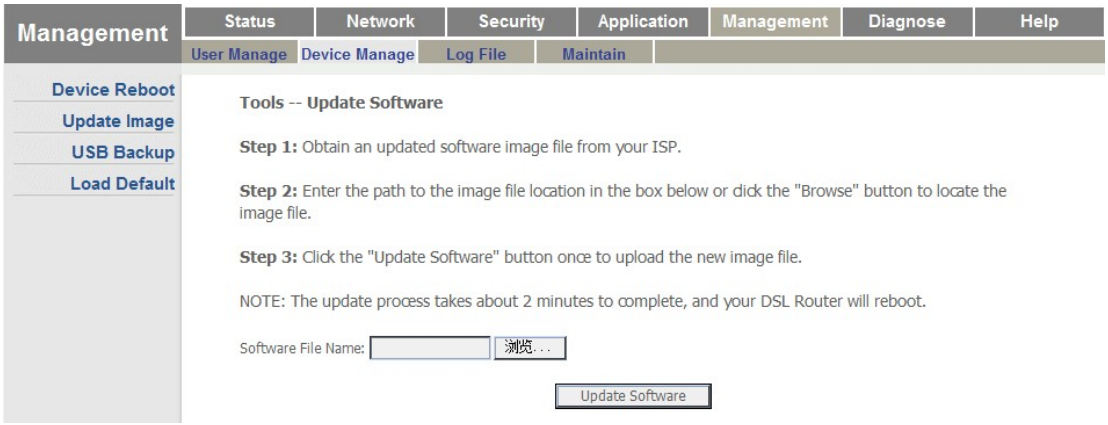

Figure 4-39: Update software

Chapter 5. Troubleshooting

Q: None of the indicators are lit.

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

(2) Indicator LED switch is turned off.

Q: The Los indicator is flashing.

A: (1) There is no optical signal. The fiber might have broken down or the connection is loose.

(2) Optical power is too low.

(3) The fiber is dusty.

Q: The LAN indicators are not lit.

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

(2) The cable broke down or the connection is loose.

(3) The cable type is incorrect or too long.

Q: The FXS indicators are not lit.

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

(2) SIP accounts aren't registered.

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. The default Admin password is "vsONU101".

(2) The cable broke down.

(3) IP conflict or there is loopback.

Q: User can't access the internet.

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

(2) There is loopback or an attack in the network.

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

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.

Q: HGU stops working after working for some time.

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

(2) The device overheats.

Ascent Communication Technology Ltd

AUSTRALIA
961 Mountain Highway, Boronia
Victoria 3155, AUSTRALIA
Phone: +61-488 293 682

HONG KONG SAR
Unit 9, 12th Floor, Wing Tuck Commercial Centre
177 Wing Lok Street, Sheung Wan, HONG KONG
Phone: +852-2851 4722

CHINA
Unit 1907, 600 Luban Road
200023, Shanghai CHINA
Phone: +86-21-60232616

USA
2710 Thomes Ave, Cheyenne
WY 82001, USA
Phone: +1-203 816 5188

EUROPE
Pfarrer-Bensheimer-Strasse 7a
55129 Mainz, GERMANY
Phone: +49 (0) 6136 926 3246

VIETNAM
15 /F TTC Building, Duy Tan Street, Cau Giay Dist.
Hanoi, VIETNAM
Phone: +84 168 481 8348

WEB: www.ascentcomtec.com **EMAIL:** sales@ascentcomtec.com

Ver. ACT_AP224S_User_Manual_V1a_Aug_2016