BEC 8920AC

Ultimum®

The Ultimate Residential Gateway with 802.11ac

VDSL2/ADSL2+/Bonded/FTTH

User Manual

Version release: v2.3

Last revised: Sept., 2015

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

Introduction to Your Router

Thank you for purchasing **BEC 8920AC_The Ultimate Residential Gateway with 802.11ac**. This unit is an all-in-one Universal Bonded Gateway supporting ultra-broadband triple-play services via multiple WAN connection options. Service providers can utilize one gateway for all major broadband technologies such ADSL2+, VDSL2, xDSL bonding and FTTH. In addition to offering the multiple WAN connection options, the 8920AC integrates multiport Ethernet switching and routing, 802.11a/b/g/n/ac Wireless networking, advanced firewall security including stateful packet inspection, Quality of Service (QoS) and remote management. Users can easily enjoy high bandwidth services such as High Definition IPTV, streaming video, interactive gaming, over-the-top (OTT) applications to multiple devices throughout the home.

Flexible Deployment Options

The BEC 8920AC provides service operators with flexible, scalable deployment options optimized to both reduce costs and provide the longest possible lifespan for the investment. The BEC 8920AC integrates dual WAN options; a VDSL2/ADSL2+ interface and a second 10/100/1000 Ethernet WAN interface which can be used for broadband connectivity to any other Ethernet broadband device. Operators can now deploy one device to support current and future network migration.

Quality of Service

Quality of Service (QoS) gives users' full control over outgoing data traffic. Priority can be assigned by the router to ensure that important transmissions like gaming packets, VoIP calls or IPTV/streaming content passes through the router at lightning speed, even when there is heavy Internet traffic. The speed of different types of outgoing data passing through the gateway is also controlled to ensure that users do not saturate bandwidth with their browsing activities.

Robust Firewall Security

The NAT default firewall has advanced anti-hacker pattern-filtering protection features that automatically detect and block Denial of Service (DoS) attacks. In addition, Packet Filtering provides high-level security for access control. Built with Stateful Packet Inspection (SPI), the router enables users to determine whether or not a data packet is allowed to pass through the firewall to the private LAN.

Dual Concurrent Wireless with Superior 802.11ac Speed & Ultimate Coverage

With the next wireless generation, 802.11ac, integrated in the 8920AC, the router delivers speed as fast 1.3 gigabit per second. Wireless AC provides high-throughput wireless speed by taking the advantage of frequency on the 5GHz band with less interference and using the beamforming technology to enable a direct signal focus on the Access Point and a wireless client to extend wireless coverage area. The 8920AC supports a link rate up to 300Mbps in 2.4GHz frequency range & 1300Mbps in 5GHz range and is also backward compatible with exiting 802.11 a / b / g / n equipment in the network. The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over Wireless

LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard for easy and secure establishment of a wireless home network. If the user's network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function expands the wireless network without needing any external wires or cables.

Pathway to the Future

The BEC 8920AC fully supports IPv6 (Internet Protocol Version 6), implementation of IPv6 is growing significantly and multiple transition methods are required to support the coexistence and migration from IPv4. With BEC IPv6 enabled devices, service providers easily adapt IPv6 to their network as we support major transition mechanisms such as Dual-Stack, Dual-Stack Lite, and 6RD.

Features & Specifications

VDSL Compliance

- Compliant with ITU-T G.993.2, G.994.1 and G.997.1 VDSL2 Standard
- VDSL2 Profiles (Single): 8a, 8b, 8c.8d, 12a, 12b, 17a, 30a
- VDSL2 Profiles (Bonded): 8a, 8b, 8c.8d, 12a, 12b, 17a
- ADSL/2/2+ fallback modes
- Comply G.993.5, G.998.2 and G.998.4

ADSL Compliance

- Compliant with ADSL Standards
  - Full-rate ANSI T1.413 Issue 2
  - G.dmt (ITU G.992.1)
  - G.lite (ITU G.992.2)
  - G.hs (ITU G.994.1)
- G.dmt.bis (ITU G.992.3) Compliant with ADSL2 Standards
  - ADSL2 Annex M (ITU G.992.3 Annex M)
- Compliant with ADSL2+ Standards
  - G.dmt.bis plus (ITU G.992.5)
- Comply ITU T G.998.1 and G.998.2

Network Protocols and Features

- NAT, static routing and RIP-1/2
- Universal Plug and Play (UPnP) Compliant
- Transparent Bridging
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS relay and IGMP proxy
- VLAN_MUX and IGMP snooping for video service
- Management based-on IP protocol, port number and address
- SMTP Client

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and address

Firewall & Virtual Private Network (VPN)

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack and Ping of Death, etc.
- Remote access control for web base access
- Anti probe function
- Packet filtering, MAC filtering, URL content filtering
- Password protection for system management
- VPN pass-through

Wireless LAN

- Compliant with IEEE 802.11a/b/g/n/ac standards
- 2.4 GHz & 5GHz frequency range
- Up to 300/1300Mbps wireless operation rate
- WPS (Wi-Fi Protected Setup) supported
- 64/128 bits WEP supported for encryption
- Wireless Security with WPA-PSK/ WPA2-PSK support
- WDS repeater function support

Management

- Quick Installation Wizard
- Web-based GUI for remote and local management
- Firmware upgrades and configuration data transfer via web-based interface
- Embedded Telnet server for remote and local management
- Available Syslog
- Supports DHCP server/client/relay
- SNMP v1/v2, MIB supported

Hardware Specifications

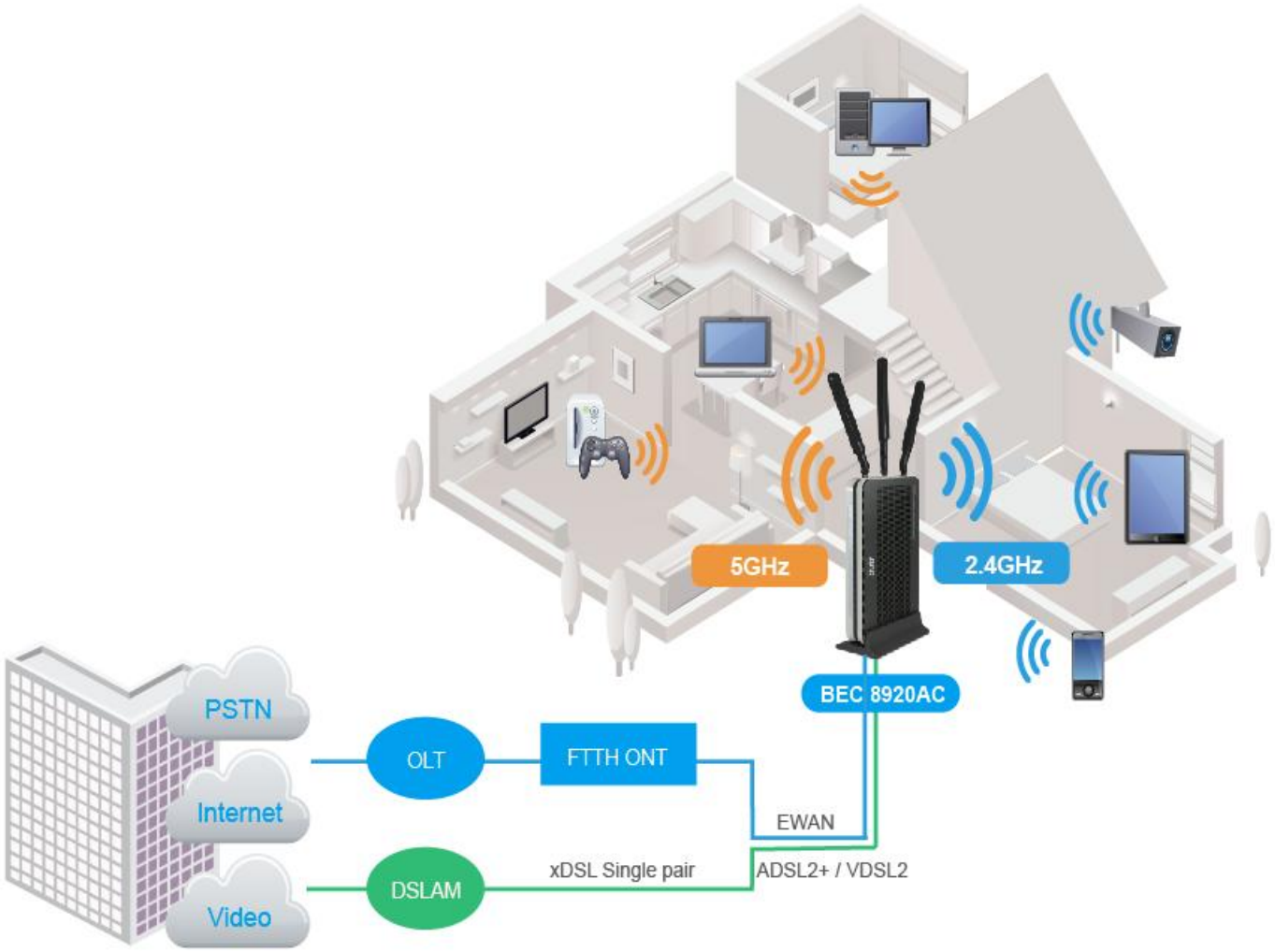
Physical interface

- DSL: Single xDSL RJ-11 Interface
- USB 2.0 for 3G/4G LTE backup
- Ethernet MDI/MDIX Switch: 5-port Gigabit 10/100/1000Mbps
- EWAN: RJ-45 Gigabit Ethernet Wan (on Ethernet 5)
- Wireless On/Off button
- WPS push button
- Reset Button
- Power jack
- Power switch
- WLAN: 3 external antennas

Physical Specifications

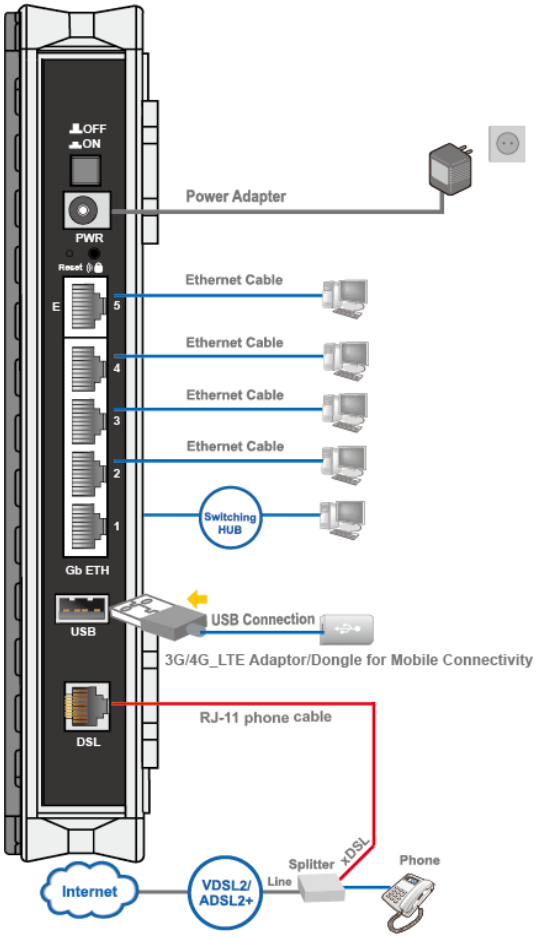
- Dimensions (W*H*D): 9.04" x 6.10" x 1.69" (229.5mm x 155mm x 43mm)

Network Application Diagrams

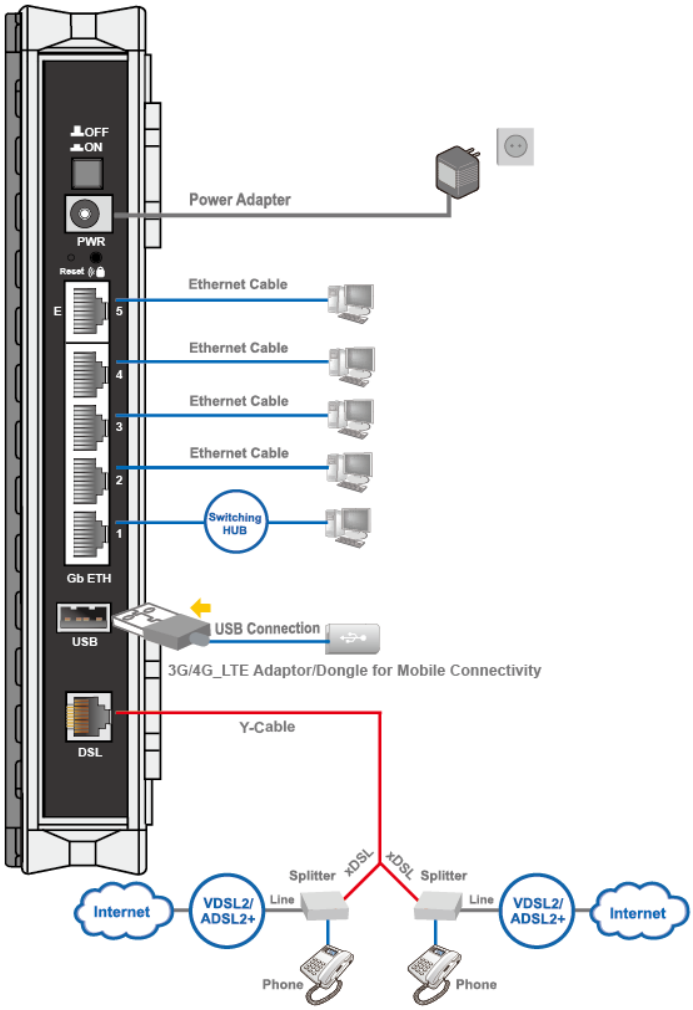


BEC 8920AC is an all-in-one gateway router supporting multiple WAN connection options (ADSL2+ single/bonding, VDSL2 single/bonding, Ethernet WAN and Auto WAN Failover) to connect to the Internet.

xDSL Connection – Single Pair

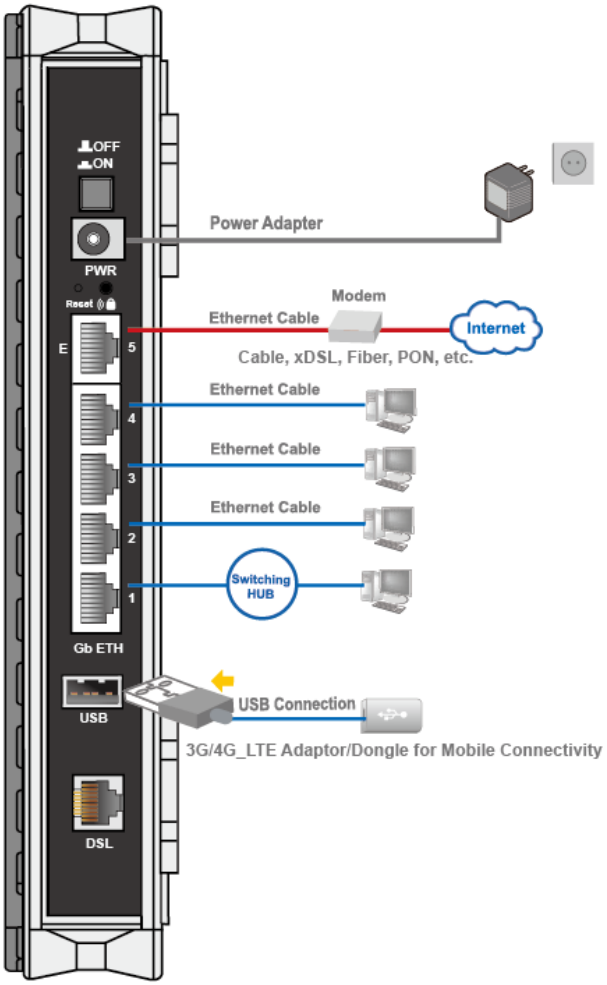


xDSL Connection – Bonding



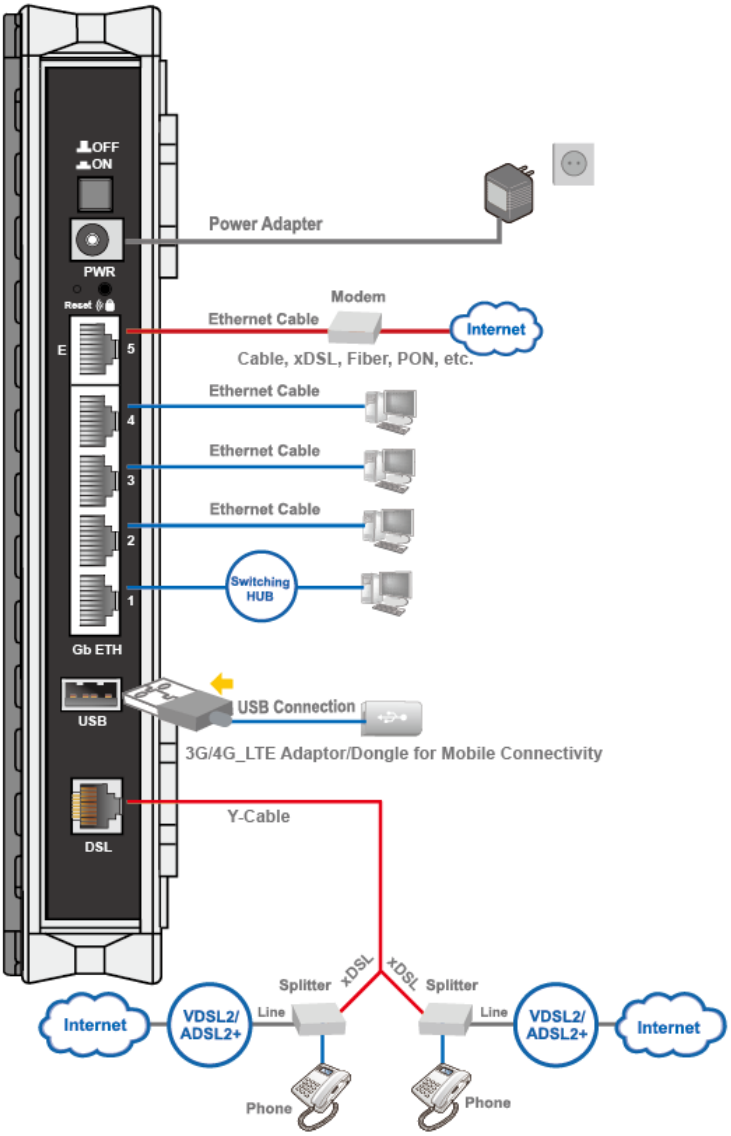
FTTH / Broadband Connection

The Ethernet 5 is an interchangeable LAN/WAN port. Refer to the User Manual to change this port to EWAN interface to connect with your Fiber, Cable, or xDSL modem.



Automatic WAN Failover

The automatic failover ensures uninterrupted operation and 24/7 Internet availability. When Primary WAN connection fails, the Secondary connection will back up the Internet connection seamlessly.



CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

Warning

- ✓ Do not use the router in high humidity or high temperature.
- ✓ Do not use same power source for the BEC 8920AC on other equipment.
- ✓ Do not open or repair the case yourself. If the device becomes too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.

Attention

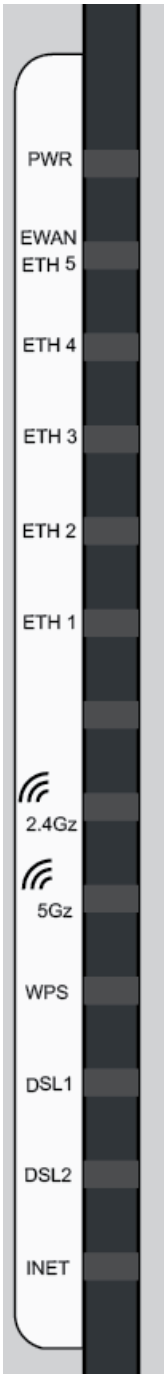
- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Package Contents

- ✓ BEC 8920ACS The Residential Gateway with 802.11ac * 1
- ✓ This Quick Installation Guide * 1
- ✓ CD containing User Manual * 1
- ✓ Vertical Stand * 1
- ✓ RJ-45 Ethernet Cable * 1
- ✓ Y-Cable for xDSL bonded operation * 1
- ✓ Detachable Antenna * 1
- ✓ Power adaptor * 1

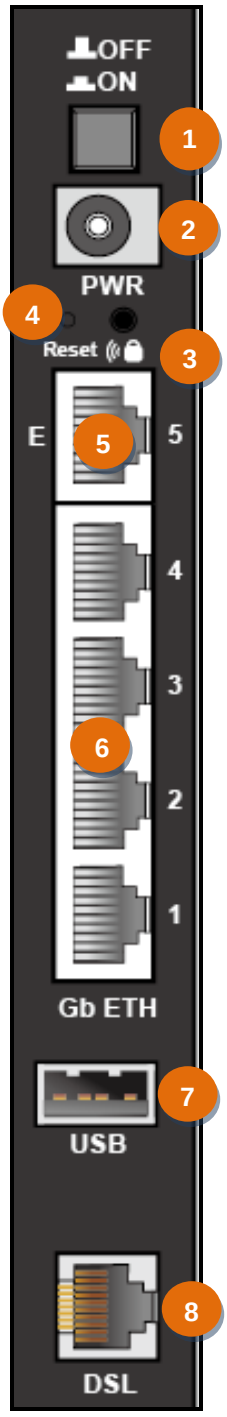
Device Description

Front Panel LEDs



LED	STATUS	DESCRIPTION
PWR (Power)	Red	System failure or in emergency mode
	Green	System is up and ready
	Off	Device has no power.
Gigabit EWAN / ETH 5 (Ethernet)	**Can be configured to be WAN port for broadband connectivity**	
	Green	**Ethernet LAN** : Connected to an Gigabit (1000Mbps) Ethernet device **Ethernet WAN**: Successfully connected with a broadband connection device
	Orange	LAN port is connected to an 10/100Mbps Ethernet device
	Blinking	Data being transmitted/received
	Off	No device is connected to the Ethernet port
Gigabit ETH 1~4 (Ethernet)	Green	LAN port is connected to an 1000Mbps Ethernet device
	Orange	LAN port is connected to an 10/100Mbps Ethernet device
	Blinking	Data being transmitted/received
	Off	No device is connected to the Ethernet port
Wireless 2.4GHz / 5GHz	Green	Wireless connection established
	Blinking	Data being transmitted / received
	Off	Wireless being turned off
WPS	Green	Wireless device(s) being connected successfully via WPS mode
	Blinking	WPS is enabled and trying to establish a WPS connection.
	Off	WPS being turned off
DSL1 / DSL2	Green	Successfully connected to an ADSL DSLAM (Line Synced).
	Off	DSL cable is unplugged
INET (Internet)	Green	IP received and traffic is passing thru the device.
	Blinking	Data being transmitted / received
	Red	BEC 8920AC is unable to get a public (WAN) IP address
	Off	BEC 8920AC is either in bridged mode or WAN (DSL) connection is not ready

Rear Panel Connectors



PORT	MEANING
1. **Power ON/OFF**	Power ON/OFF switch
2. **PWR (Power)**	Connect the supplied Power Adapter to this port.
3. **WPS / Wi-Fi On/Off**	By controlling the pressing time, users can achieve two different effects: **(1) WPS*: ** Press &hold the button for **less than 6 seconds** to trigger WPS function. **(2) Wireless ON/OFF button**: Press & hold the button for **more than 6 seconds** to On/Off the wireless. *** For detailed WPS configuration, please refer to the WPS section in this User Manual.**
4. **Reset**	Push and hold the reset button for five (5) seconds to restore to its factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
5. **E (Gb EWAN)**	Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable, for broadband connectivity. **Note: LAN 5 automatically becomes an EWAN port when EWAN internet interface is being selected in the GUI**
6. **Gb LAN Ethernet (1~5)**	Connect PCs, Laptops or any other office/home LAN devices with the supplied RJ-45 Ethernet cable (Cat-5 or Cat-5e) to any of the five LAN ports. **Note: Port 5 is a LAN / WAN Configurable Port.**
7. **USB**	Connect with a 3G or 4G/LTE USB adaptor/dongle for mobile connectivity.
8. **DSL**	Connect the device to an ADSL/VDSL telephone jack or splitter using a RJ-11 telephone cable / Y-Cable for xDSL bonded

Hardware Installation

1. Attach the Vertical Stand to the 8920AC

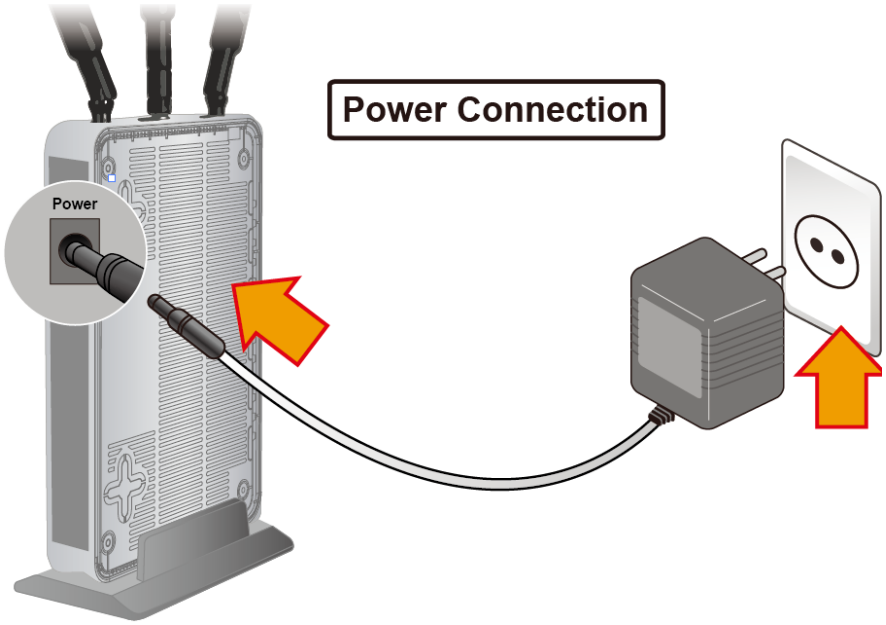
Setup your 8920AC in a vertical position using the stand provided in the package and place it on a stable surface for proper operation.

To correctly insert the vertical stand to the 8920AC, left up the router with PWR (Power LED) facing upward then slide it into the stand by attaching the wider side of the vertical stand to the top casing (BEC Logo) and shorter side on the back of the 8920AC

.

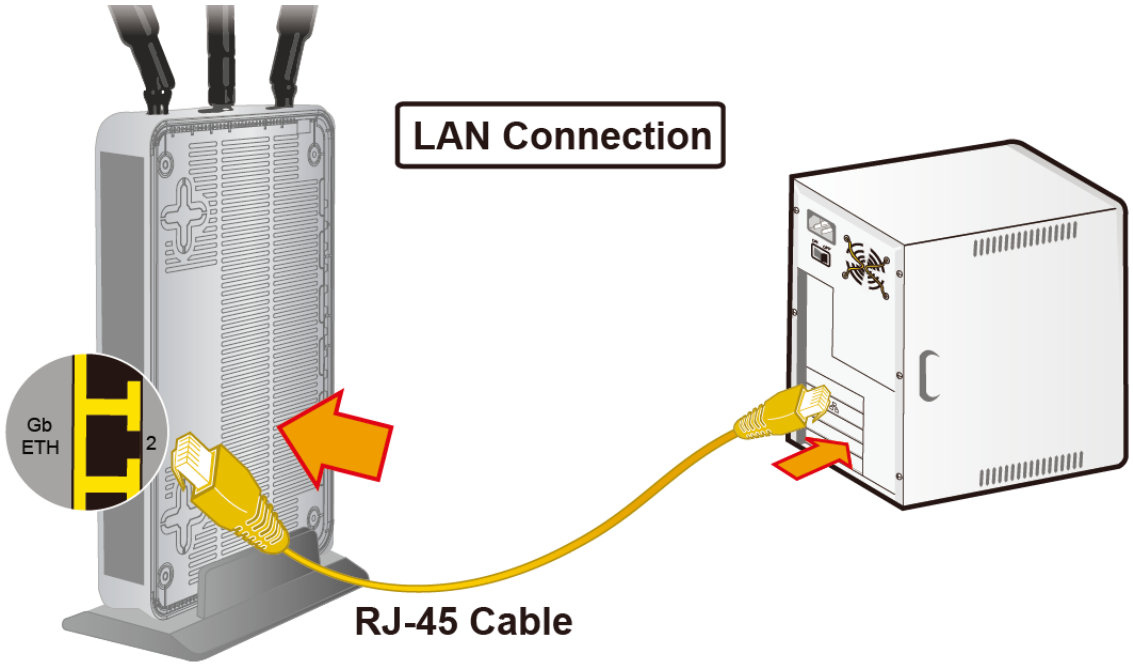
2. Power Connection

Plug in the supplied power adapter to the wall jack, the other side to the 8920AC then power **ON** the 8920AC by pressing the Power On/Off button.



3. LAN Connection

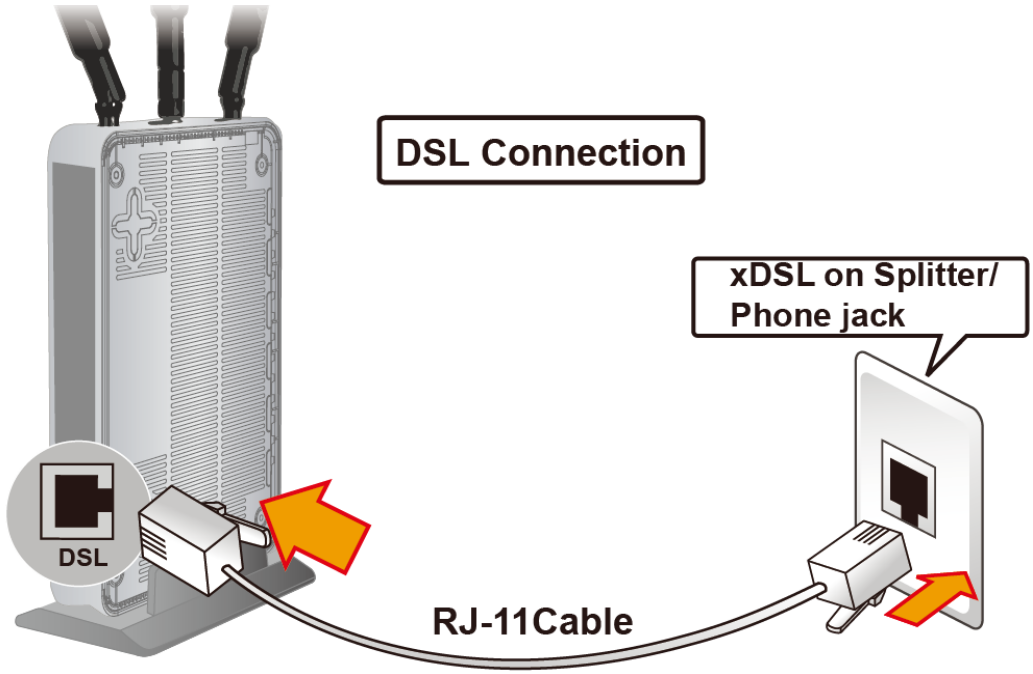
Connect the supplied RJ-45 Ethernet cable to one of the Ethernet ports, and the other side to the PC's Ethernet interface.



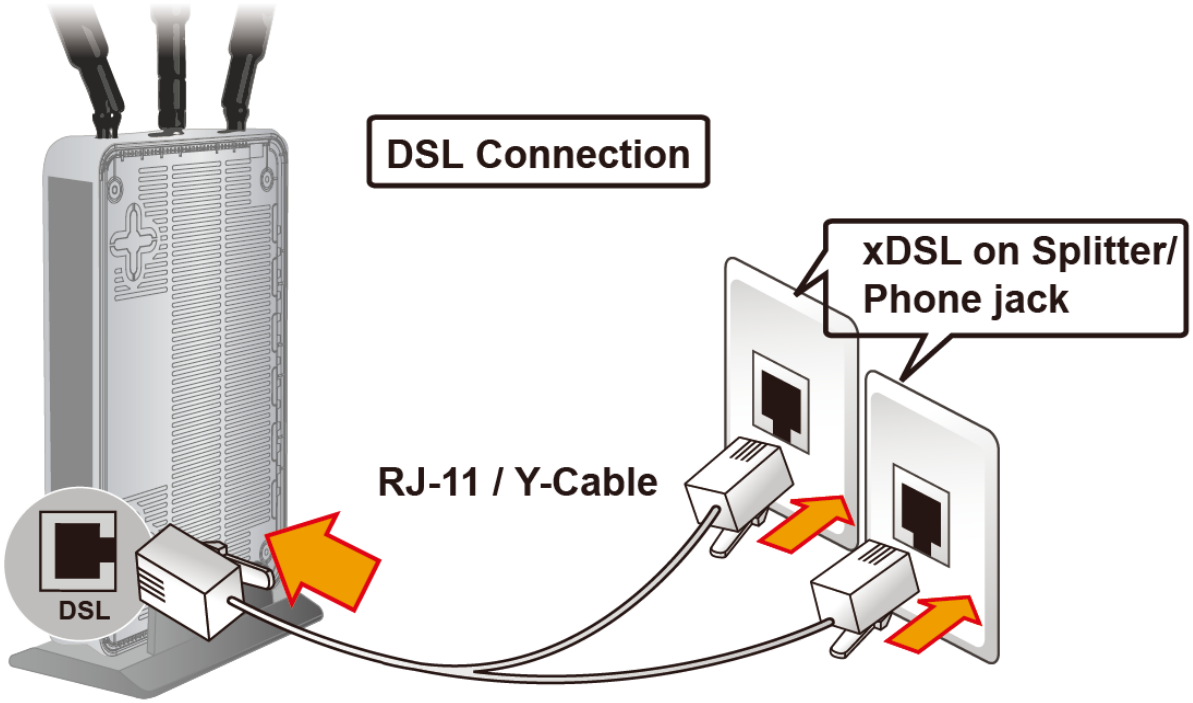
4. WAN Connection

4.1 xDSL Interface

For **single line xDSL**, please connect the supplied Y-Cable or a regular RJ-11 phone cable to the **DSL port** and the other side to the phone jack on the wall.

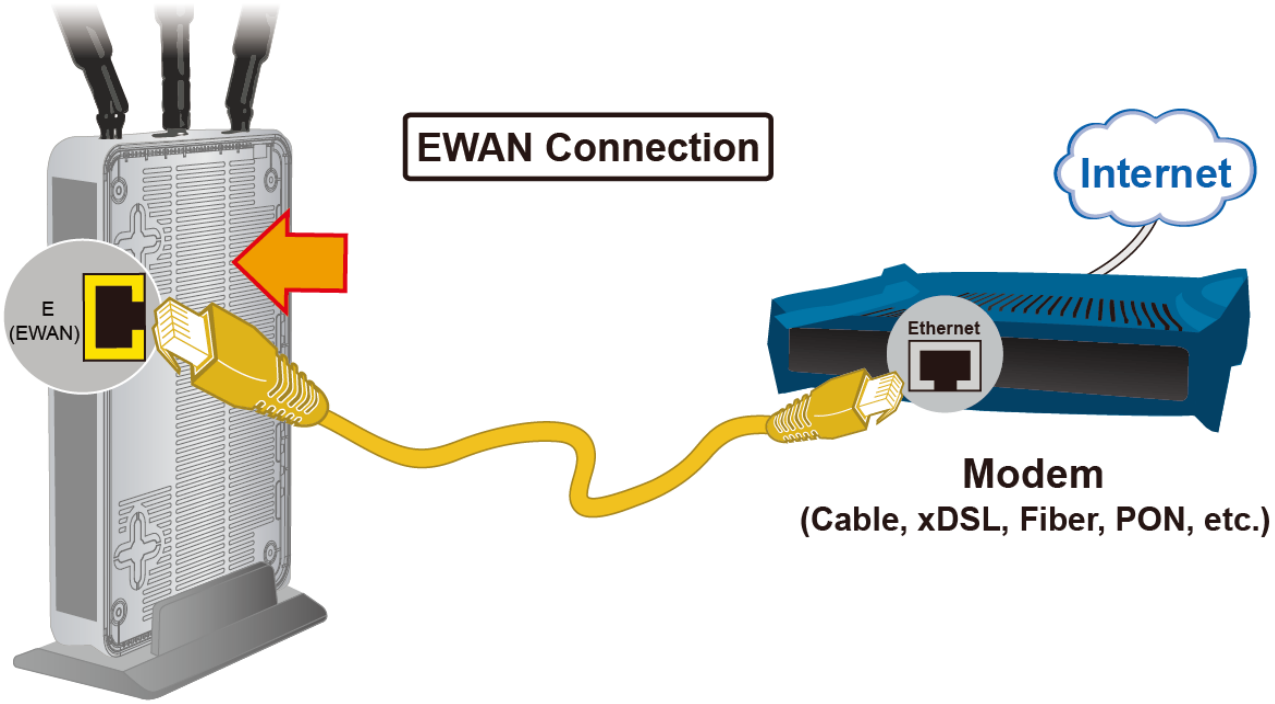


For **bonded xDSL**, please connect the supplied Y-cable to the **DSL port**, and the other two ends (both pairs) to the phone jacks on the wall.



4.2 EWAN Interface

Connect RJ-45 Ethernet cable to the **EWAN port**, and connect the other side to another alternative broadband device, such as Cable Modem, VDSL, Fiber Modem or PON optic lines. **<Please refer to User Manual for detailed instruction.>**



Cabling

The most common problem associated with Ethernet is bad cabling. Check the LAN and WAN LEDS to see if they are lit and make sure that all connected devices are turned on and cables are connected properly. Please contact your Internet Service Provider for further support if problems persist.

Make sure a line filter is installed before connecting devices (e.g. telephones, fax machines, analogue modems) to the telephone line on the wall socket (unless you are using a Central Splitter or

Central Filter installed by a qualified and licensed electrician). Missing or wrong installation of a line filter can cause xDSL frequent disconnection.

If you have a back-to-base alarm system, please consult with your Security provider to see if any necessary changes are required.

CHAPTER 3: BASIC INSTALLATION

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows 98 / NT /2000 / XP / ME / 7 / Vista, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed or configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

Any TCP/IP capable workstation can be used to communicate with or through the **BEC 8920AC**. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

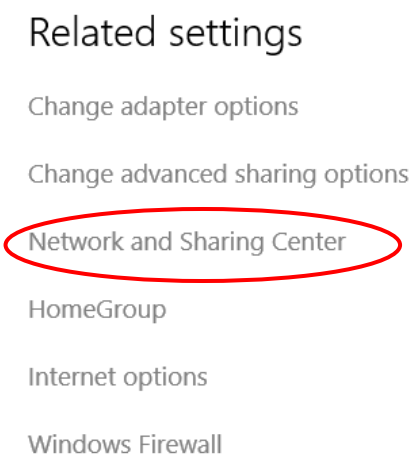
Configuring PC in Windows 10 (IPv4)

1. Click .

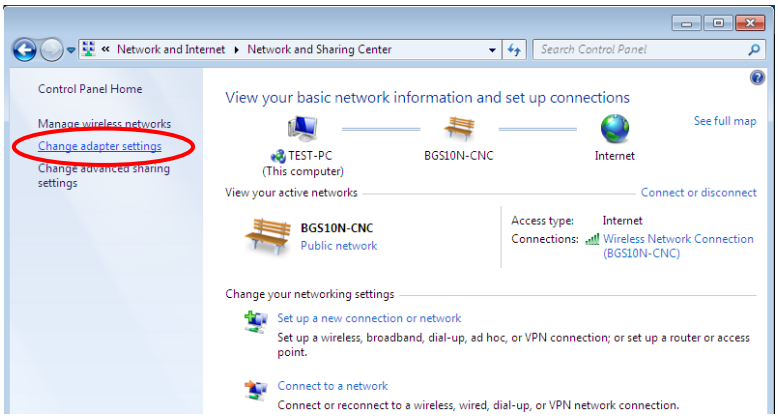
2. Click Settings

3. Then click on **Network and Internet**.

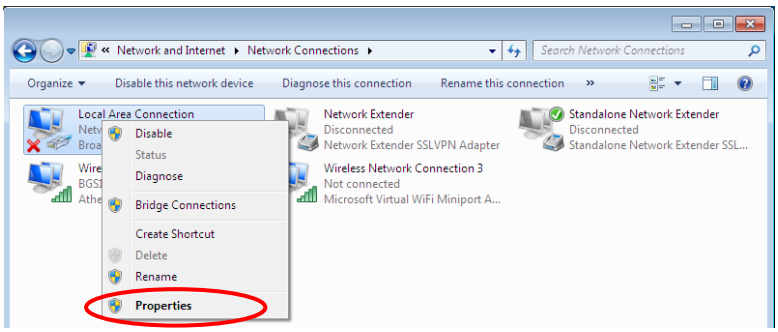
4. Under **Related settings,** select **Network and Sharing Center**



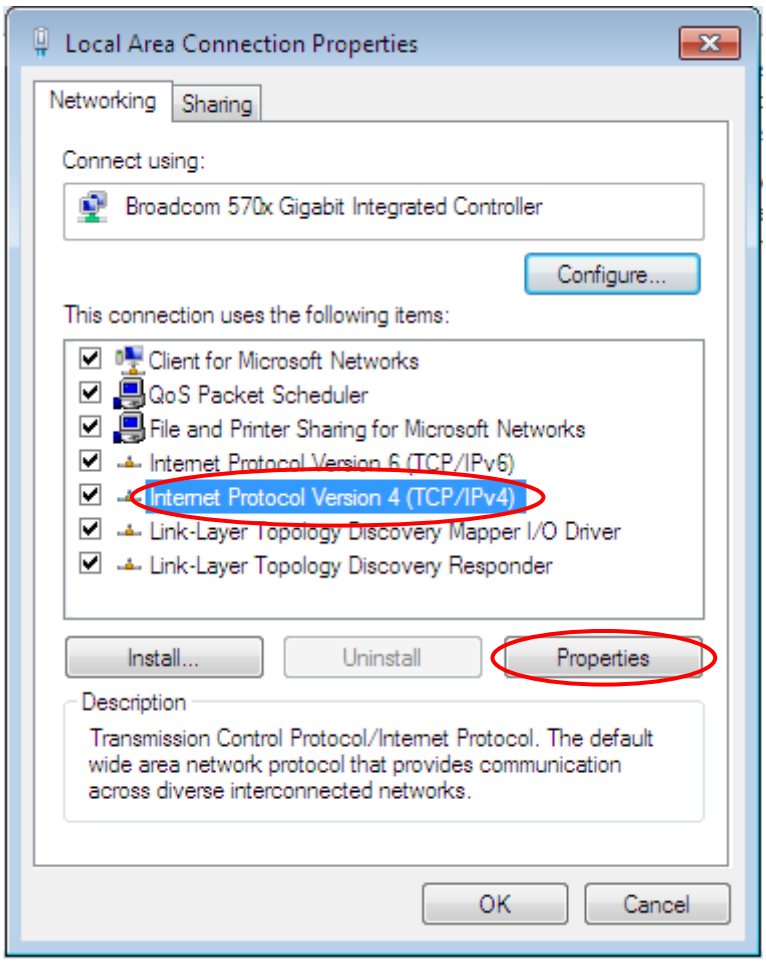
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



6. Select the **Local Area Connection**, and right click the icon to select **Properties**.

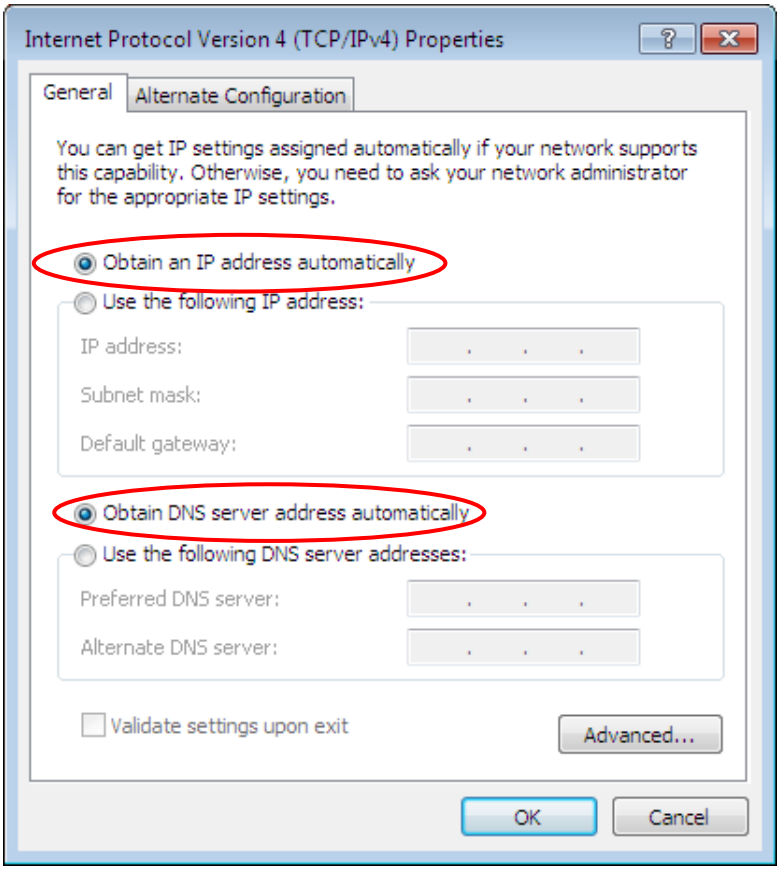


7. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



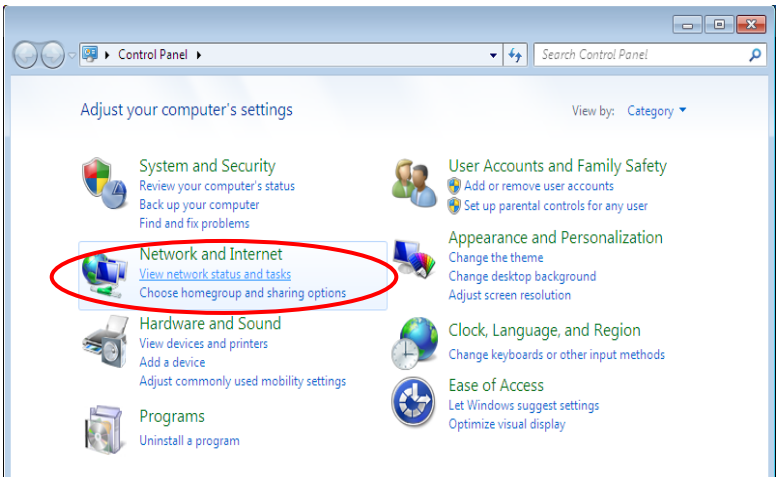
8. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



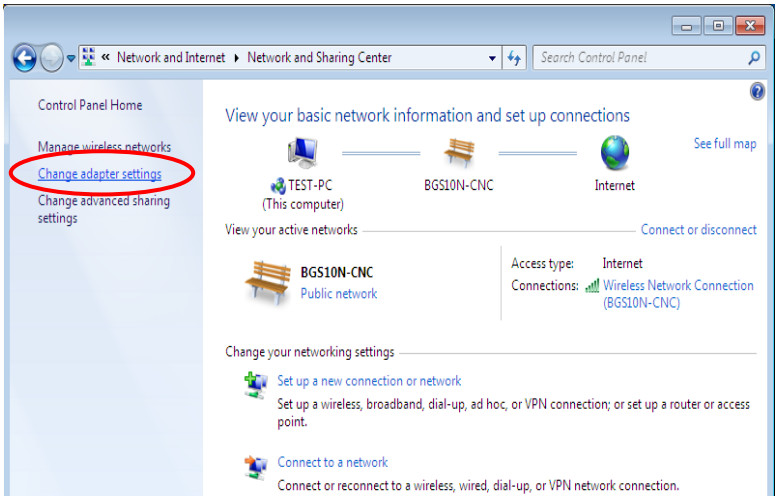
Configuring PC in Windows 7/8 (IPv4)

1. Go to **Start**. Click on **Control Panel**.

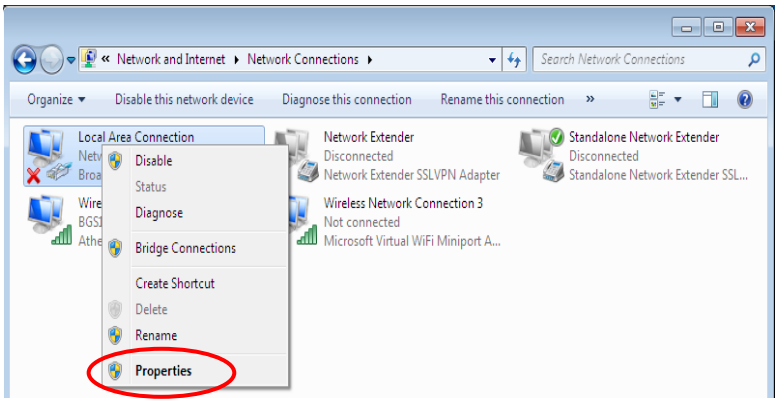


2. Then click on **Network and Internet**.

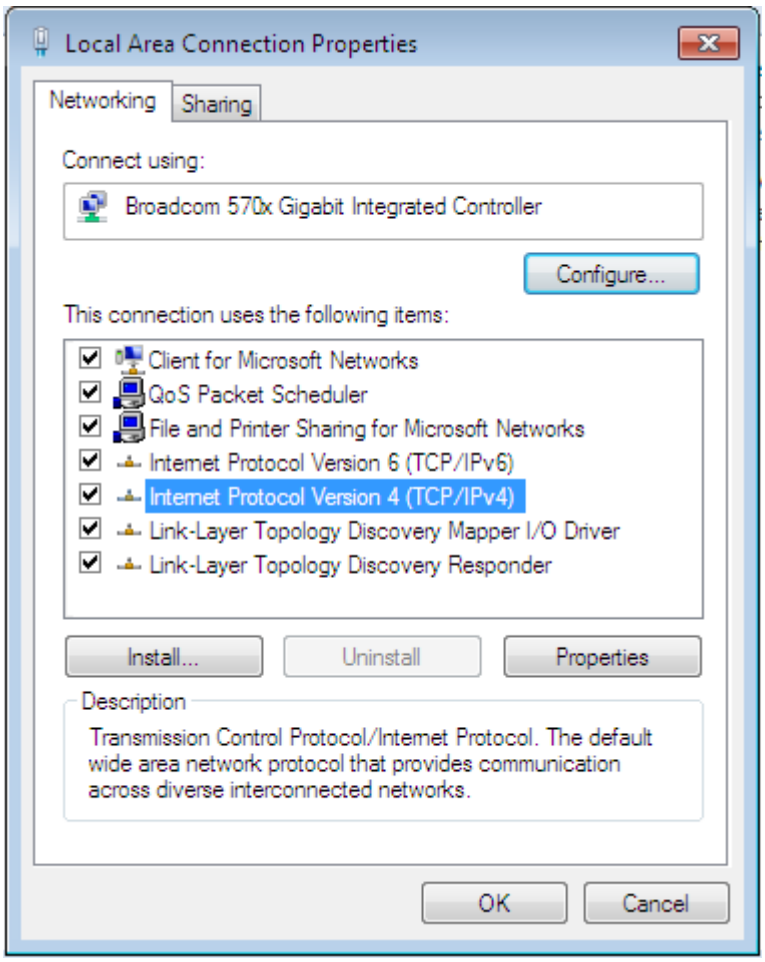
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



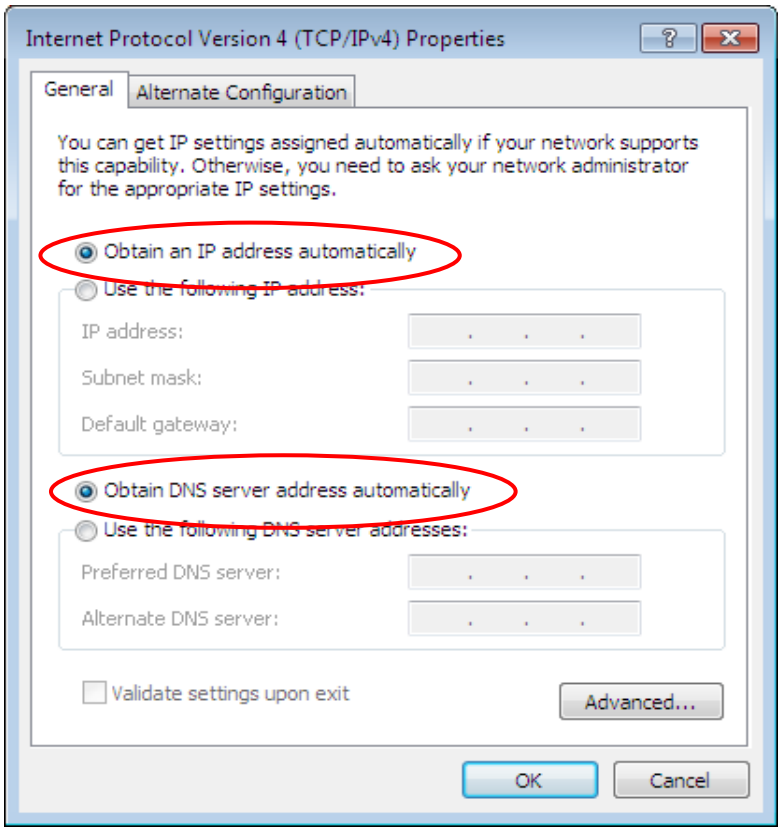
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

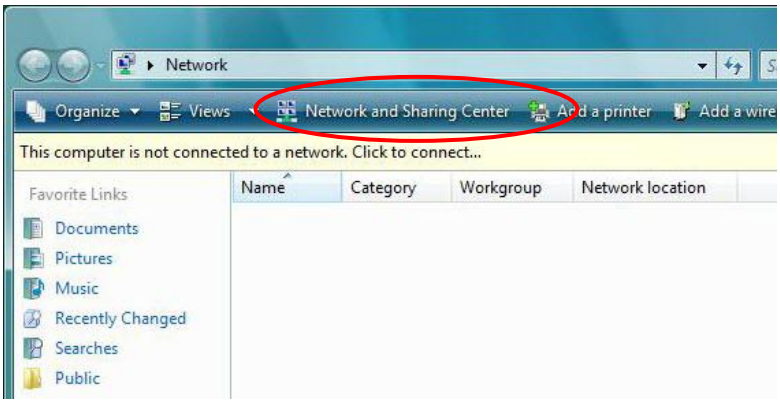


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

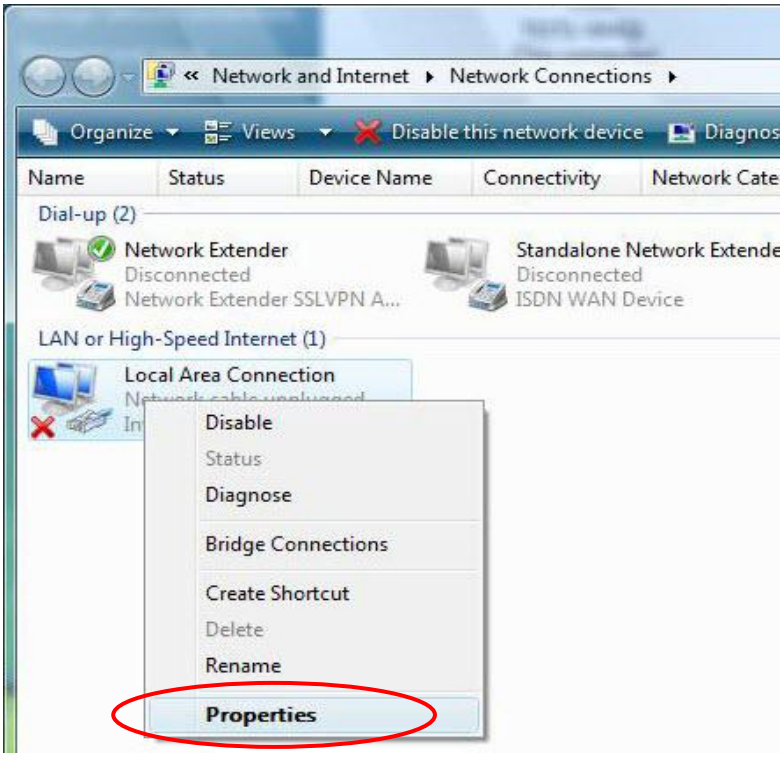
1. Go to **Start**. Click on **Network**.



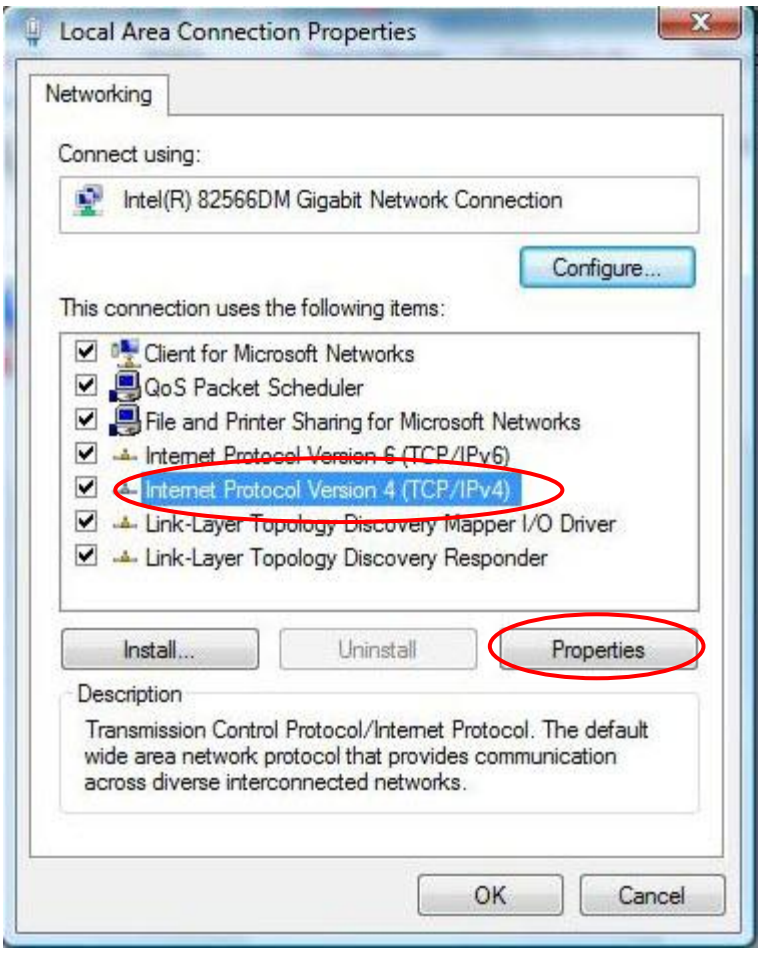
2. Then click on **Network and Sharing Center** at the top bar.

3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

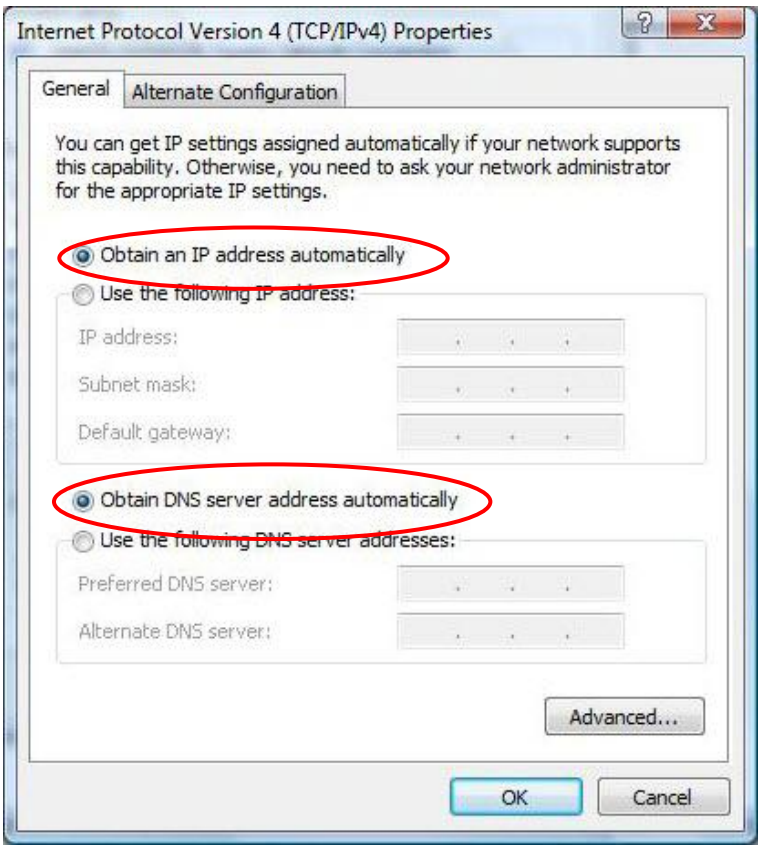


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



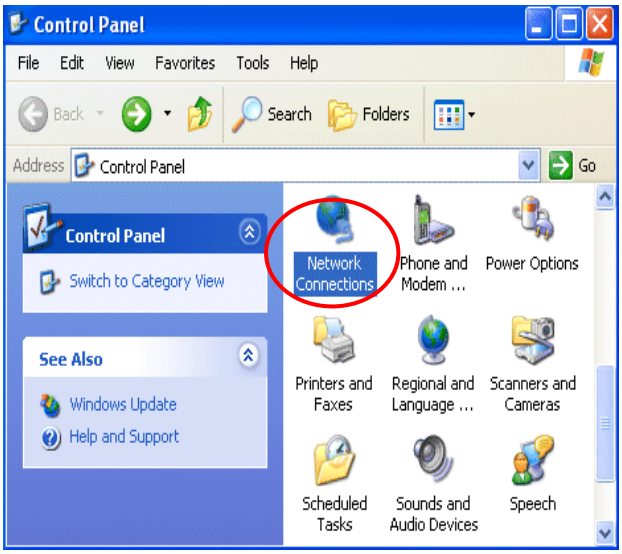
6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

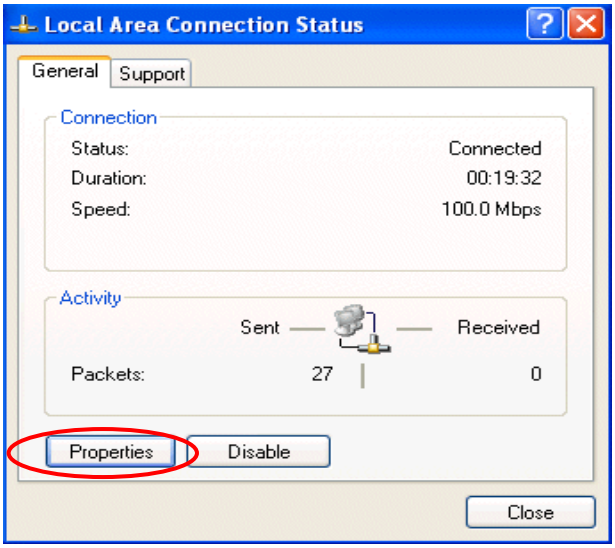


Configuring PC in Windows XP (IPv4)

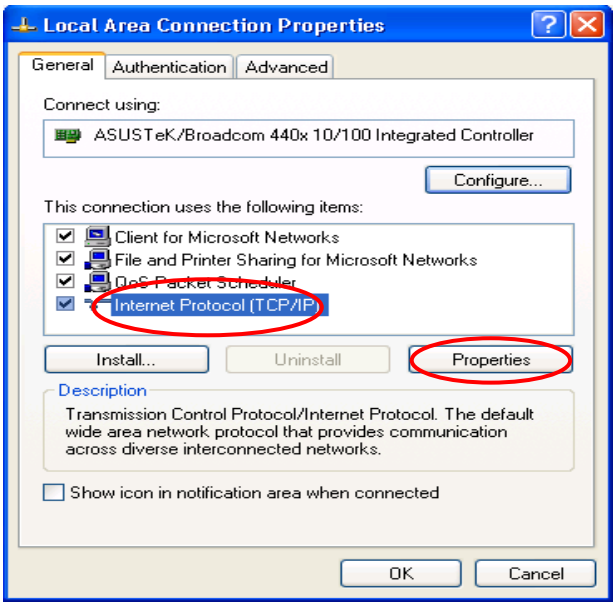
1. Go to **Start**. Click on **Control Panel.**
2. Then click on **Network and Internet**.



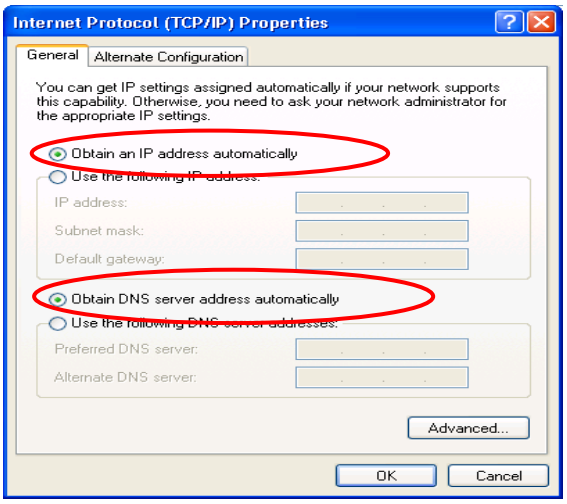
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.



6. Click **OK** to finish the configuration.

Network Configuration – IPv6

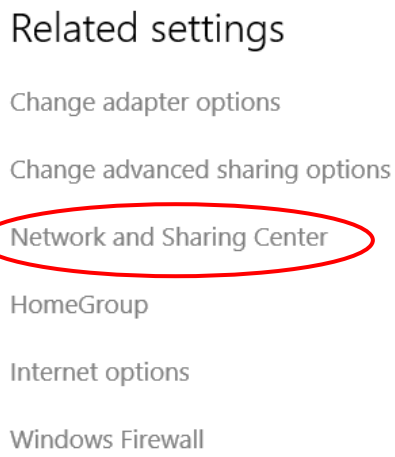
Configuring PC in Windows 10 (IPv6)

1. Click .

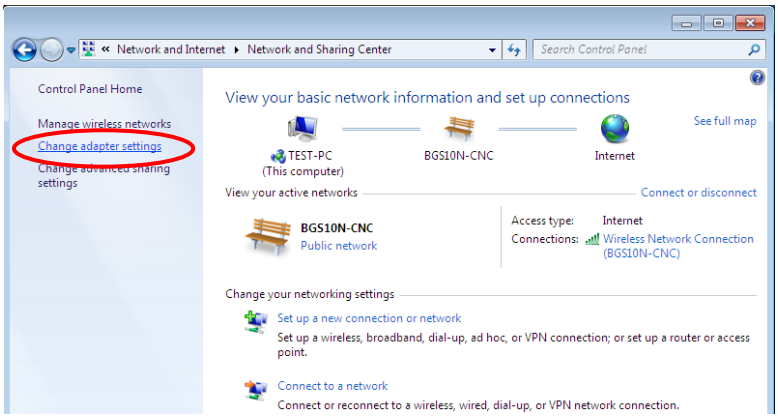
2. Click Settings

3. Then click on **Network and Internet**.

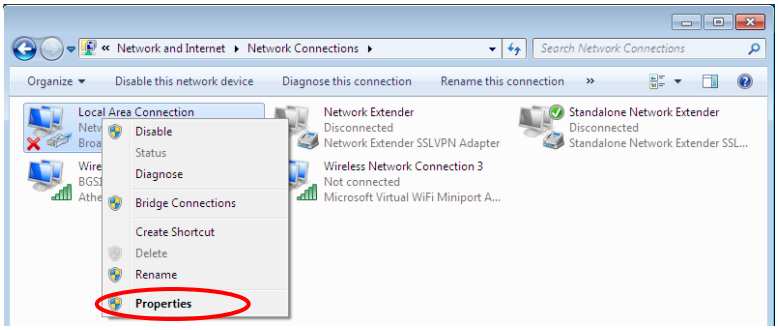
4. Under **Related settings,** select **Network and Sharing Center**



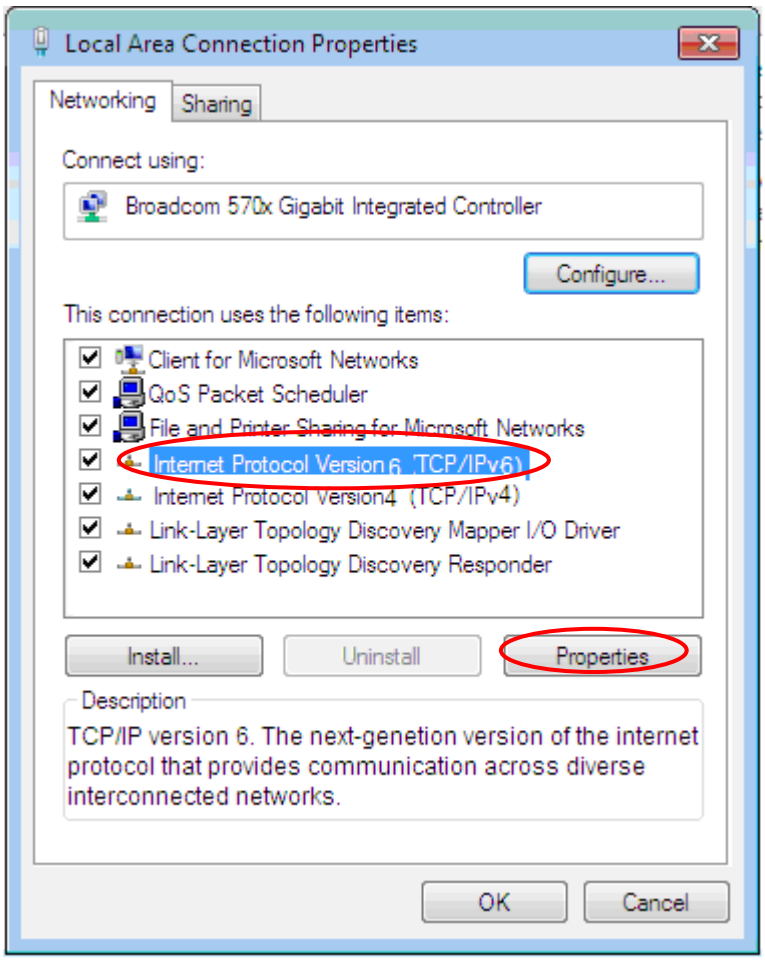
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



6. Select the **Local Area Connection**, and right click the icon to select **Properties**.

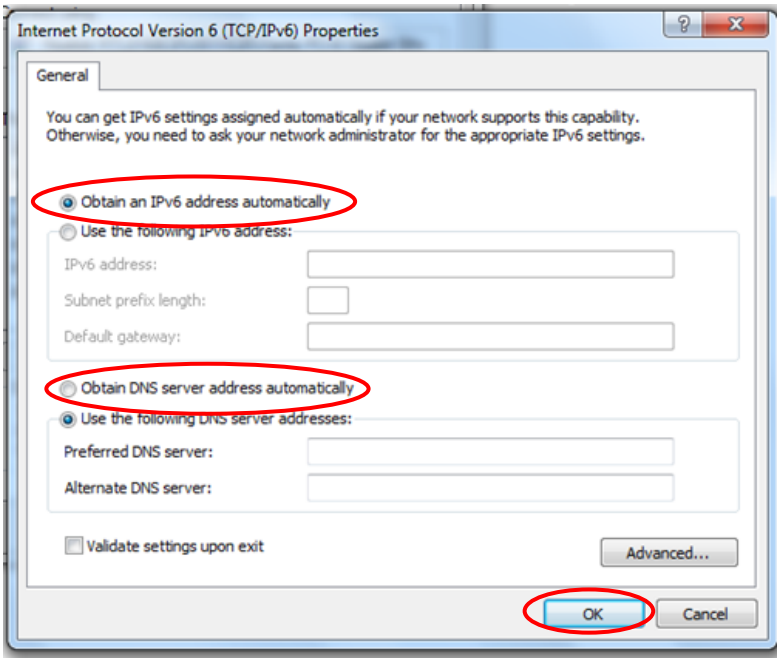


7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



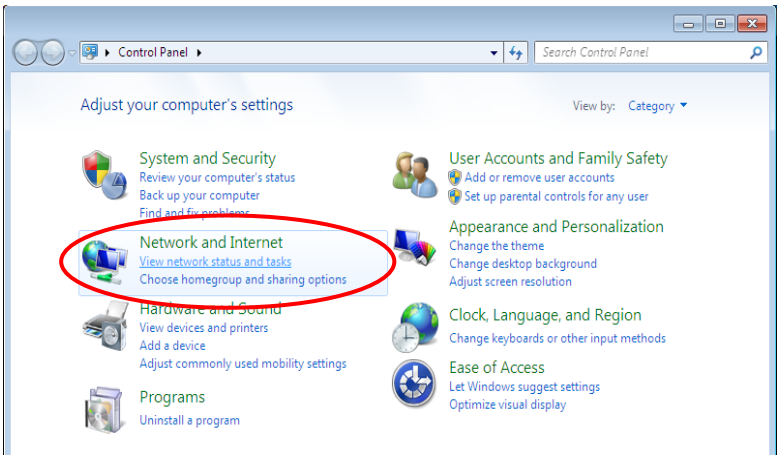
8. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



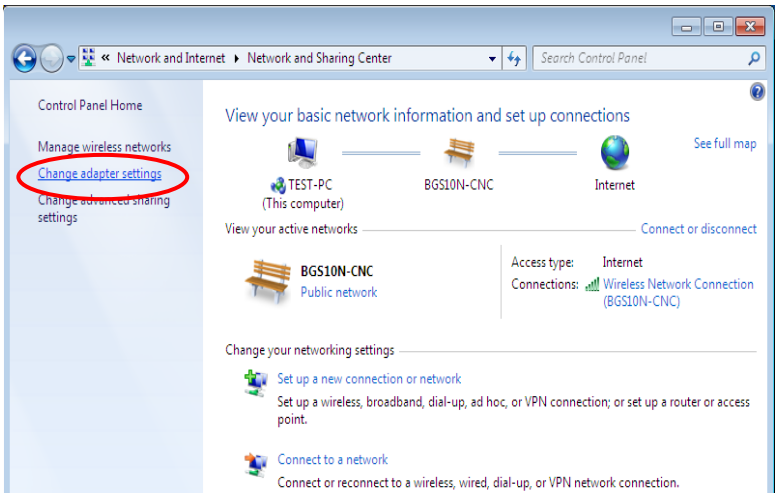
Configuring PC in Windows 7/8 (IPv6)

1. Go to **Start**. Click on **Control Panel**.

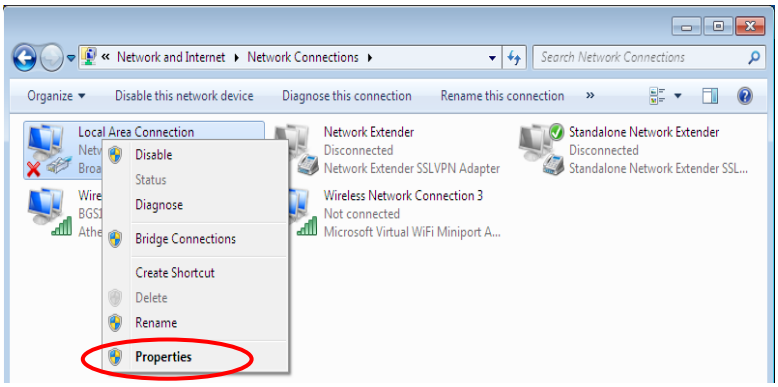


2. Then click on **Network and Internet**.

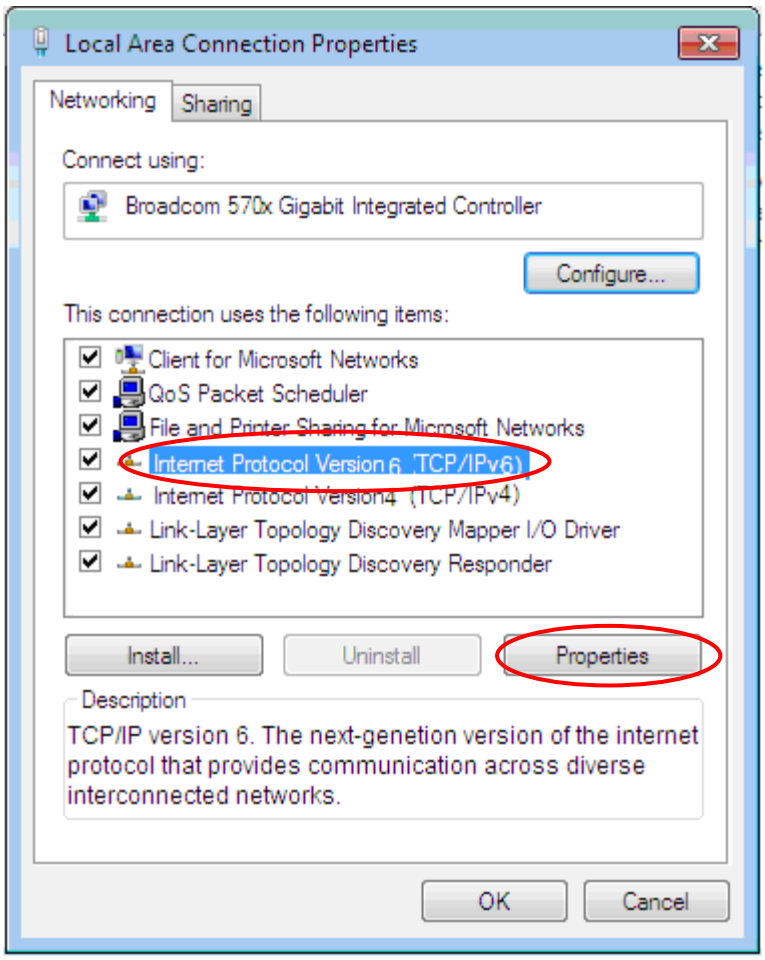
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

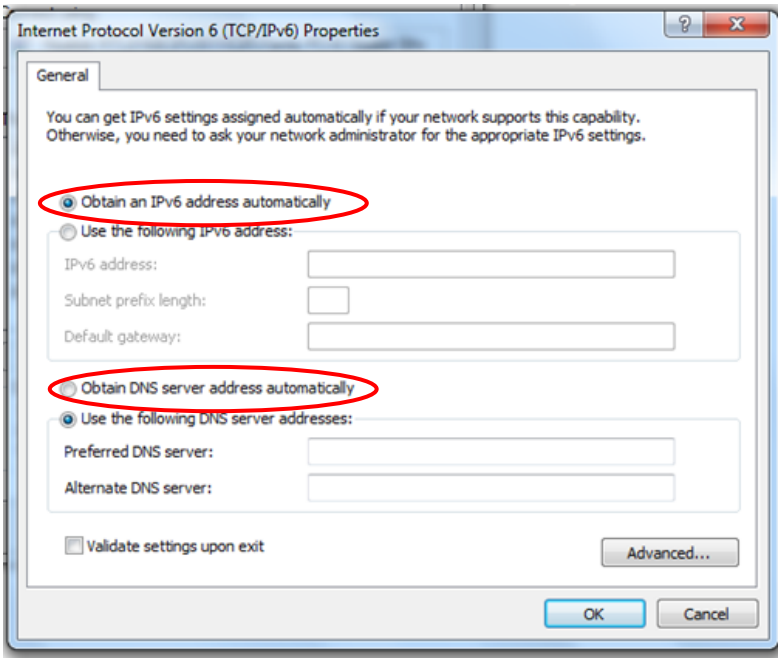


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

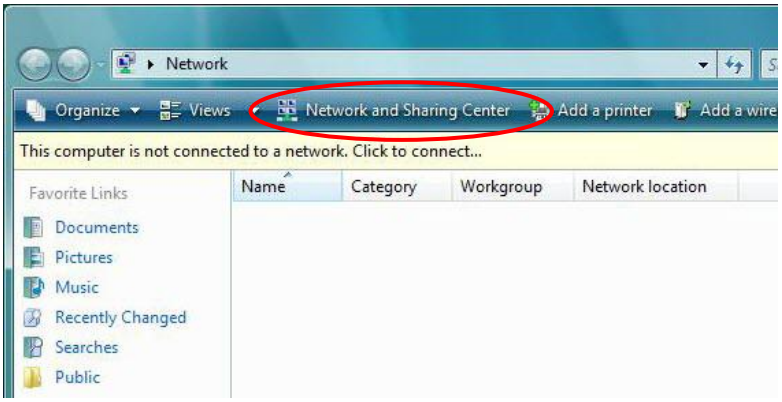
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



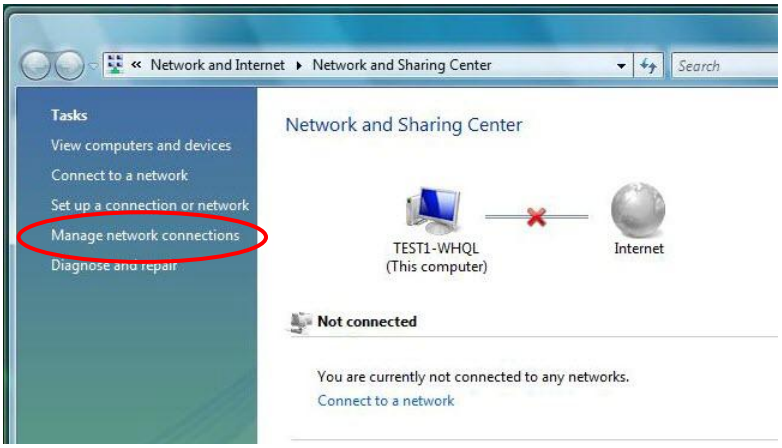
Configuring PC in Windows Vista (IPv6)

1. Go to **Start**. Click on **Network**.

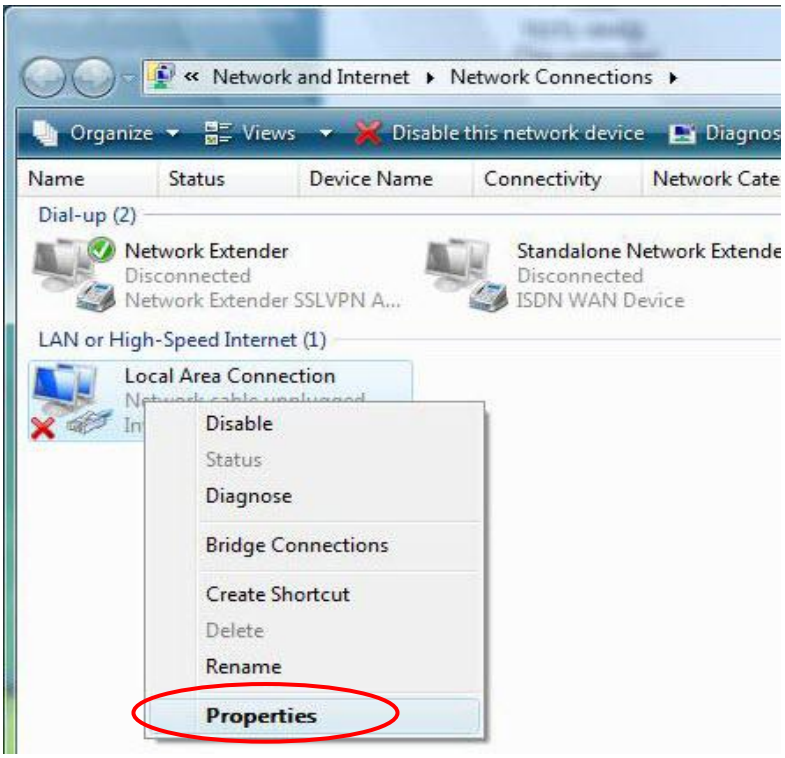
2. Then click on **Network and Sharing Center** at the top bar.



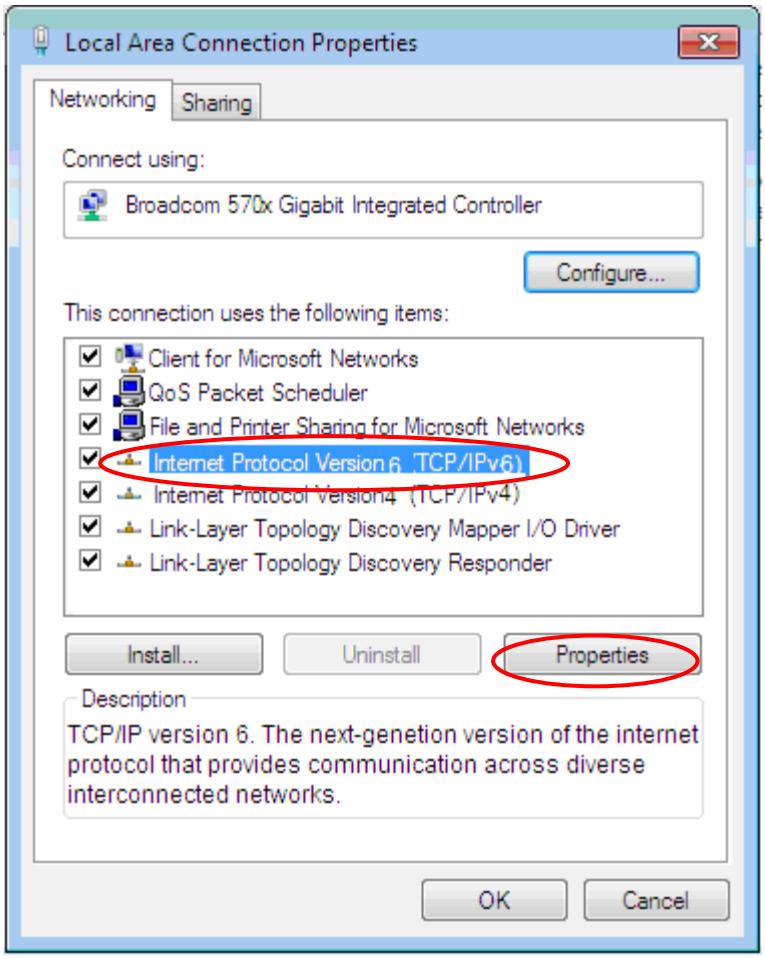
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

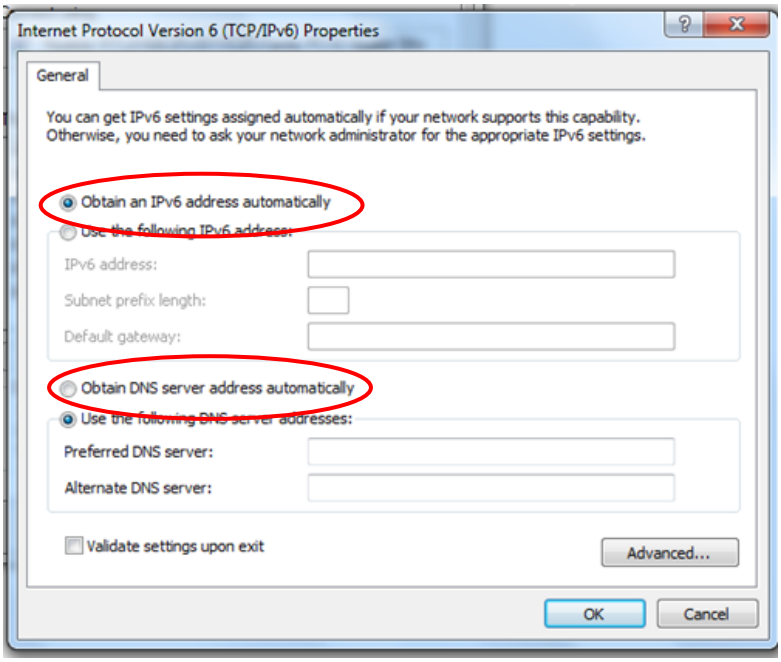


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



6. In the **TCP/IPv6 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

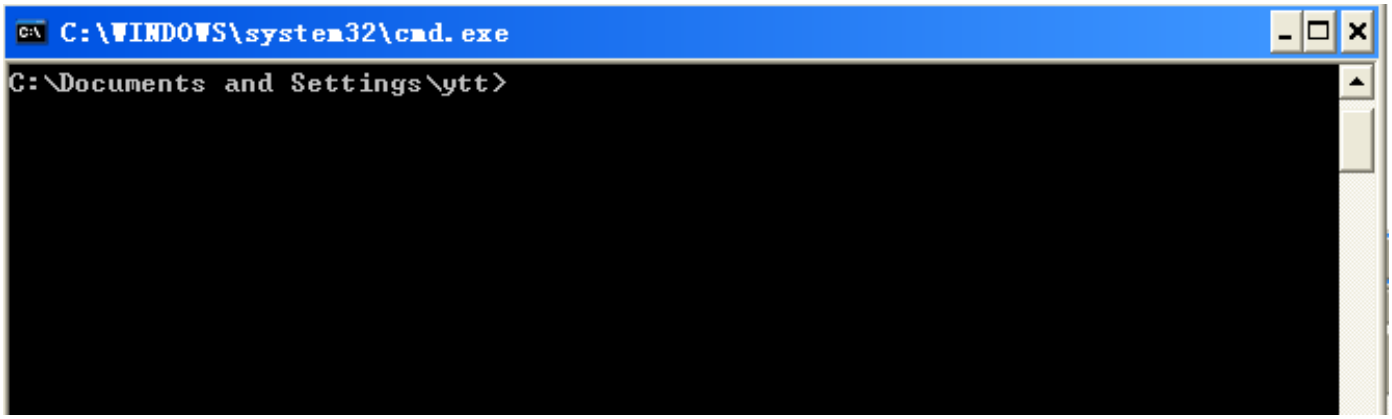


Configuring PC in Windows XP (IPv6)

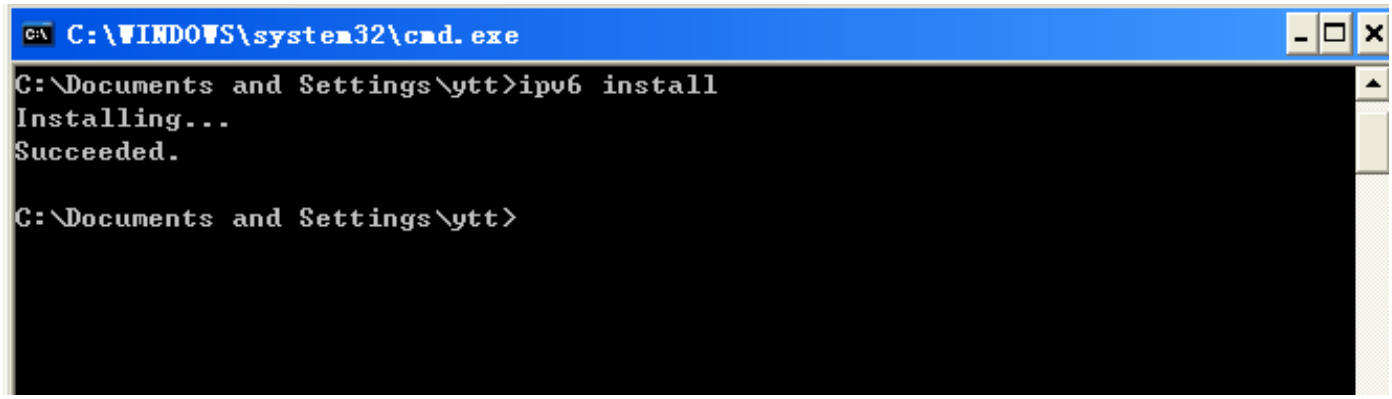
IPv6 is supported by Windows XP, but you need to install it first.

Please follow the steps to install IPv6:

1. On the Desktop, Click **Start** > **Run**, type **cmd**, then press **Enter** key in the keyboard, the following screen appears.



2. Key in command **ipv6 install**



Installation of IPv6 is now completed. Test it to see if it can work.

Default Settings

Before configuring the router, you need to know the following default settings.

Web Interface: (Username and Password)

- ✔ Username: admin
- ✔ Password: admin

The default username and password are "**admin**" and "**admin**" respectively.

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IPv4 Settings

- ✔ IP Address: 192.168.1.254
- ✔ Subnet Mask: 255.255.255.0

Device LAN IPv6 settings

- ✔ IPv6 Address / prefix: Default is a link-local address and is different from each other as MAC address is different from one to one.
- ✔ For example: fe80:0000:0000:0000:0204:edff:fe01:0001 / 64, the prefix initiates by fe80::

DHCP IPv4 Server:

- ✔ DHCP server is enabled.
- ✔ Start IP Address: 192.168.1.100
- ✔ IP pool counts: 100

Information from Your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of services are provided, such as PPPoE, Obtain an IP Address Automatically, Fixed IP address.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually)
PPPoA(RFC2364)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually)
Obtain an IP Address Automatically	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
Fixed IP Address	IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode

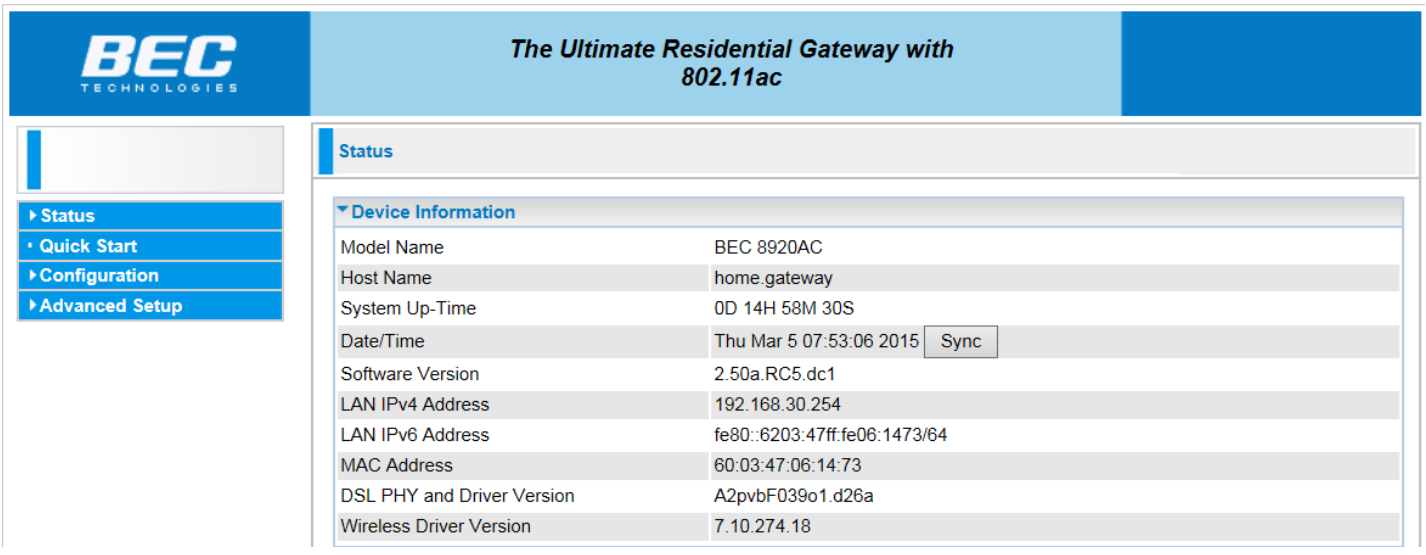
CHAPTER 4: CONFIGURING YOUR ROUTER

Login to Your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click "**Go**", a user name and password window prompt appears. Enter the user name and password that your administrator has set for you then click **OK**.

The default username and password is **"admin"** and **"admin"** respectively for the **Administrator** account type. **NOTE: This username / password may vary by different Internet Service Providers.**

Congratulations! You have successfully logged on to your **BEC 8920AC.**



Once you have logged on to your 8920AC via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration	Advanced
Sub-Items	**Summary**		**LAN** - Ethernet - IPv6 Auoconfig - Interface Grouping	**Routing** - Default Gateway - Static Route - Policy Routing - RIP
	WAN		**Wireless 5G (wl0)/2.4G (wl1)** - Basic - Security - MAC Filter - Wireless Bridge - Advanced - Station Info - Schedule Control	**DNS** - DNS - Dynamic DNS - DNS Proxy - Static DNS
	Statistics - LAN - WAN Service - xTM - xDSL		**WAN** - WAN Service - Failover - DSL - DSL Bonding - SNR	**Static ARP**
	Bandwidth Usage - LAN - WAN Service		**System** - Internet Time - Firmware Upgrade - Backup / Update - Access Control - Mail Alert - SMS Alert - Configure Log	**UPnP**
	3G/4G LTE Status		**IP Tunnel** - IPv6 in IPv4 - IPv4 in IPv6	**Certificate** - Trusted CA
	Route		**Security** - IP Filtering Outgoing - IP Filtering Incoming - MAC Filtering - Block WAN Ping - Time Restriction - URL Filtering - Parental Control Provider	**Management** - SNMP Agent - TR-069 Client - HTTP Port - Remote Access - Mobile Networks - 3G/4G LTE Usage Allowance - Power Management - Time Schedule - Auto Reboot
	ARP		**Quality of Service** - Quality of Service QoS Port Shaping	**Multicast**
	DHCP		**NAT** - Exceptional Rule Group - Virtual Servers - DMZ Host - One-to-One NAT - Port Triggering - ALG	**Diagnostics** - Diagnostics Tools - Push Service - Diagnostics - Fault Management
	Log - System Log - Security Log		**Wake on LAN**	

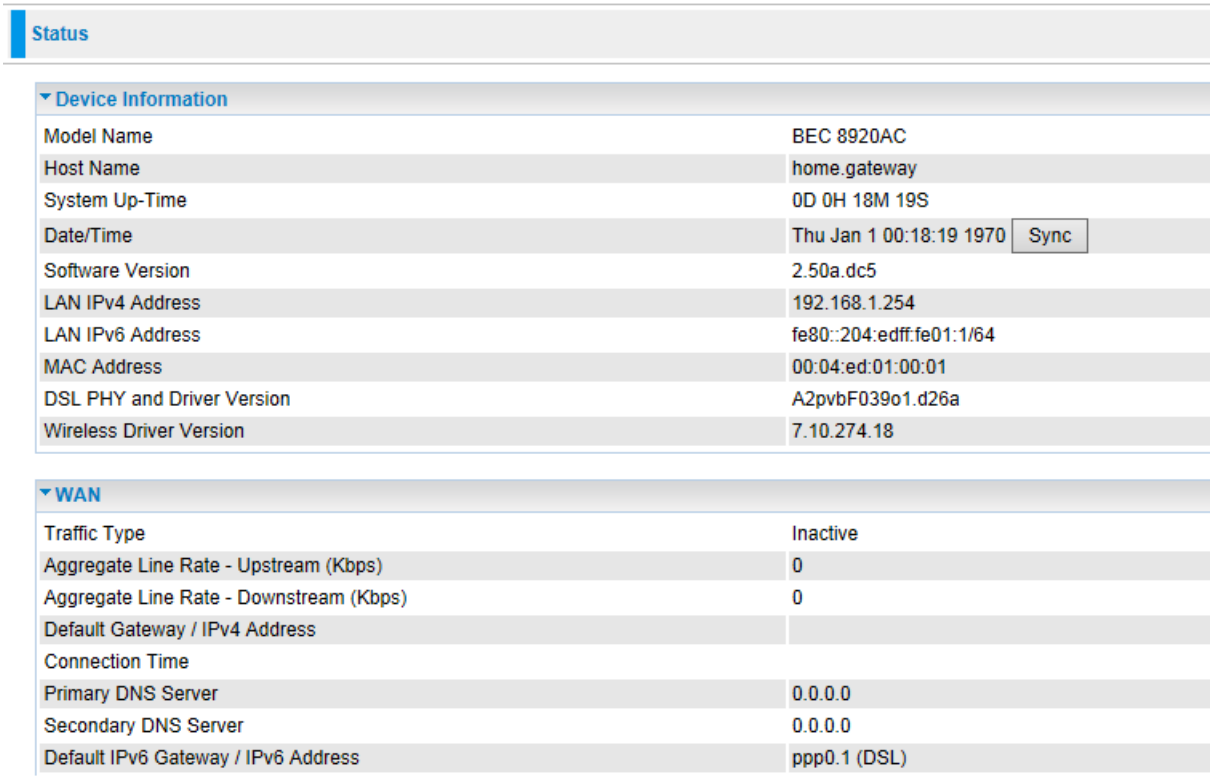
Please see the relevant sections of this manual for detailed instructions on how to configure your **BEC 8920AC** gateway router.

Status

This Section gives users an easy access to the information about the working router and access to view the current status of the router.

Summary

The basic information about the device is provided here (the following is a configured screenshots to let users understand clearly).



Device Information

Model Name: Provide a name for the router for identification purposes.

Host Name: Displays the name of the router.

System Up-Time: Display how long the BEC 8920AC has been powered on.

Date/Time: Setup correct time on the BEC 8920AC with your PC. Check on **Internet Time** for detailed configuration information.

Software Version: Software version currently loaded in the router

LAN IPv4 Address: Displays the LAN IPv4 address.

LAN IPv6 Address: Displays the LAN IPv6 address. Default is a Link-Local address, but when connects to ISP, it will display the Global Address, like above figure.

MAC Address: Displays the MAC address.

DSL PHY and Driver Version: Display DSL PHY and Driver version.

Wireless Driver Version: Displays wireless driver version.

WAN

Traffic Type:

Line Rate – Upstream (Kbps): Displays Upstream line Rate in Kbps.

Line Rate – Downstream (Kbps): Displays Downstream line Rate in Kbps.

Default Gateway / IPv4 Address: Displays selected default WAN interface and IP address.

Connection Time: Displays the elapsed time since the WAN connection is up.

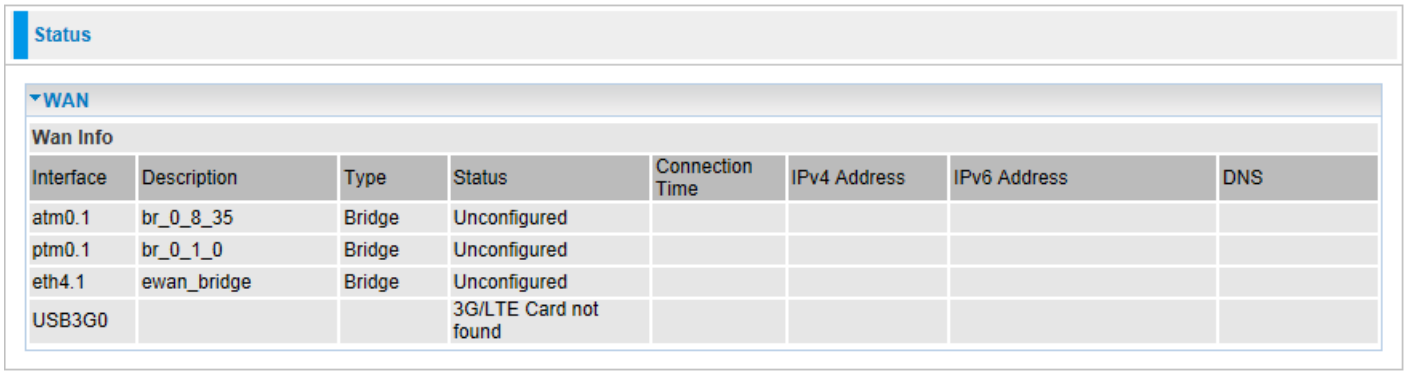
Primary DNS Server: Displays IPV4 address of Primary DNS Server.

Secondary DNS Server: Displays IPV4 address of Secondary DNS Server.

Default IPv6 Gateway / IPv6 Address: Displays IPv6 Gateway and WAN IP address.

WAN

The WAN Info screen displays the configured PVC(s) and the status.



Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
atm0.1	br_0_8_35	Bridge	Unconfigured				
ptm0.1	br_0_1_0	Bridge	Unconfigured				
eth4.1	ewan_bridge	Bridge	Unconfigured				
USB3G0			3G/LTE Card not found				

Interface: The WAN connection interface.

Description: The description of this connection.

Type: The protocol used by this connection.

Status: To disconnect or connect the link.

Connection Time: The WAN connection time since WAN is up.

IPv4 Address: The WAN IPv4 Address the device obtained.

IPv6 Address: The WAN IPv6 Address the device obtained.

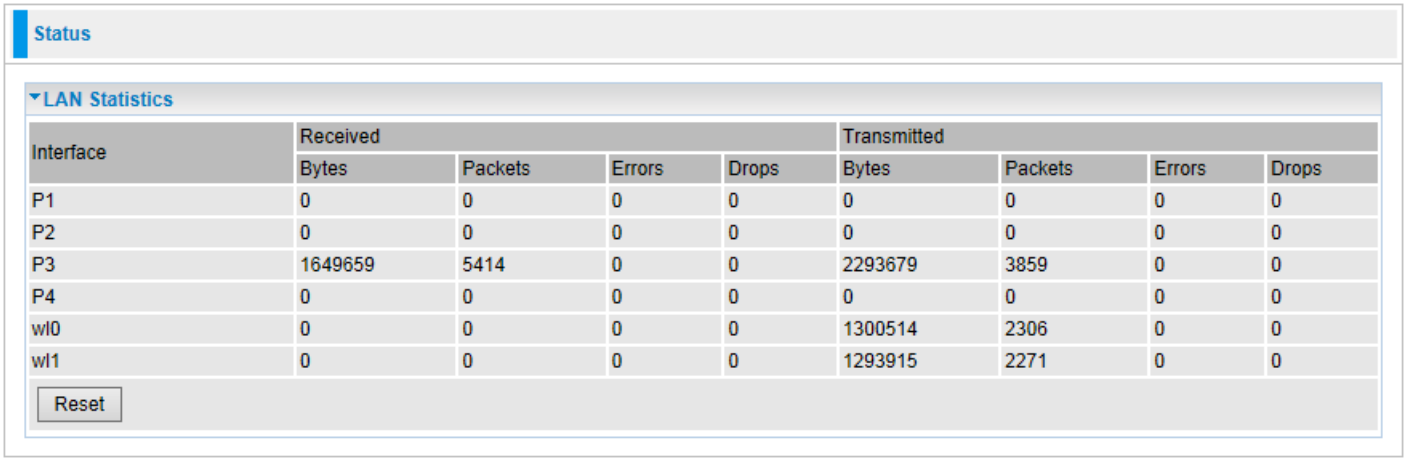
DNS: Display the used of DNS IP Address for each WAN Interface

Statistics

These are the items within the Statistics section: **LAN**, **WAN Service**, **xTM** and **xDSL**.

LAN

This screen shows interface statistics of Ethernet LAN interfaces.



Status

LAN Statistics

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P1	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0
P3	1649659	5414	0	0	2293679	3859	0	0
P4	0	0	0	0	0	0	0	0
wl0	0	0	0	0	1300514	2306	0	0
wl1	0	0	0	0	1293915	2271	0	0

Reset

Interface: List each LAN interface. P1-P4 indicates the four LAN interfaces.

Bytes: Display the Received and Transmitted traffic statistics in Bytes.

Packets: Display the Received and Transmitted traffic statistics in Packets.

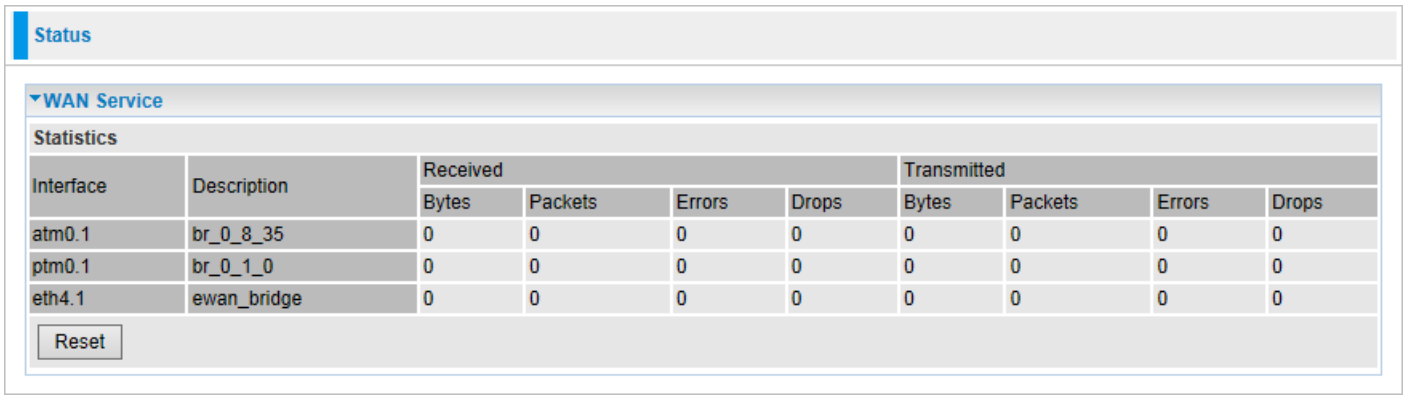
Errors: Display the statistics of errors arising in Receiving or Transmitting data.

Drops: Display the statistics of drops arising in Receiving or Transmitting data.

Reset: Press this button to refresh the statistics.

WAN

The table shows the statistics of WAN.



Status

WAN Service

Statistics

Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
atm0.1	br_0_8_35	0	0	0	0	0	0	0	0
ptm0.1	br_0_1_0	0	0	0	0	0	0	0	0
eth4.1	ewan_bridge	0	0	0	0	0	0	0	0

Reset

Interface: Shows connection interfaces.

Description: Shows the user defined name of WAN service.

Received/Transmitted Bytes: Rx/TX (receive/transmit) packet in Byte.

Received/Transmitted Pkts: Rx/TX (receive/transmit) packets.

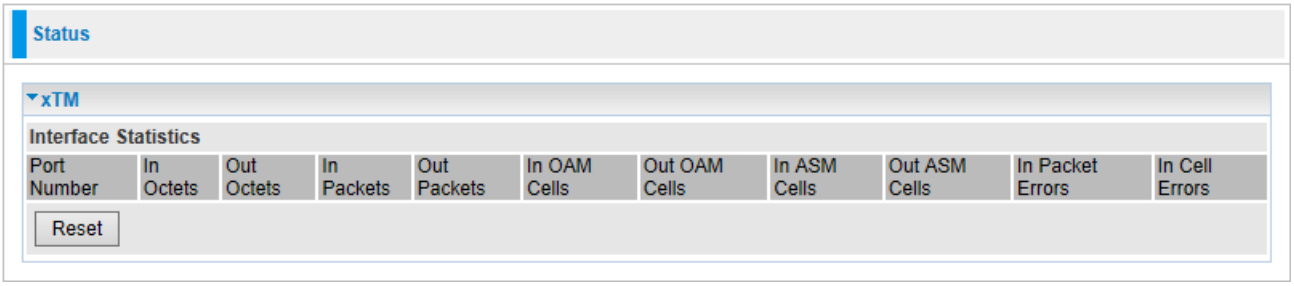
Received/Transmitted Errs: Rx/TX (receive/transmit) packets that are errors.

Received/Transmitted Drops: Rx/TX (receive/transmit) packets that are dropped.

Reset statistics: Click to update the statistics.

xTM

The Statistics-xTM screen displays all the xTM statistics



Port Number: Shows number of the port for xTM.

In Octets: Number of received octets over the interface.

Out Octets: Number of transmitted octets over the interface.

In Packets: Number of received packets over the interface.

Out Packets: Number of transmitted packets over the interface.

In OAM Cells: Number of OAM cells received.

Out OAM Cells: Number of OAM cells transmitted.

In ASM Cells: Number of ASM cells received.

Out ASM Cells: Number of ASM cells transmitted.

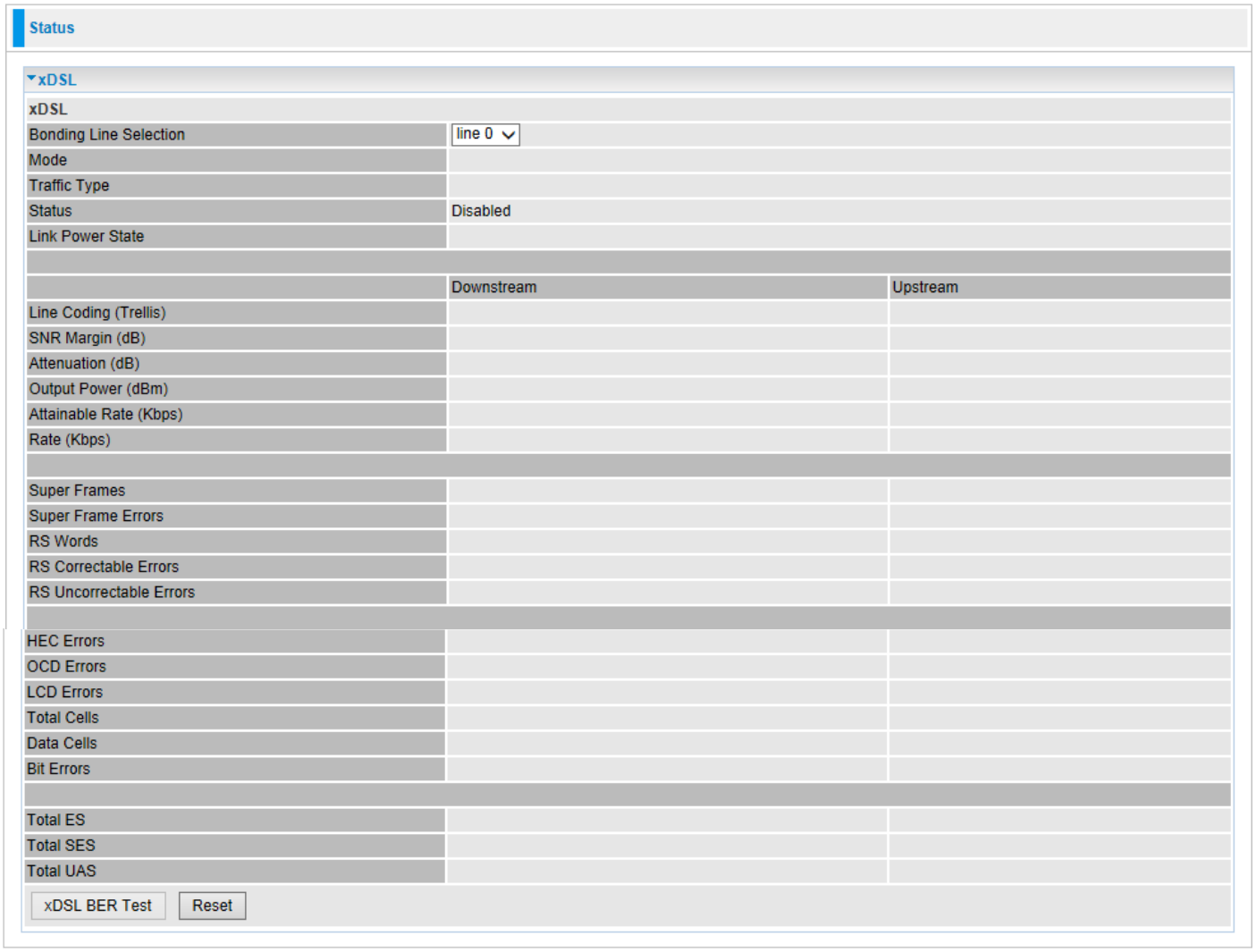
In Packet Errors: Number of received packets with errors.

In Cell Errors: Number of received cells with errors.

Reset: Click to reset the statistics.

xDSL

The Statistics-xDSL screen displays all the xDSL network statistics.



Mode: Modulation protocol, including G.dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM.

Traffic Type: transfer mode, here supports ATM and PTM.

Status: Show the status of DSL link.

Link Power State: Show link output power state.

Line Coding (Trellis): Trellis on/off.

SNR Margin (0.1 dB): show the Signal to Noise Ratio (SNR) margin.

Attenuation (0.1 dB): This is estimate of average loop attenuation of signal.

Output Power (0.1 dBm): show the output power.

Attainable Rate (Kbps): The sync rate you would obtain.

Rate (Kbps): show the downstream and upstream rate in Kbps.

K (number of bytes in DMT frame): show the number of bytes in DMT frame.

R (number of check bytes in RS code word): show the number of check bytes in RS code word.

S (RS code word size in DMT frame): show the RS code word size in DMT frame.

D (interleave depth): show the interleave depth.

Delay (msec): show the delay time in msec.

INP (DMT symbol): show the DMT symbol.

Super Frames: the total number of super frames.

Super Frame Errors: the total number of super frame errors.

RS Words: Total number of Reed-Solomon code errors.

RS Correctable Errors: Total number of RS with correctable errors.

RS Uncorrectable Errors: Total number of RS words with uncorrectable errors.

HEC Errors: Total number of Header Error Checksum errors.

OCD Errors: Total number of out-of-cell Delineation errors.

LCD Errors: Total number of Loss of Cell Delineation.

Total Cells: Total number of cells.

Data Cells: Total number of data cells.

Bit Errors: Total number of bit errors.

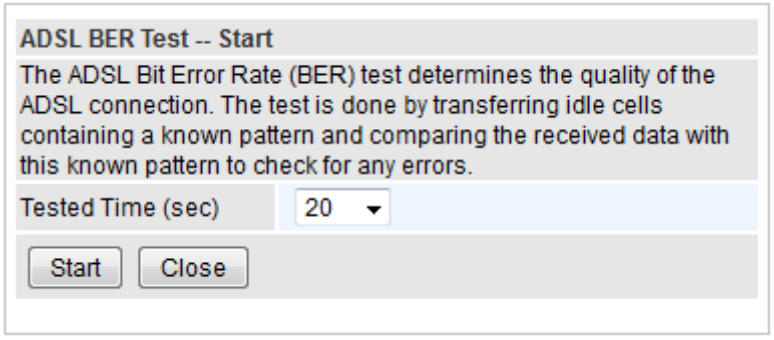
Total ES: Total Number of Error Seconds.

Total SES: Total Number of Severely Error Seconds.

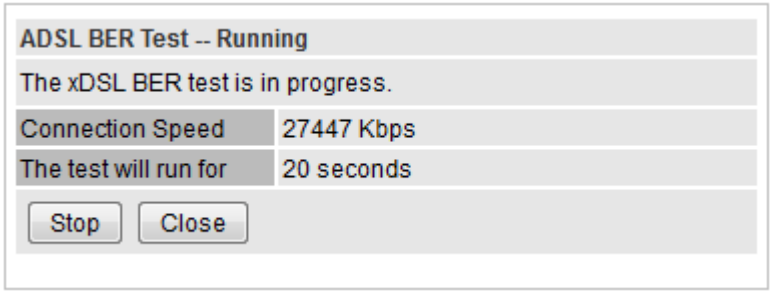
Total UAS: Total Number of Unavailable Seconds.

XDSL BER Test: The ADSL Bit Error Rate (BER) test checks the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern then comparing the received data with this known pattern to check for any errors.

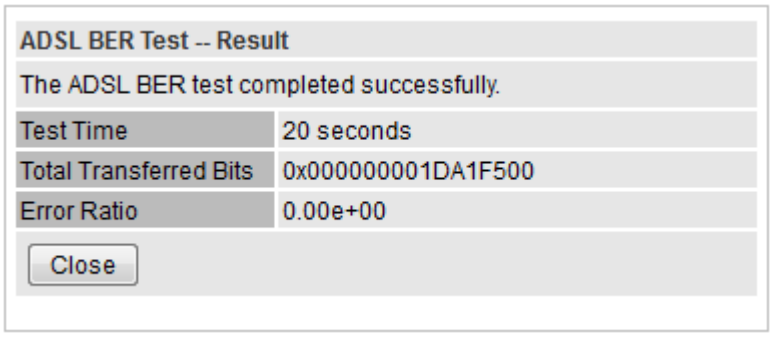
Pick a Tested Time in seconds; click **Start** to start the test.



Testing is still in process.



When completed, the test result window will appear. You can review the quality of your xDSL connection.



Reset: Click this button to reset the statistics.

Bandwidth Usage

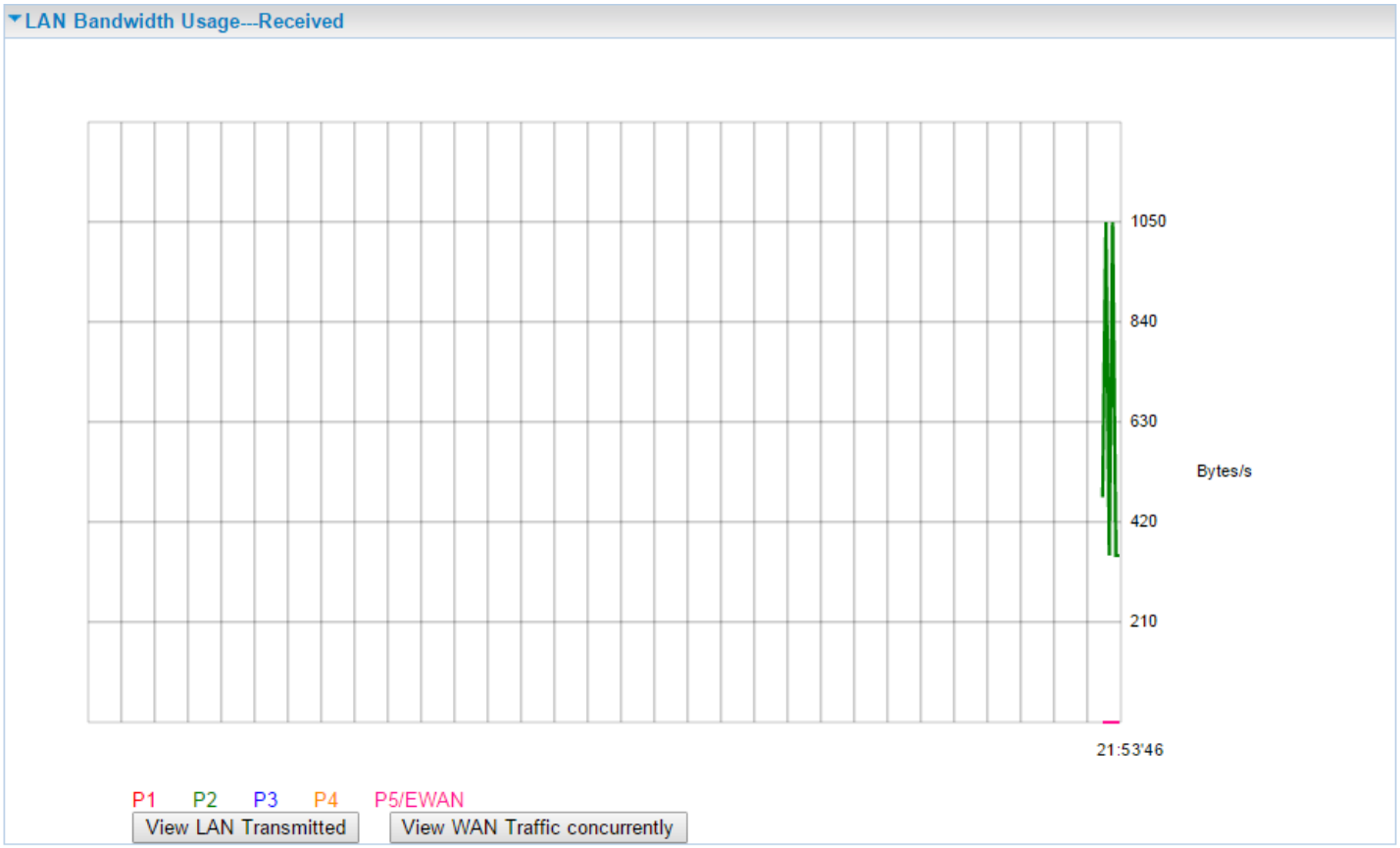
Collecting WAN bandwidth usage data and displaying in a clear graphic with numeric, in Bytes per second, utilization of received / transmit of the WAN Interface. You can see how much Internet bandwidth is being used to transmit data send over to and receive data from the Internet.

LAN and WAN Bandwith Usage

View LAN Bandwidth Usage - Received

Current diagram shows total received data by all network devices.

LAN #5 is LAN/WAN configurable. When P5 is used for Broadband access, P5/EWAN interface will not appear on the screen.

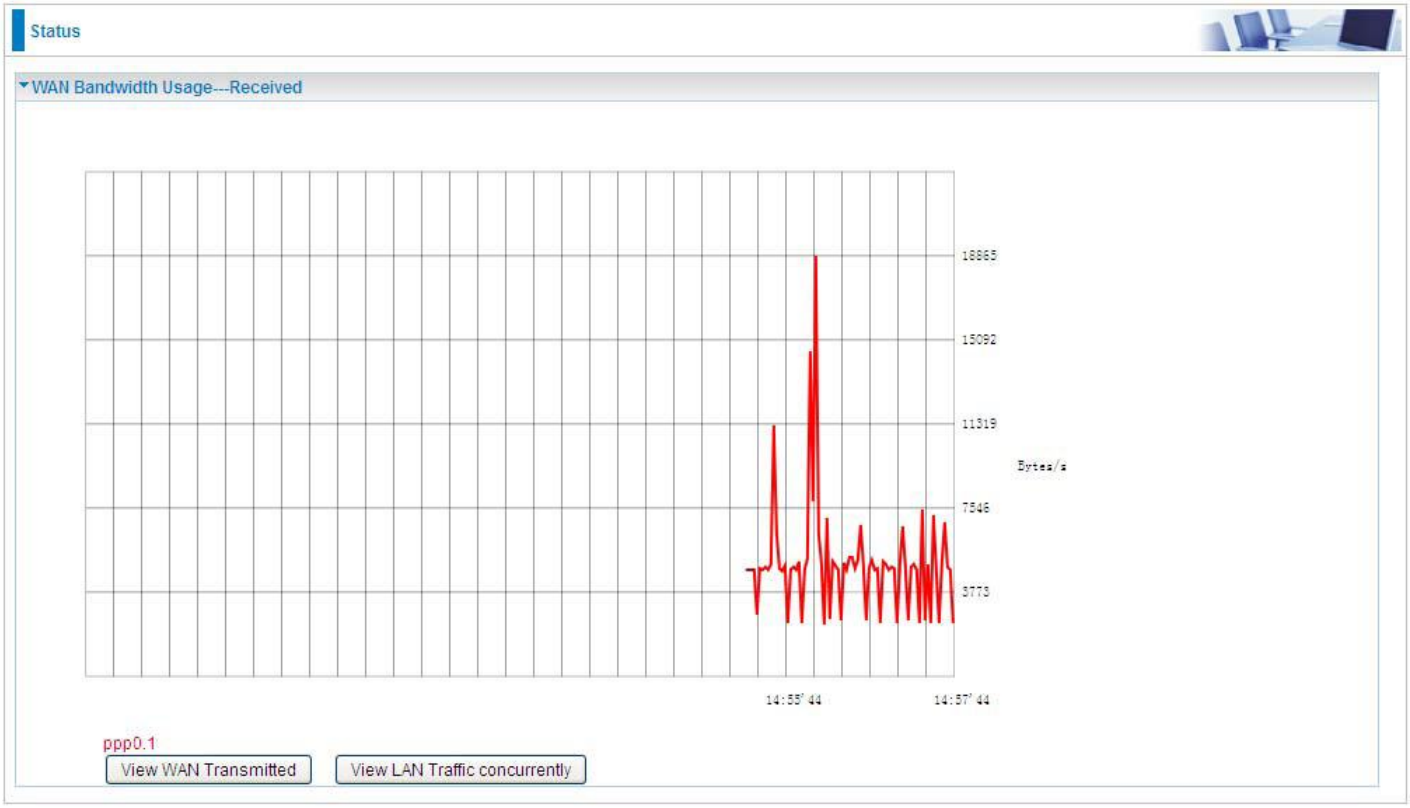


Click **View LAN Transmitted** button to view data sent to the Internet on each individual LAN port.

Example: P3 means Ethernet LAN #3, and the traffic information of the port #3 is identified with green, the same color with P3 in the diagram; other ports all take the same mechanism.

Click **View WAN Traffic concurrently** to monitor both the LAN and WAN data traffics concurrently. A new window, displaying WAN traffic, will appear on the screen.

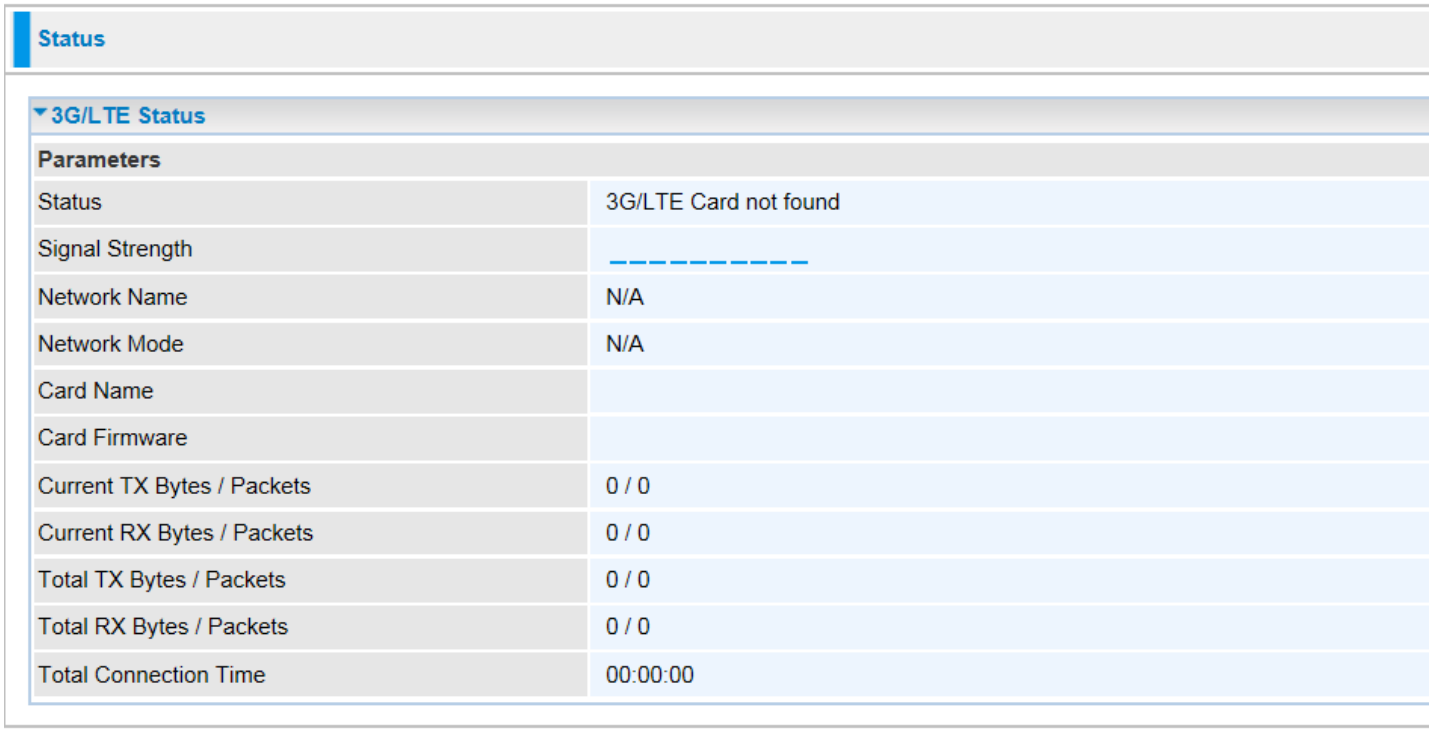
View WAN Bandwidth Usage - Received



Click **View WAN Transmitted** button to view total data sent to the Internet by all network devices per WAN interface.

Click **View LAN Traffic concurrently** to monitor both the LAN and WAN data traffics concurrently. A new window, displaying LAN traffic, will appear on the screen.

3G/4G LTE Status



Status: The current status of the 3G/4G LTE connection.

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G LTE Signal Strength LED indicates the signal strength as well.

Network Name: The name of the 3G/4G LTE network the router is connecting to.

Network Mode: The current operation mode for 3G/4G LTE module, it depends on service provider and card's limitation, GSM or UMTS.

Card Name: Given a name for the embedded 3G/4G LTE module.

Card Firmware: Current used FW in the 3G/4G LTE module.

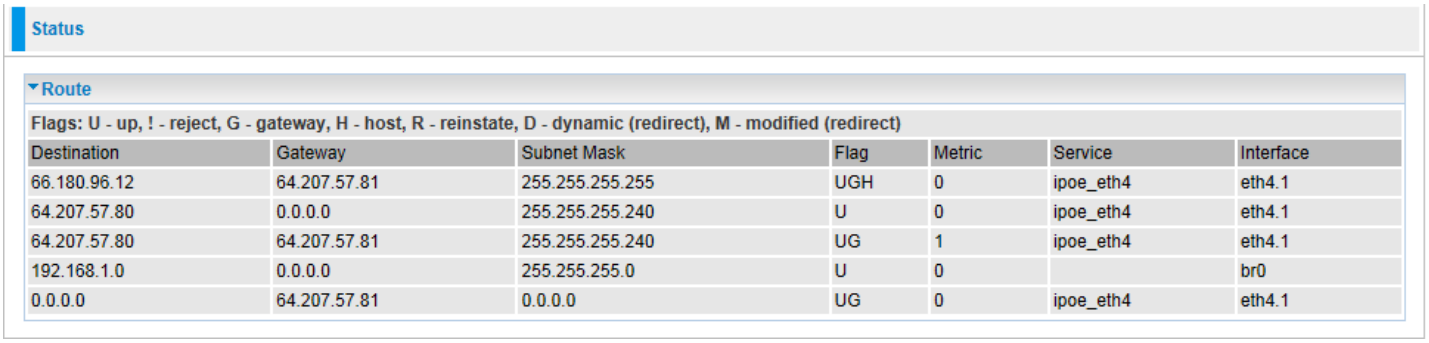
Current Received (RX) /Transmitted (TX) Bytes: Current Rx/TX (receive/transmit) packets in Byte

Total Received (RX) /Transmitted (TX) Bytes: The total Rx/TX (receive/transmit) packets in Byte

Total Connection Time: The total of 3G/4G LTE dongle connection time since the 3G/4G LTE is up and running

Route Table

The Rout Table provides users with a database in the router that contains current network topology such as current paths for transmitted packets. Both static and dynamic routes are displayed.



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
66.180.96.12	64.207.57.81	255.255.255.255	UGH	0	ipoe_eth4	eth4.1
64.207.57.80	0.0.0.0	255.255.255.240	U	0	ipoe_eth4	eth4.1
64.207.57.80	64.207.57.81	255.255.255.240	UG	1	ipoe_eth4	eth4.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	64.207.57.81	0.0.0.0	UG	0	ipoe_eth4	eth4.1

Destination: The IP address of destination network.

Gateway: The IP address of the gateway this route uses.

Subnet Mask: The destination subnet mask.

Flag: Show the status of the route.

- **U:** Show the route is activated or enabled.
- **G:** Show that the outside gateway is needed to forward packets in this route.
- **H (host):** destination is host not the subnet.
- **R:** Show that the route is reinstated from dynamic routing.
- **D:** Show that the route is dynamically installed by daemon or redirecting.
- **M:** Show the route is modified from routing daemon or redirect.

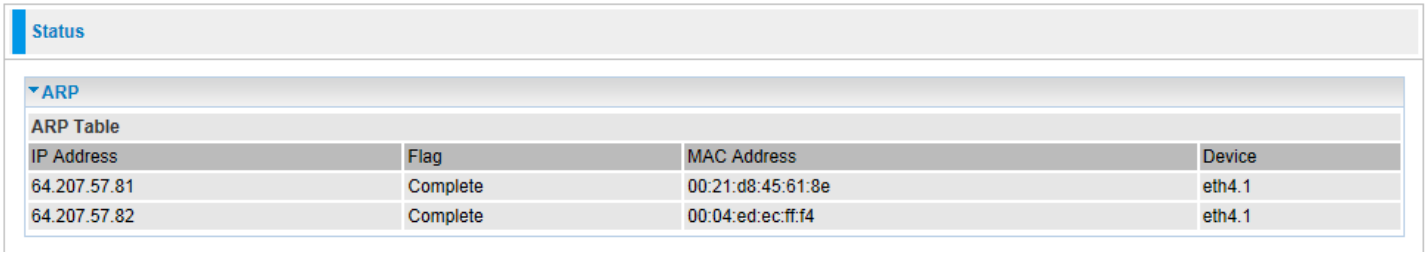
Metric: Display the number of hops counted as the Metric of the route.

Service: Display the service that this route uses.

Interface: Display the existing interface this route uses.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's ***Security*** – ***MAC Filter*****ing** function. Here IPv6 Neighbor Table, listed with IPv6 address-MAC mapping, is supported.



ARP Table

IP Address: Shows the IP Address of the device that the MAC address maps to.

Flag: Shows the current status of the ARP entries.

- Complete: the route resolving is processing well.
- M (Marked as permanent entry): the route is permanent.
- P (publish entry): publish this route item.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. Example, the Clients in LAN displays as eth4 (client is connected to Ethernet port 4).

Neighbor Cache Table

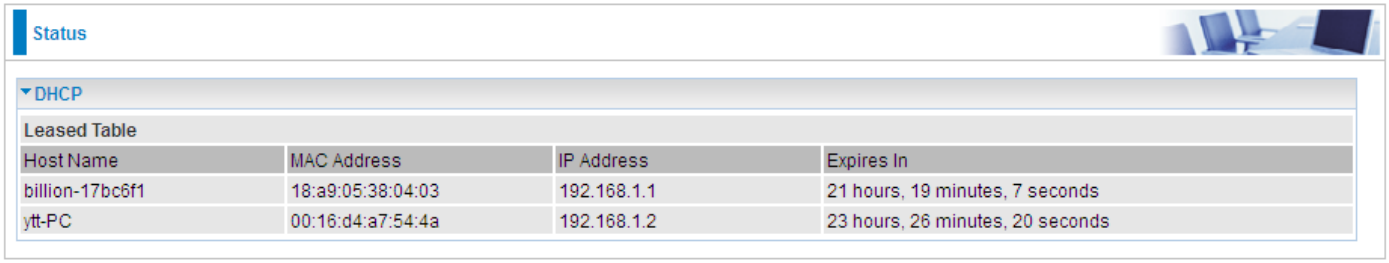
IPv6 address: Shows the IPv6 Address of the device that the MAC address maps to.

MAC Address: Shows the MAC address that is corresponded to the IPv6 address of the device it is mapped to.

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. Example, the Clients in LAN displays as eth4 (client is connected to Ethernet port 4).

DHCP Table

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.



Host Name: Displays the Host Name of the DHCP client.

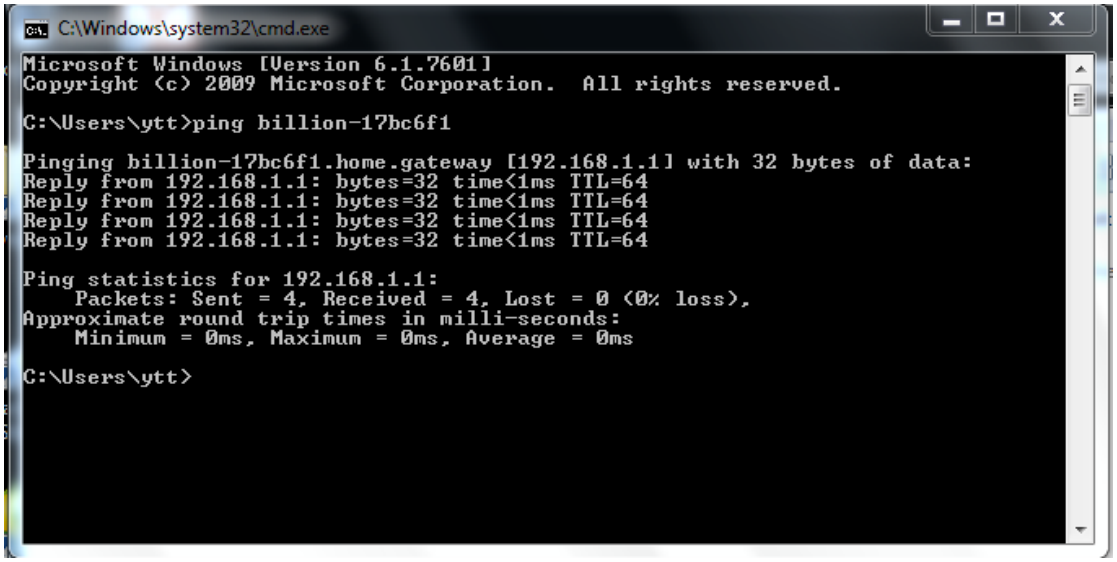
MAC Address: The MAC Address of internal DHCP client host.

IP Address: The IP address which is assigned to the host with this MAC address.

Expires in: Displays the remaining time before the lease expired

Note: The devices are free to access each other through device name on condition that they all obtain their IPs from the DHCP. If the device IP is obtained from the DHCP, other devices can access the device through the device name.

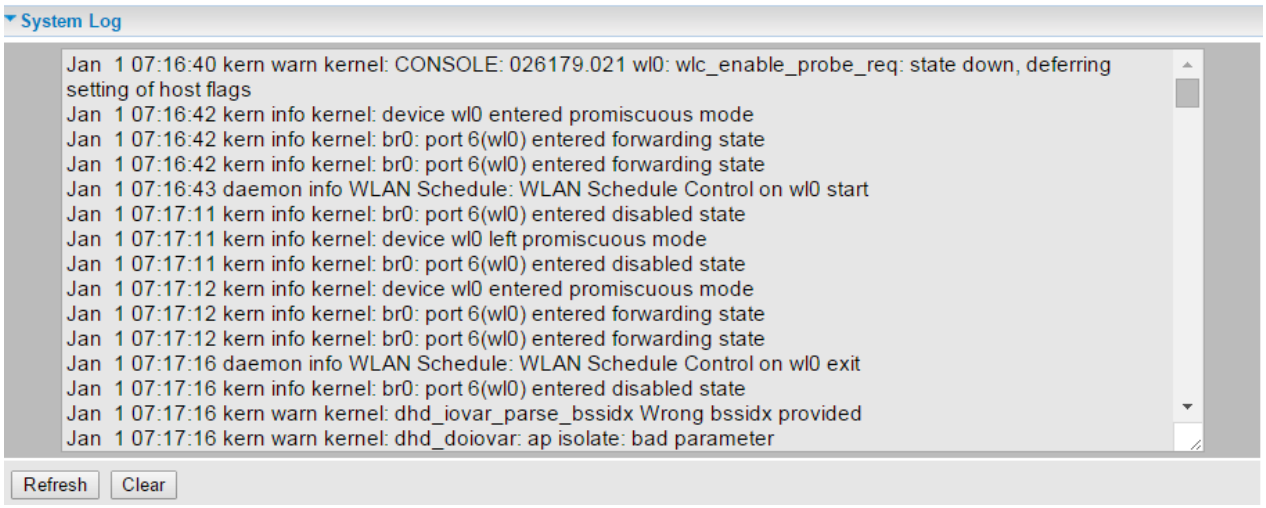
For example, the PC ytt-PC can ping the billion-17bc6f1 using the host name instead of its IP.



Log

System Log

Displays system logs accumulated up to the present time. You can trace historical information with this function. And the log policy can be configured in Configure Log section.

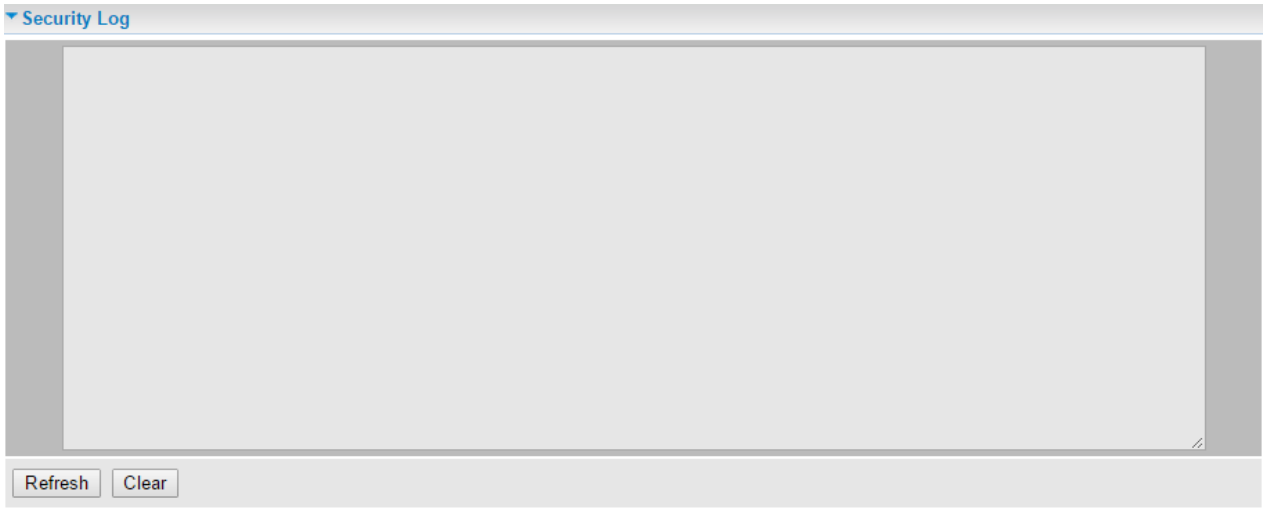


Refresh: Click to update the system log.

Clear: Click to clear the current log from the screen.

Security Log

Security log displays the message logged about security, like filter messages and some firewall message. You can turn to IP Filtering Outgoing, IP Filtering Incoming, and URL Filter to determine if you want to log this information. Also you can turn to Configure Log section below to determine the level to log the message. You can use this to track potential threats to your system and network.



Refresh: Click to update the system log.

Clear: Click to clear the current log from the screen.

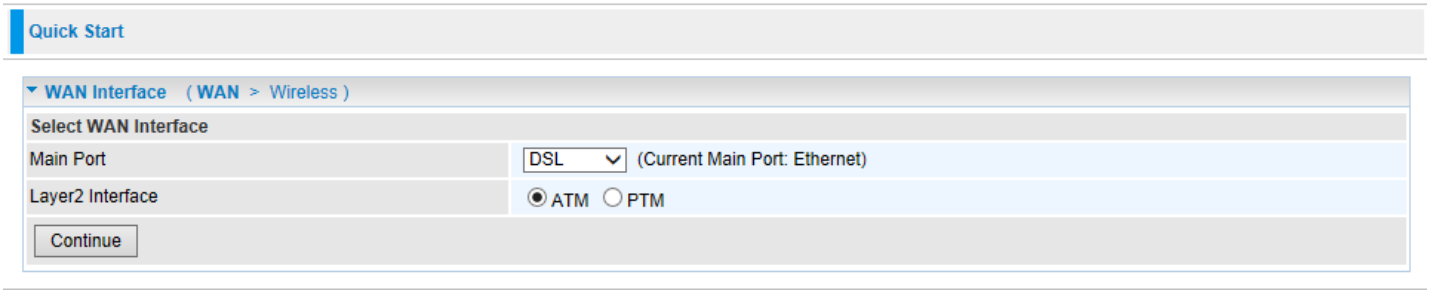
Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup time zone and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

Step 1 – WAN Connection Type

Set up your WAN Internet connection.

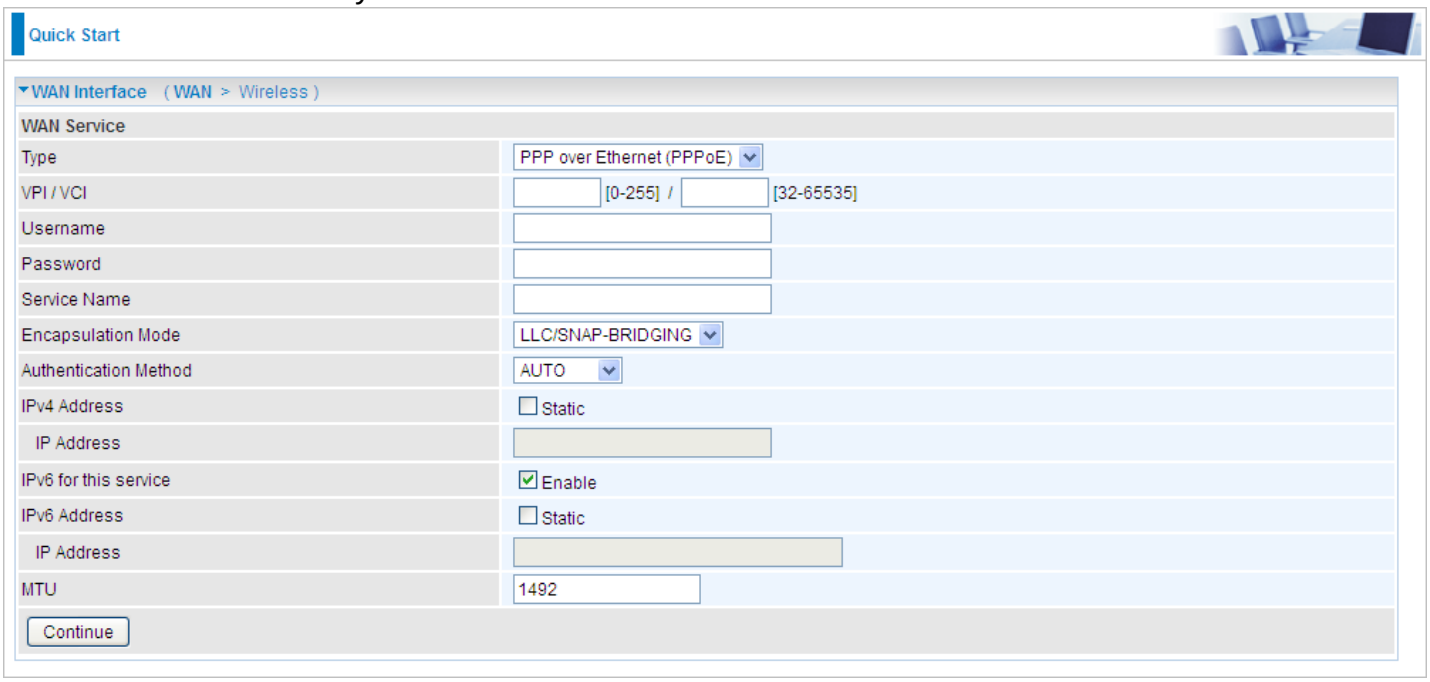
Select a WAN Main Port then click **Continue** to continue



Step 2 – WAN Setup

2.1 If selected **DSL / PPPoE**

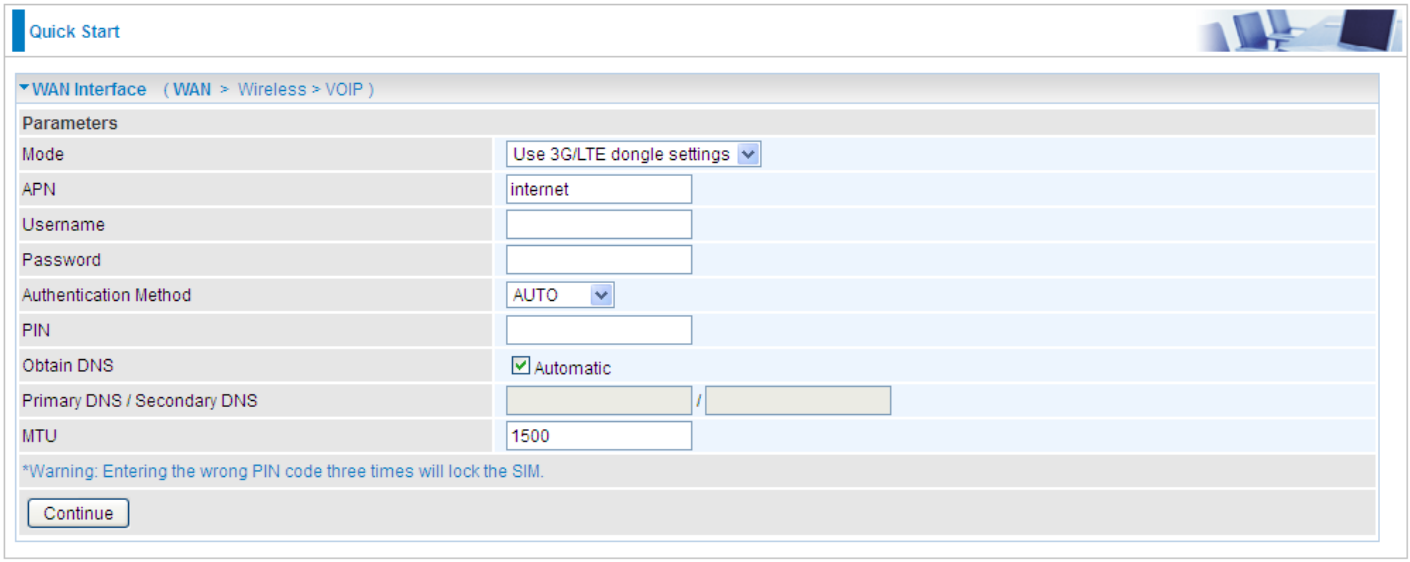
Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.



If the DLS line is not synchronized, the page will pop up warning of the DSL connection failure.

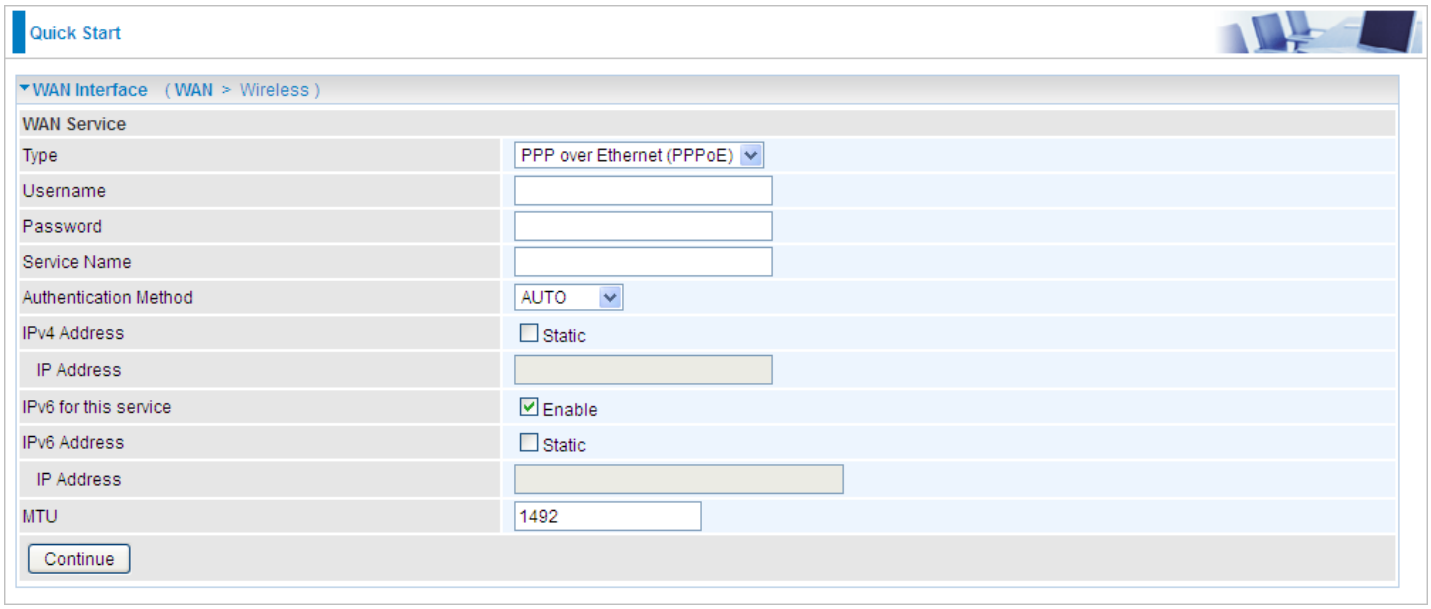
2.2 If selected **3G/4G-LTE USB**

Enter the APN, username, password from your ISP; and check with your ISP with the authentication method setting.



2.3 If selected **EWAN / PPPoE**

Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default

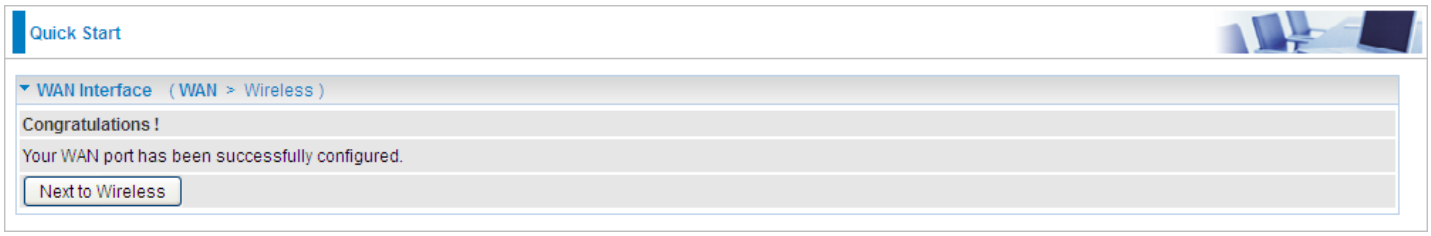


Step 3 – Configuration in Process

It takes about 15~30 seconds to save current configured settings. Once it is done, you will see a “Configurations!” window.

Step 4 – WAN Connection Ready

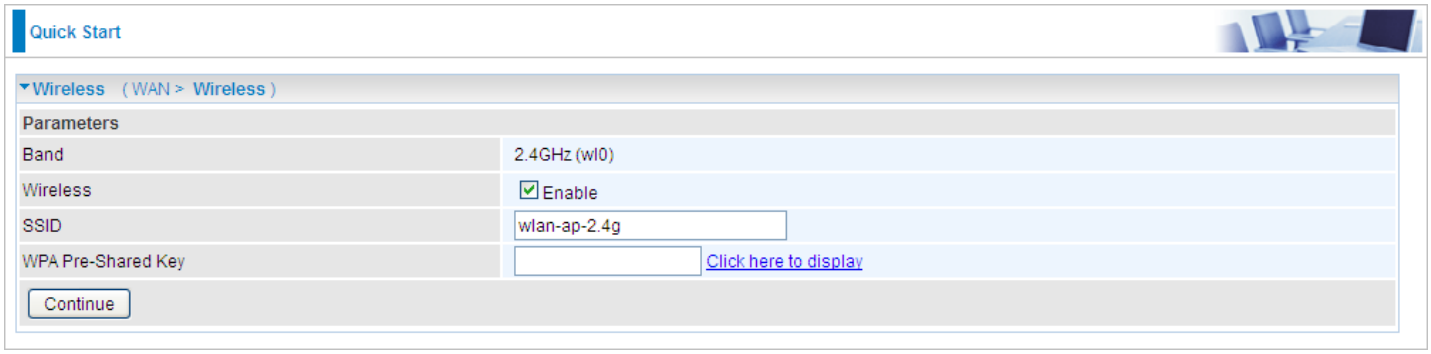
You now may be able to access to the Internet. If not, please check your WAN, Internet Connection, setup again.



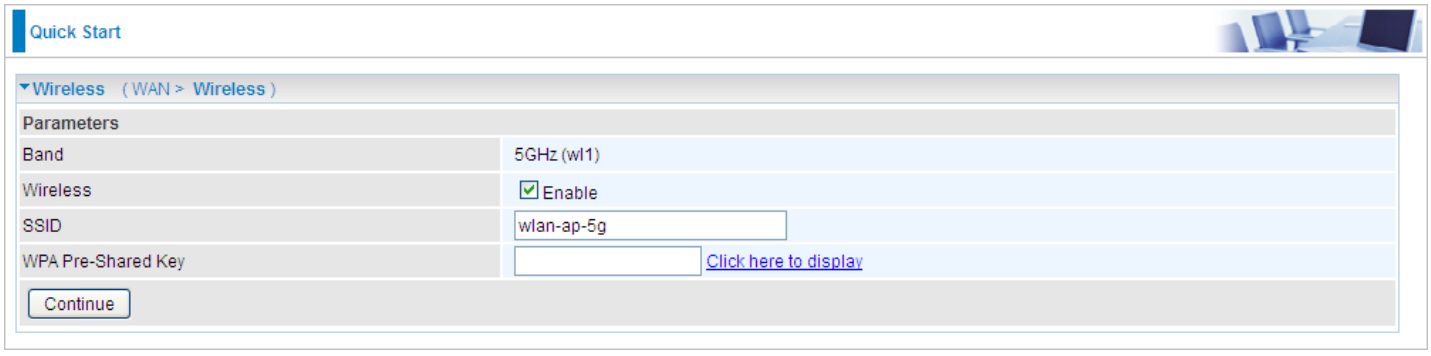
Step 5 – Wireless Setup

After the configuration is successful, click Next to Wireless button and you may proceed to configure the Wireless settings, SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

2.4GHz Wireless



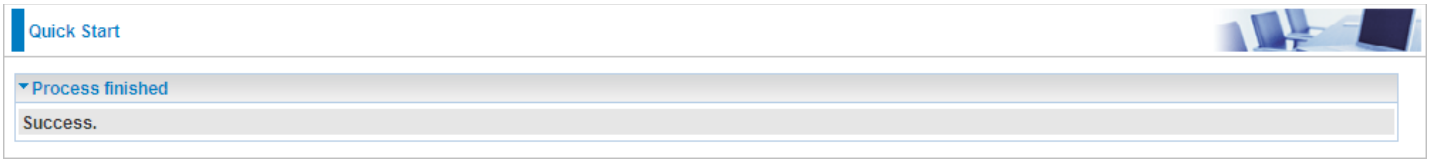
5GHz Wireless



Step 6 – Quick Start Completed!

You now may be able to access to the Internet via the Ethernet cable or Wireless.

Go back to **Status** > **Summary** for more information.

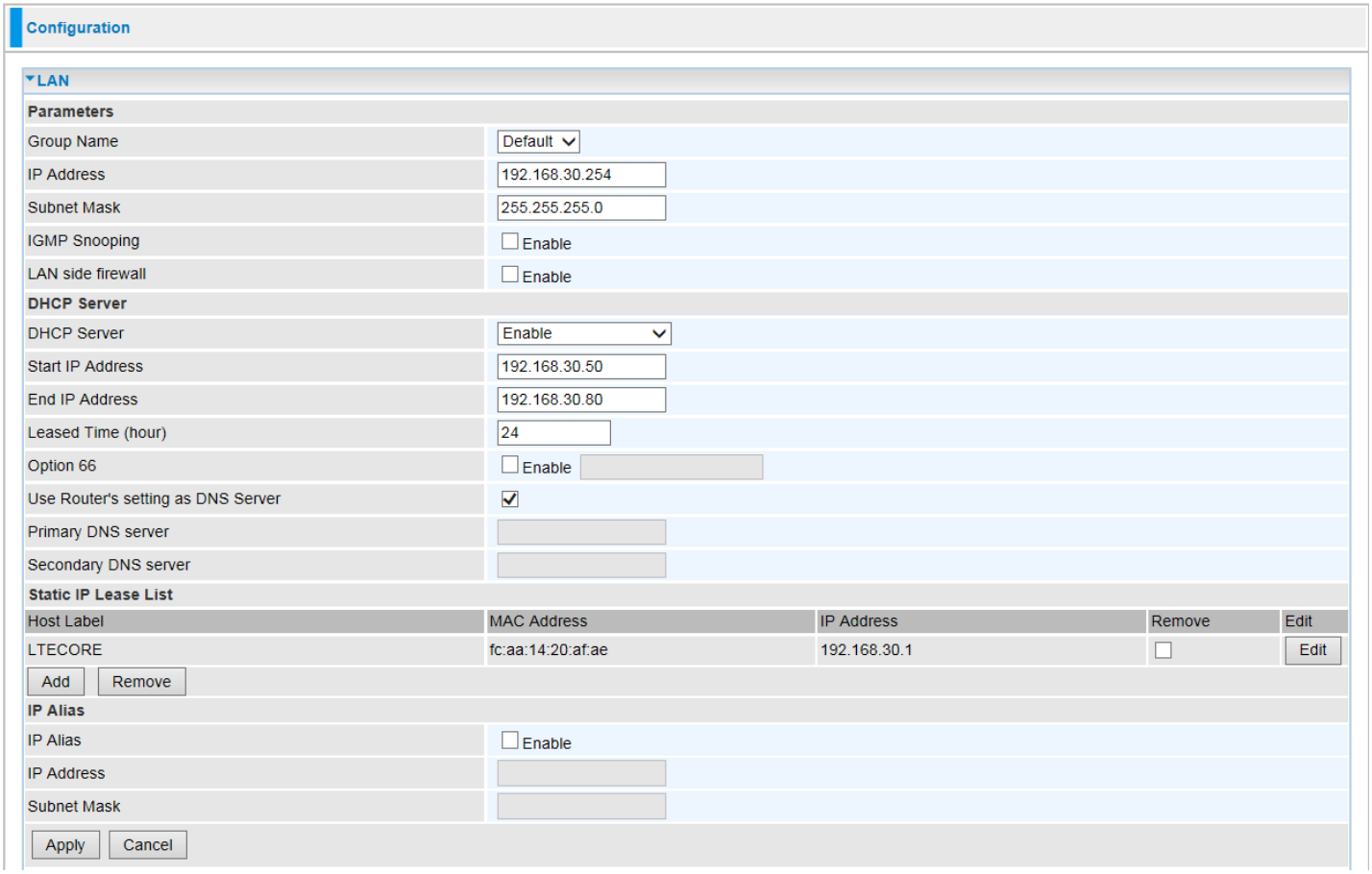

Quick Start
Process finished
Success.

Configuration

LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building.

Ethernet



Parameters

Group Name: This refers to the group you set in **Interface Grouping** section; you can set the parameters for the specific group. Select the group via the drop-down box. For more information please refer to Interface Grouping of this manual.

IP address: the IP address of the router. Default is 192.168.1.254.

Subnet Mask: the default Subnet mask on the router.

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

When enabled, you will see two modes:

- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

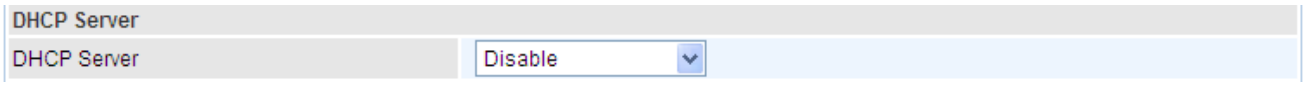
LAN side firewall: Enable to drop all traffic from the specified LAN group interface. After activating it, all incoming packets by default will be dropped, and the user on the specified LAN group interface can't access CPE anymore. But, you can still access the internet service. If user wants to manage the CPE, please turn to IP Filtering Incoming to add the allowing rules.

Note: that all incoming packets by default will be dropped if the LAN side firewall is enabled and user cannot manage this CPE from the specified LAN group.

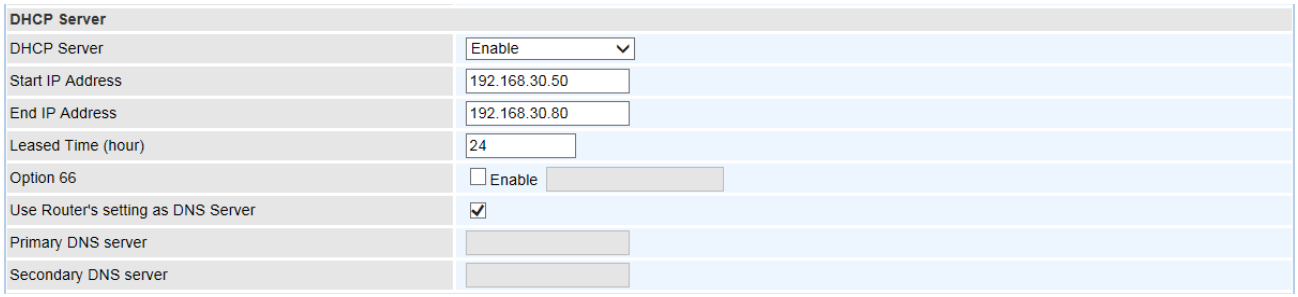
DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

- **Disable**: to disable DHCP server function



- **Enable**: to enable DHCP function and enter the IP Range information.



Start / End IP Address: The range of IP addresses to be assigned to clients.

Leased Time (hour): the period of time the IP address assigned will be valid. When expires, the assigned IP will be recycled and reassigned.

Option 66: Click Enable to activate DHCP option 66 for some special devices, like IPTV Set Box. The devices can get firmware or some special service from the TFTP server. User needs to set the IP or hostname of the TFTP server.

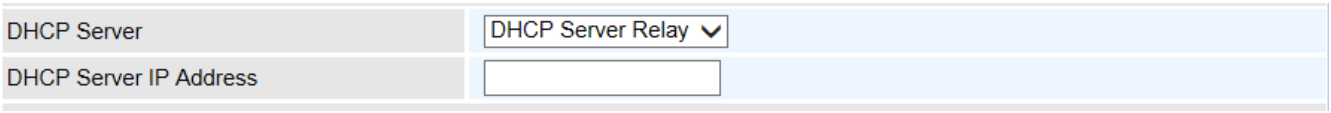
Use Router's Setting as DNS Server: After enabling it, BEC 8920AC would act as a DNS server and would provide DNS services to all LAN connected devices. Manually specify primary/secondary DNS server IP addresses when disabling this feature.

Primary / Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

- **DHCP Server Relay**

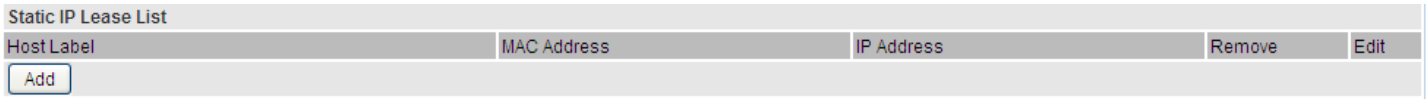
The DHCP Server Relay acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual,

remote DHCP server in the Remote DHCP Server field in this case.

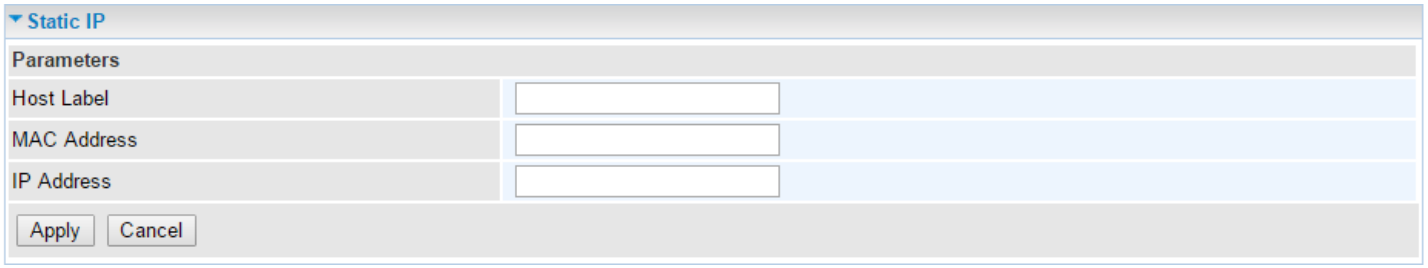


Static IP Lease List

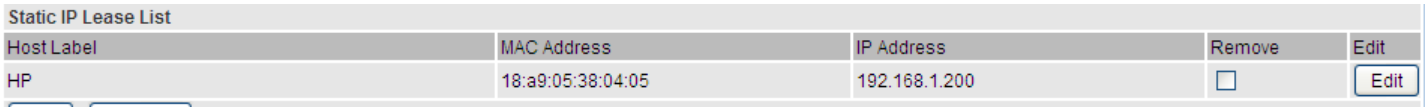
The specified IPs will be assigned to corresponding LAN devices with exact MAC Address listed in the following table.



Press **Add** to the Static IP List.

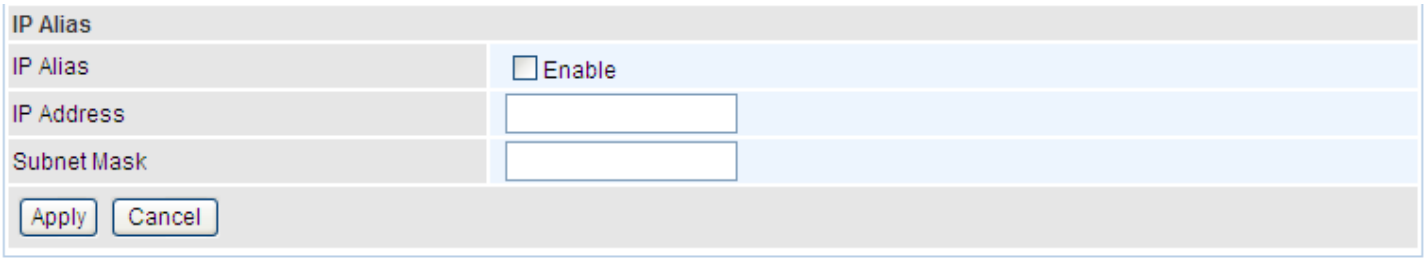


Enter a LAN device's MAC Address, desired IP Address, and then click Apply to confirm the settings. The assigned IP address must be outside of the Start / End DHCP Server range).



IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote nodes.



IP Alias: Check whether to enable this function.

IP Address: Specify an IP address on this virtual interface.

Subnet Mask: Specify a subnet mask on this virtual interface.

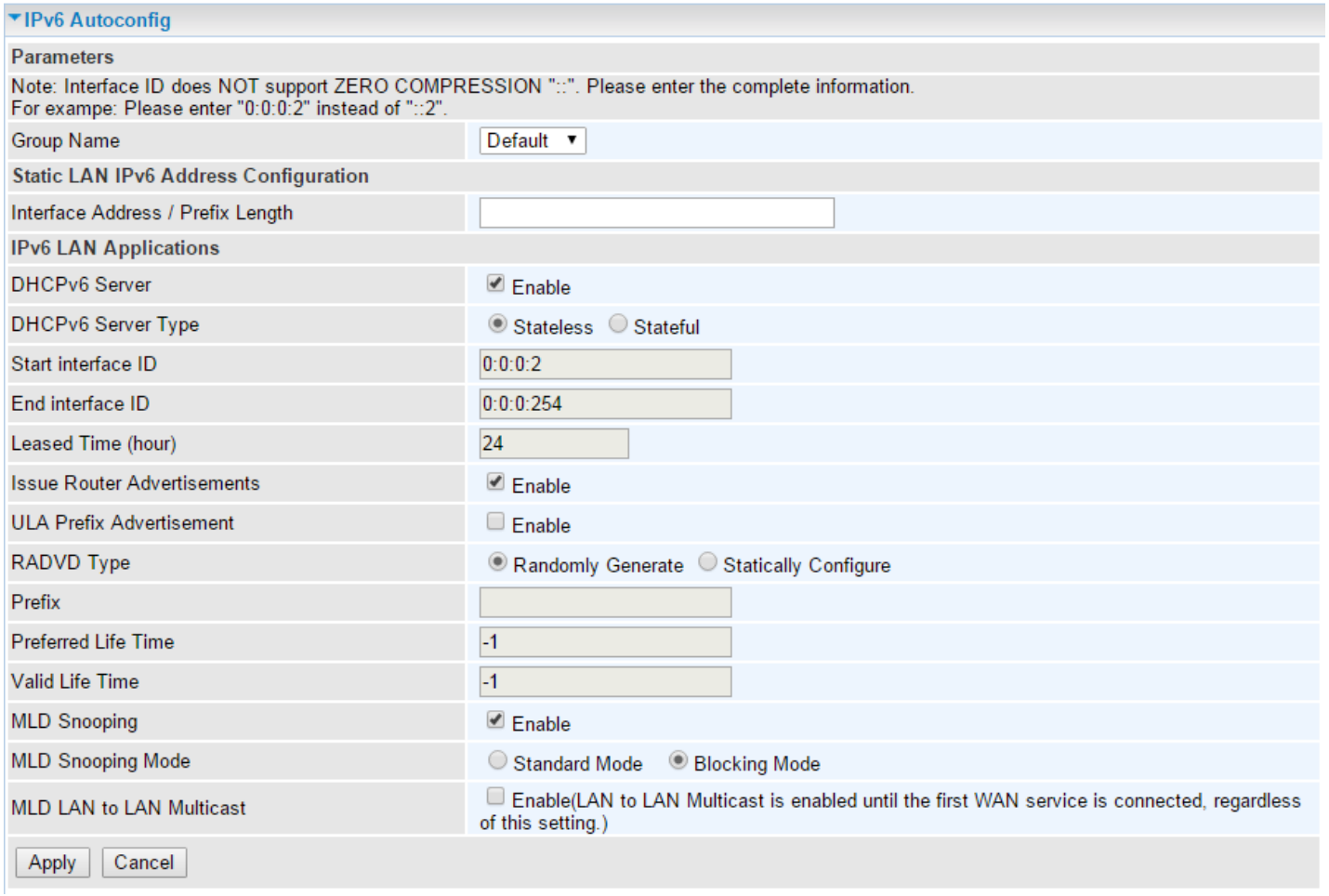
Click **Apply** to apply your settings.

IPv6 Autoconfig

The IPv6 address composes of two parts, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is “stateful” configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto-configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is “stateless” configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn’t configure anything on the client.



Parameters

Group Name: Here group refers to the group you set in **Interface Grouping** section; you can set the parameters for the specific group. Select the group by the drop-down box. For more information please refer to **Interface Grouping** of this manual.

Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: Enter the static LAN IPv6 address.

IPv6 LAN Application

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available.

- **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server.

  Stateless IPv6 address Configuration

  Stateless: Two methods can be carried.

  1. With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv6 Server	☐ Enable
Issue Router Advertisements	☑ Enable

  With this method, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers.

  2. With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	☑ Enable
DHCPv6 Server Type	◉ Stateless ○ Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	☑ Enable

  With this method, the PCs' addresses in LAN are configured like above method, but they can obtain such information like DNS from DHCPv6 Server.

- **Stateful:** if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

  Stateful IPv6 address Configuration

  Stateful: two methods can be adopted.

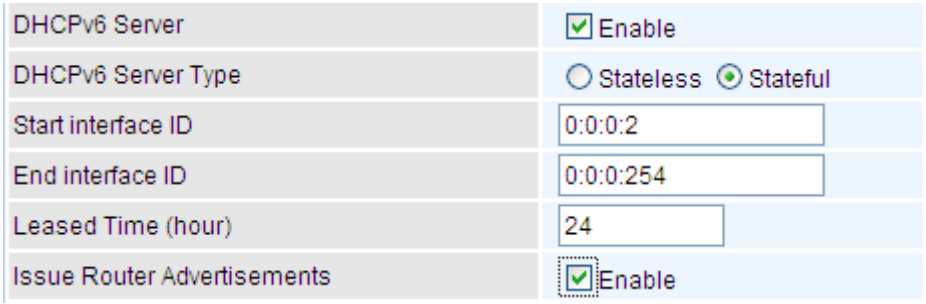
  1. With only DHCPv6 enabled

DHCPv6 Server	☑ Enable
DHCPv6 Server Type	○ Stateless ◉ Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	☐ Enable

  With this method, the PCs' addresses are configured the same as in IPv4, that is addresses are

assigned by DHCPv6 server.

2. With both DHCPv6 and Issue Router Advertisement Enabled



With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

Start interface ID: Enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: Enter the end interface ID. **Note:** Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.
For example: Please enter "0:0:0:2" instead of "::2".

Leased Time (hour): The period of time the IP address assigned will be valid. When expires, the assigned ID will be recycled and reassigned.

Issue Router Advertisement: Check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

ULA Prefix Advertisement: Enable this parameter to include the ipv6 ULA address in the RA messages. ULA, unique local address, is an IPv6 address in the block fc00::/7. It is approximately the IPv6 counterpart of the IPv4 private address. They are not routable in the global IPv6 Internet.

RADVD Type: The way that ULA prefix is generated.

- **Randomly Generated**
- **Statically Configured**: select to set manually in the following parameters.

  Prefix: Set the prefix manually.

  Preferred Life Time: The ULA prefix life time. When the time is over, the ULA prefix is invalid any more, -1 means no limit.

  Valid Life Time: It is a time threshold, when the time is over, clients should obtain new IPv6 address from the router through RA; -1 means to be limitless.

MLD snooping: Similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

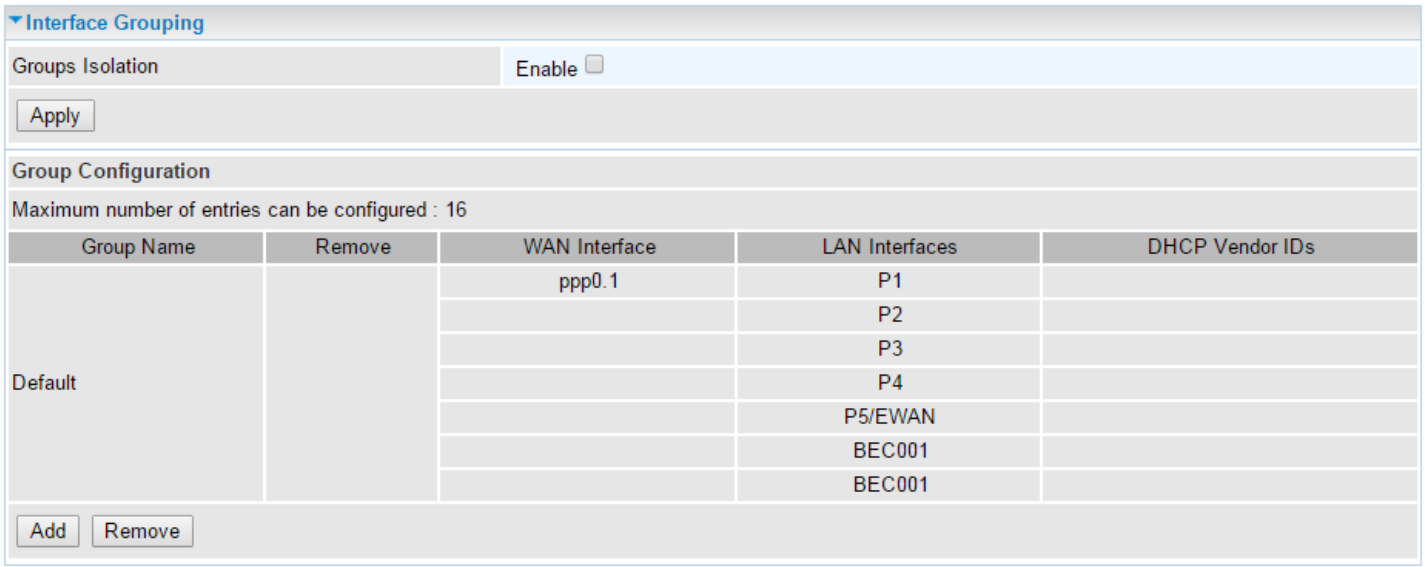
- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **Blocking Mode:** In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won't flood to the bridge ports.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

Note: LAN Port 5 is a LAN / WAN port. When it is configured to EWAN, Available LAN ports are from P1 ~ P4.



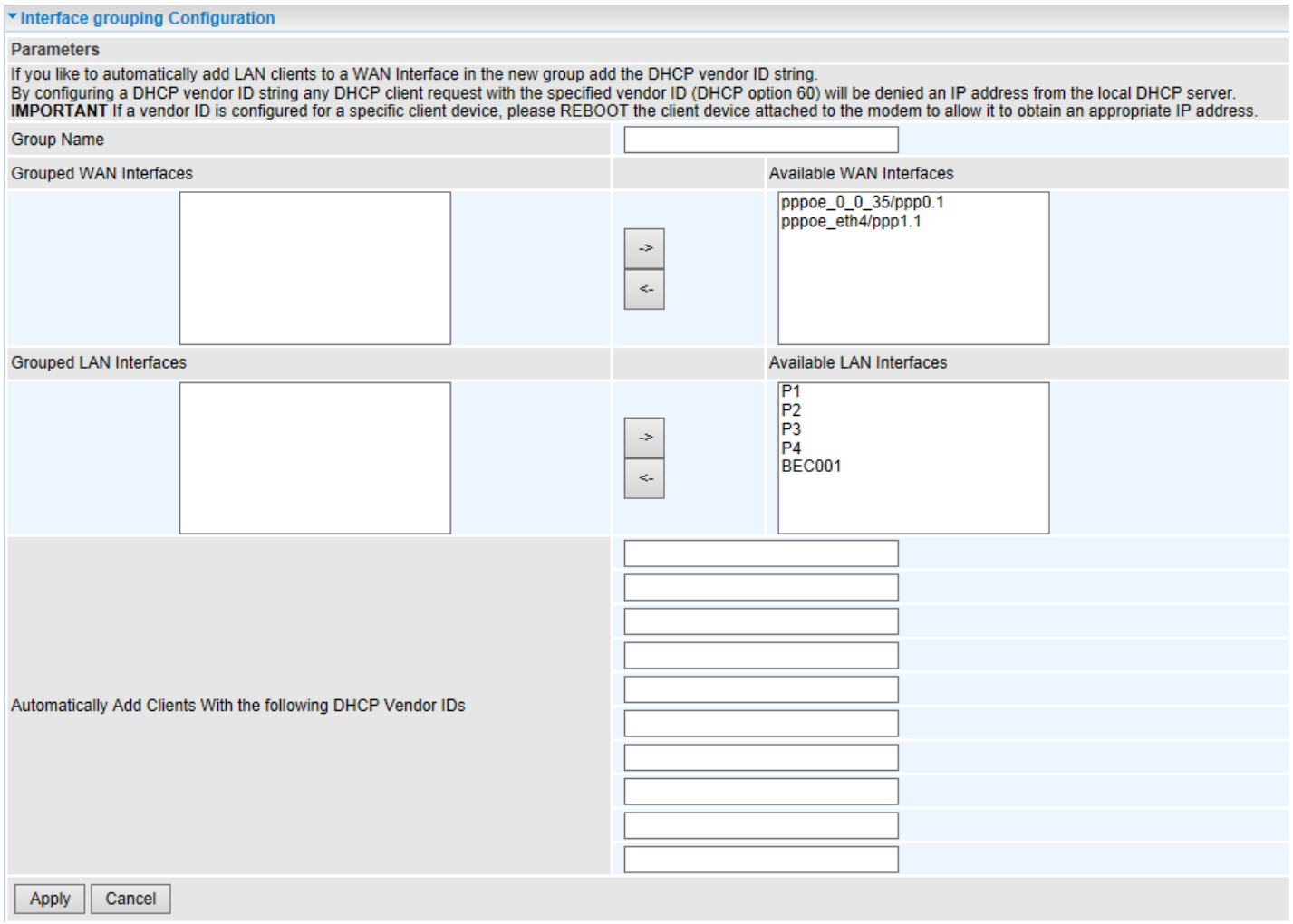
Groups Isolation

Groups Isolation: If enabled, all groups created below, in **Group Configuration**, will not be able communicate with one another.

Click **Apply** to save the settings.

Group Configuration

Click **Add** to add and create groups.



Group Name: Type a group name.

Grouped WAN Interfaces: Select from the box the WAN interface you want to apply in the group.

Grouped LAN Interfaces: Select the LAN interfaces you want to group as a single group from the *Available LAN Interfaces*.

Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click **Apply** to confirm your settings and your added group will be listed in the Interface Grouping table below.

Examples:

To Create a Group

In group "test", P2 and PPP0.1 are grouped in one group, they have their only network.

If **Group Isolation** is being turned on, Group “Default” and “test” are now isolated to each other. All devices connect to default group ports (P1, P3, P4, Wireless 2.4g, Wireless 5.g, and P5/EWAN), will not be able to communicate with device in the test group, P2.

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P1	
			P3	
			P4	
			wlan-ap-5g	
			wlan-ap-2.4g	
			P5/EWAN	
test	☐	ppp0.1	P2	

Add Remove

To Delete a Group

If you want to remove the group, check the box as the following then click **Remove**.

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P1	
			P3	
			P4	
			wlan-ap-5g	
			wlan-ap-2.4g	
			P5/EWAN	
test	☑ 1	ppp0.1	P2	

Add Remove 2

To Automatically Add a Group

If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Each LAN interface can only be added into one group and one WAN interface can only be used in one group.

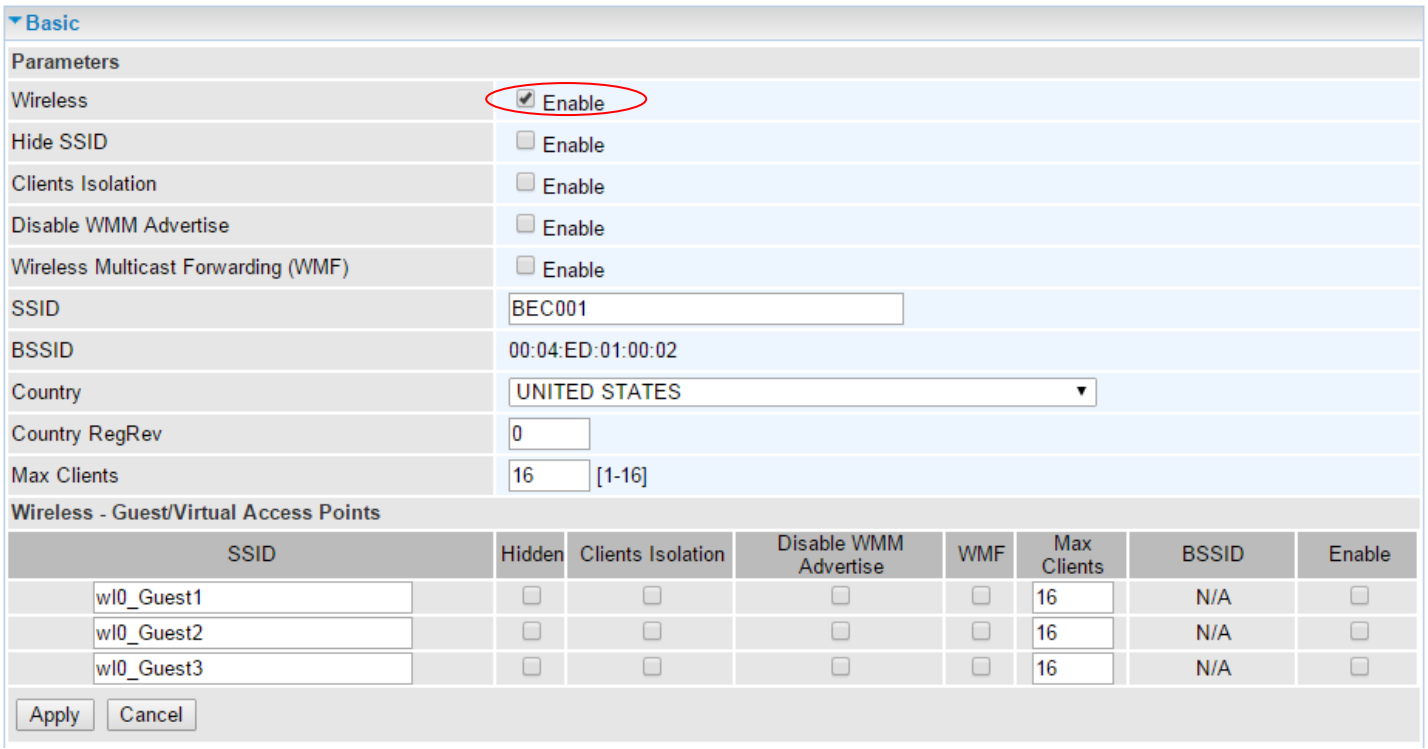
Wireless 5G (wl0) & 2.4G (wl1)

BEC 8920AC is a simultaneous dual-band (2.4G and 5G) wireless router support 11b/g/n/a/ac wireless standards. It allows multiple wireless users in 2.4G and 5G radio bands to surf the Internet, checking e-mail, watching video, listening to music over the Internet concurrently.

You can choose the optimum radio band wireless connection base on your environment.

Basic

Click **Enable** then **Apply** to activate the Wireless.



Wireless: Default setting is set to **Enable**. If you do not have any wireless devices, check the checkbox again to unselect.

Hide SSID: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: if you enabled this function, then each of your wireless clients will not be able to communicate with each other.

Disable WMM Advertise: Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).

Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap-2.4g to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Note: SSID is case sensitive and must not exceed 32 characters.

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to your location.

Max Clients: enter the number of max clients the wireless network can supports, 1-16.

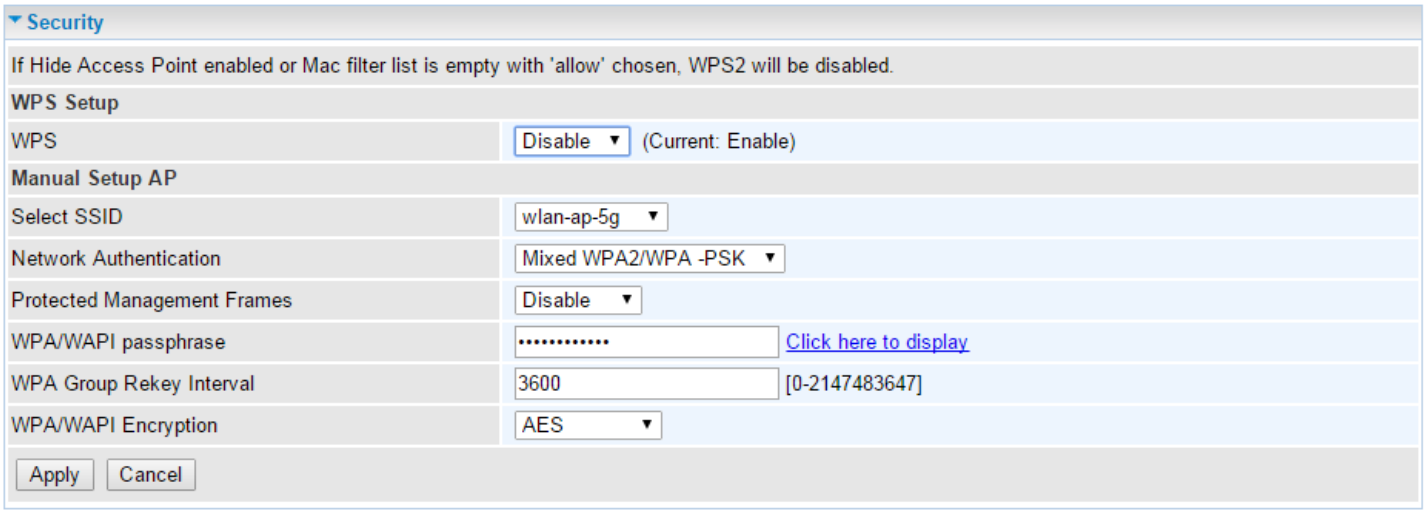
Guest/virtual Access Points: A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

Security

Wireless security prevents unauthorized access or damage to computers using wireless network.



WPS Setup

The Wi-Fi Protected Setup (WPS) is designed to simplify configuration process of connecting to a wireless network. With the WPS enabled, network must use either WPA (stronger security) or WEP OPEN (no security) wireless authentication method.

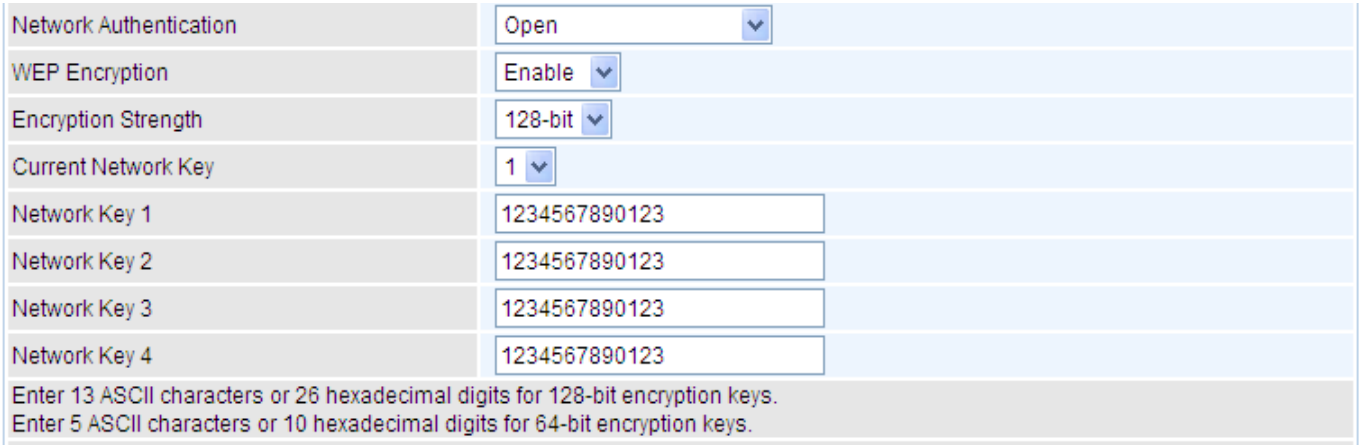
WPS: Enable to activate this feature. For detailed configuration, please refer to **WPS Configuration Setup** section.

Manual Setup AP

Select SSID: select the SSID you want these settings apply to.

Network Authentication

- **Open / WEP Enabled**



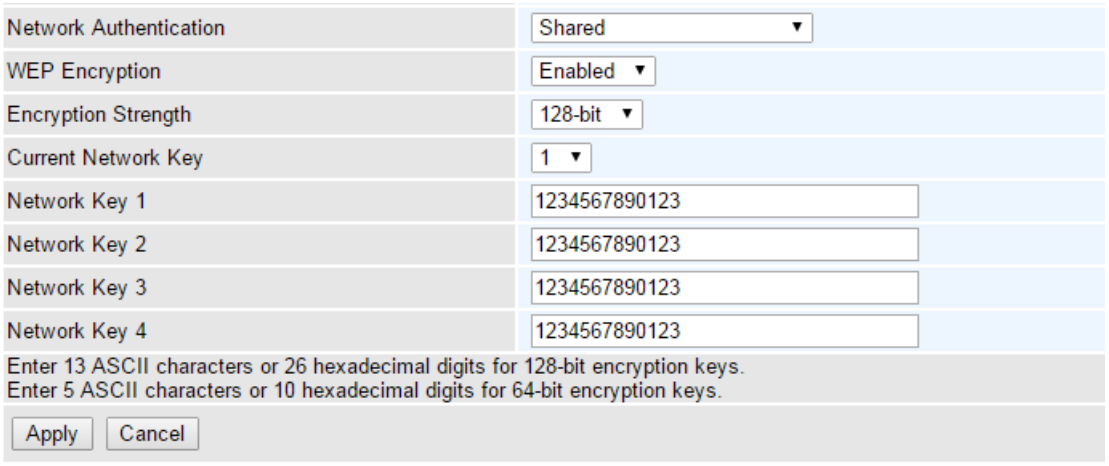
WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1- 4 below.

Network Key (1~4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

- **Shared / WEP Enabled**



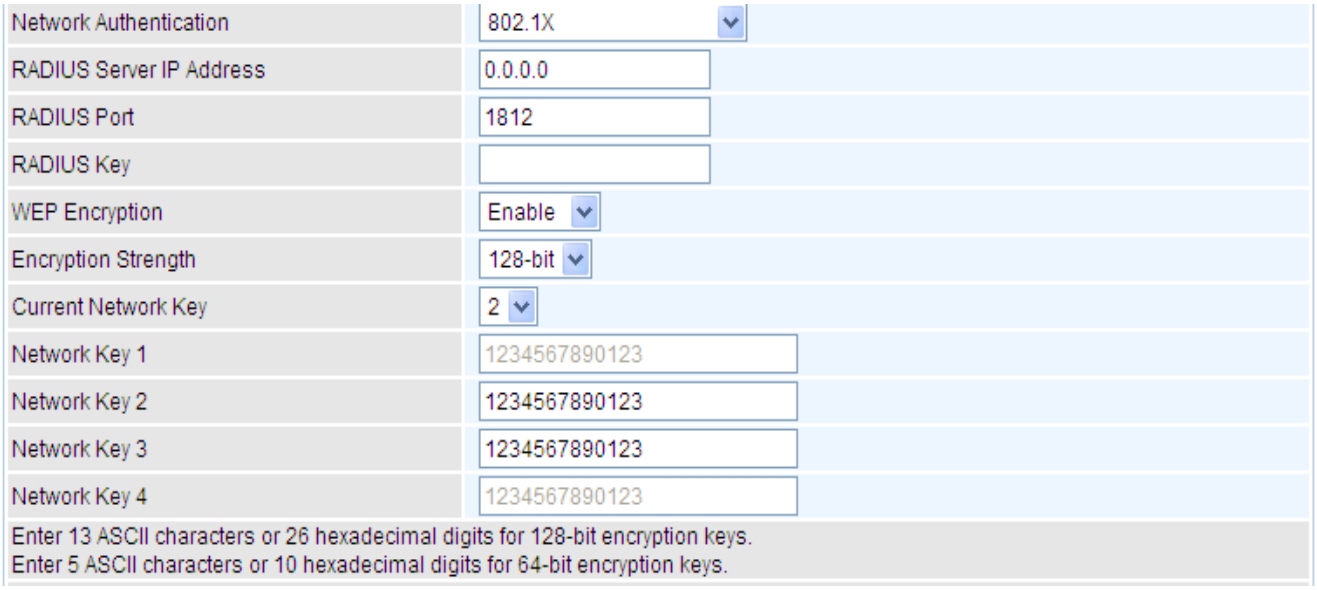
WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1- 4 below.

Network Key (1~4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

- **802.1x**



RADIUS Server IP Address: Remote Authentication Dial In User Service (RADIUS), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

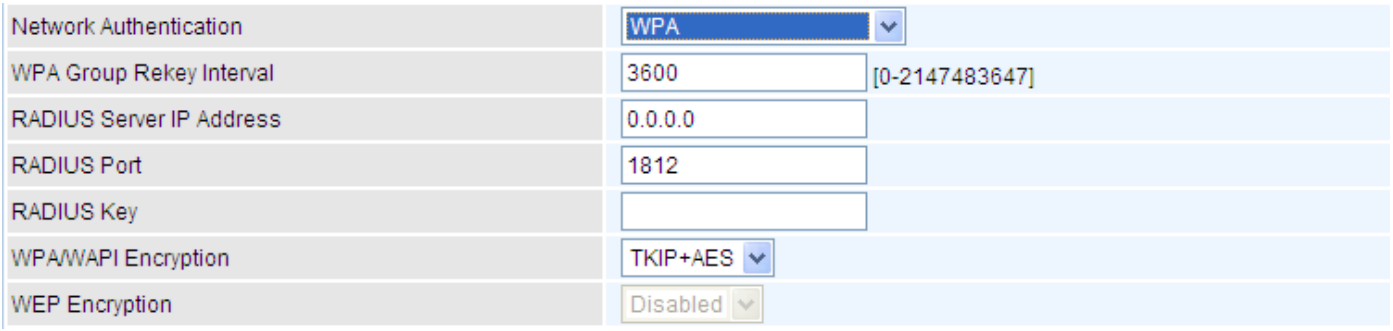
RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: Select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

WPA



WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

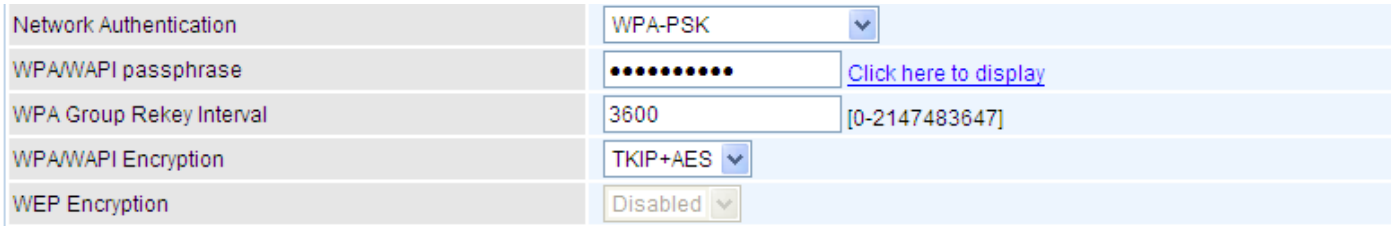
RADIUS Server IP Address: RADIUS (Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPA-PSK / WPA2-PSK



WPA/WAPI passphrase: Enter the WPA.WAPI passphrase; you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

- **WPA2**

Network Authentication	WPA2
WPA2 Preauthentication	Disable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA2 Pre-authentication: When a wireless client wants to handoff to another AP, with pre-authentication, it can perform 802.1X authentication to the new AP, and when handoff happens, this mode will help reduce the association time.

Network Re-auth Interval: the interval for network Re-authentication. This is in seconds.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

RADIUS Server IP Address: RADIUS (Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. This is in seconds.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

- **Mixed WPA2/WPA**

Network Authentication	Mixed WPA2/WPA
WPA2 Preauthentication	Disable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA2 Pre-authentication: When a wireless client wants to handoff to another AP, with pre-authentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

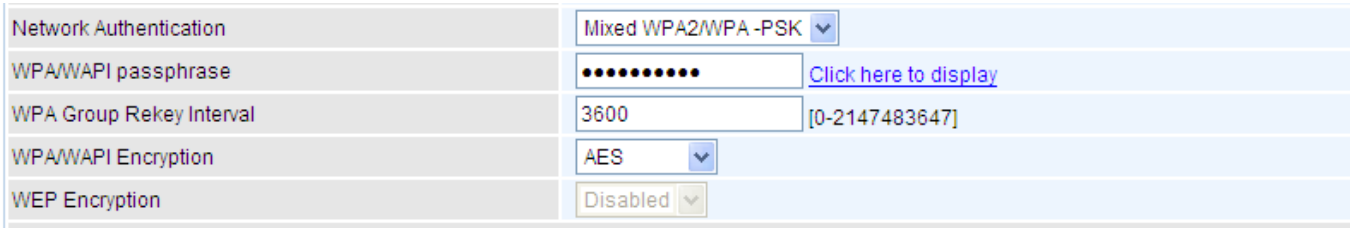
RADIUS Server IP Address: RADIUS (Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

- **Mixed WPA2/WPA-PSK**



WPA/WAPI passphrase: enter the WPA.WAPI passphrase; you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Configuration Setup

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure AP settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known **PIN method** is supported to configure WPS.

WPS: Select enable to enable WPS function. Please note that WPS can only be available when WPA2-PSK or OPEN mode is configured.

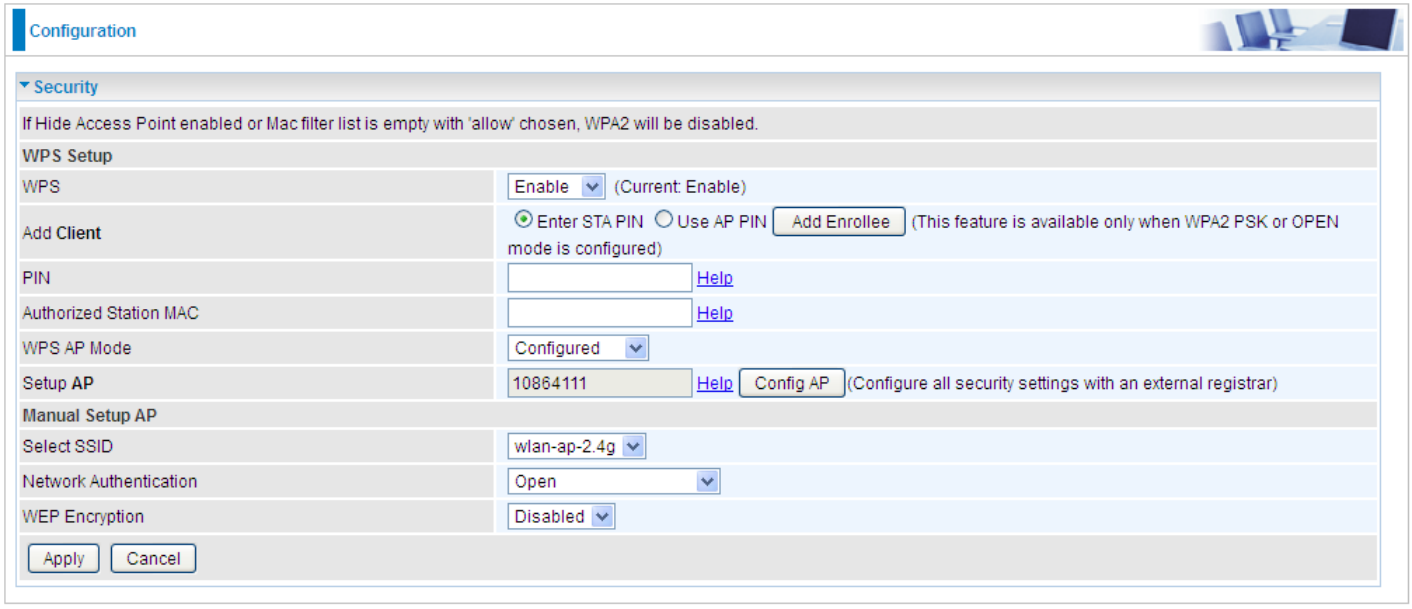
Attention:

1) With the WPS enabled, network must use either WPA (stronger security) or WEP OPEN (no security) wireless authentication method.

2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select “Configured” in the WPS AP Mode below.

Default WPS AP Mode is “Configured”.

When AP is configured as Enrollee, the WPS AP Mode below should be changed to “Unconfigured”. Follow the following steps.

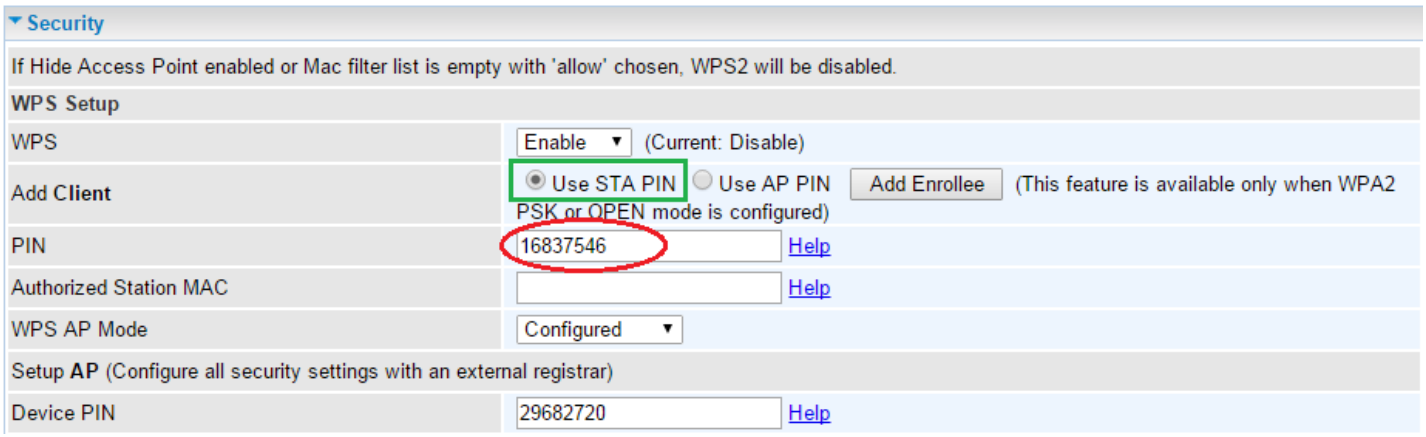


Example: Wi-Fi Protected Setup (WPS) – Configure AP as Registrar

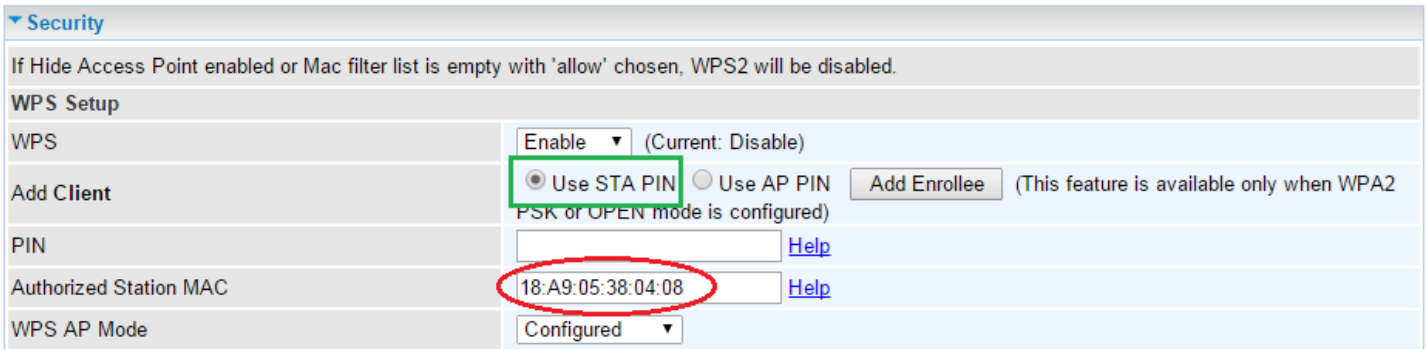
Add Enrollee with PIN method

1. Select radio button "***Enter STA PIN***".
2. Input PIN from Enrollee Station (16837546 in this example), Or else users can **alternatively** enter the authorized station MAC ***Help:*** it is to help users to understand the concept and correct operation.
3. Click Add Enrolee.

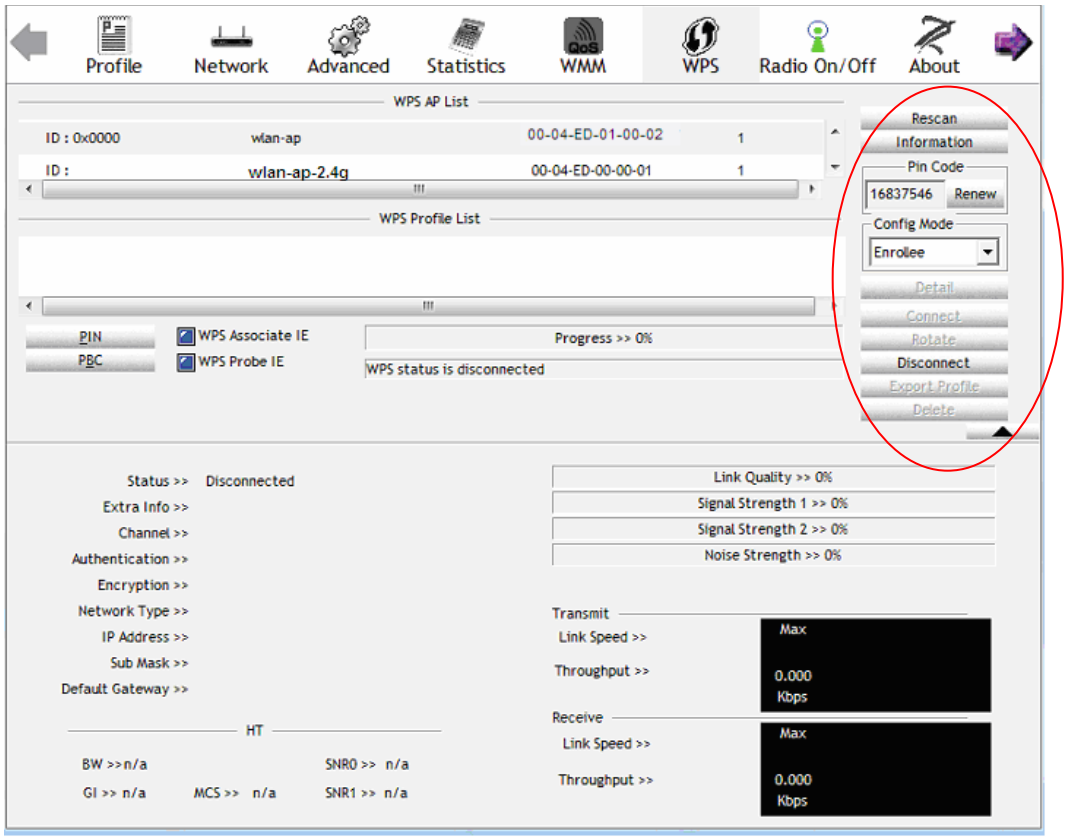
▸ Using PIN from the Enrollee Station



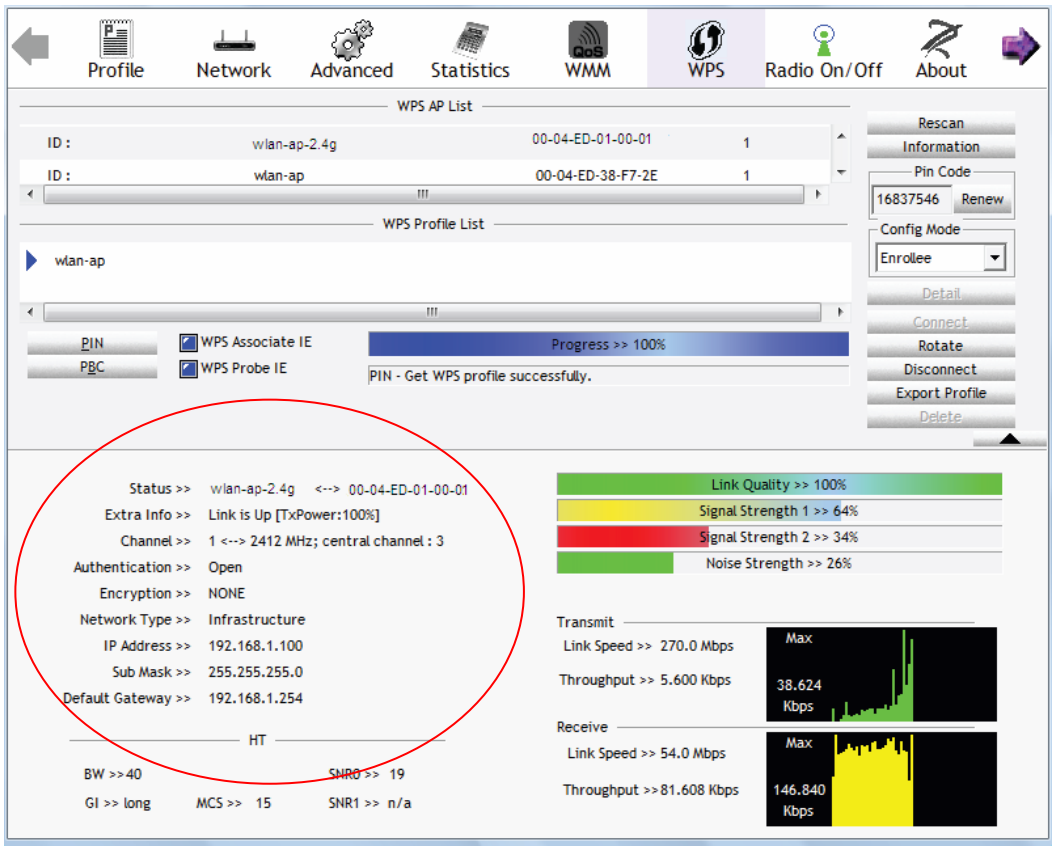
▸ Using MAC address of the Enrollee Station



4. In the wireless client's WPS utility (e.g.Ralink Utility), set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (e.g. Wlan-ap-2.4g) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



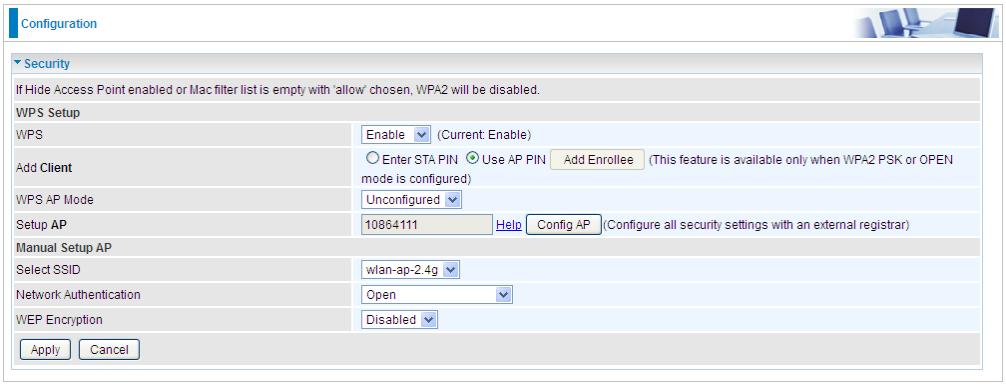
5. The client's SSID and security settings will now be configured to match the SSID and security settings of the registrar.



Example: Wi-Fi Protected Setup (WPS) – Configure AP as Enrollee

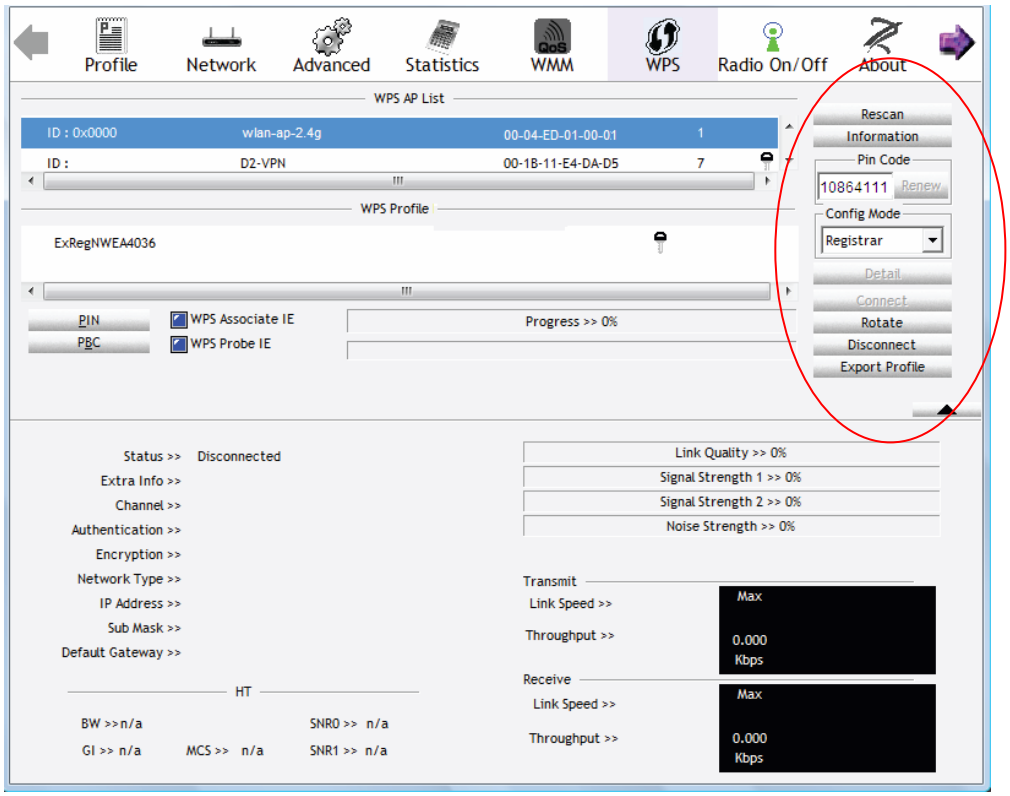
Add Registrar with PIN Method

1. Set AP to "***Unconfigured Mode***" and Click "***Config AP***" button.

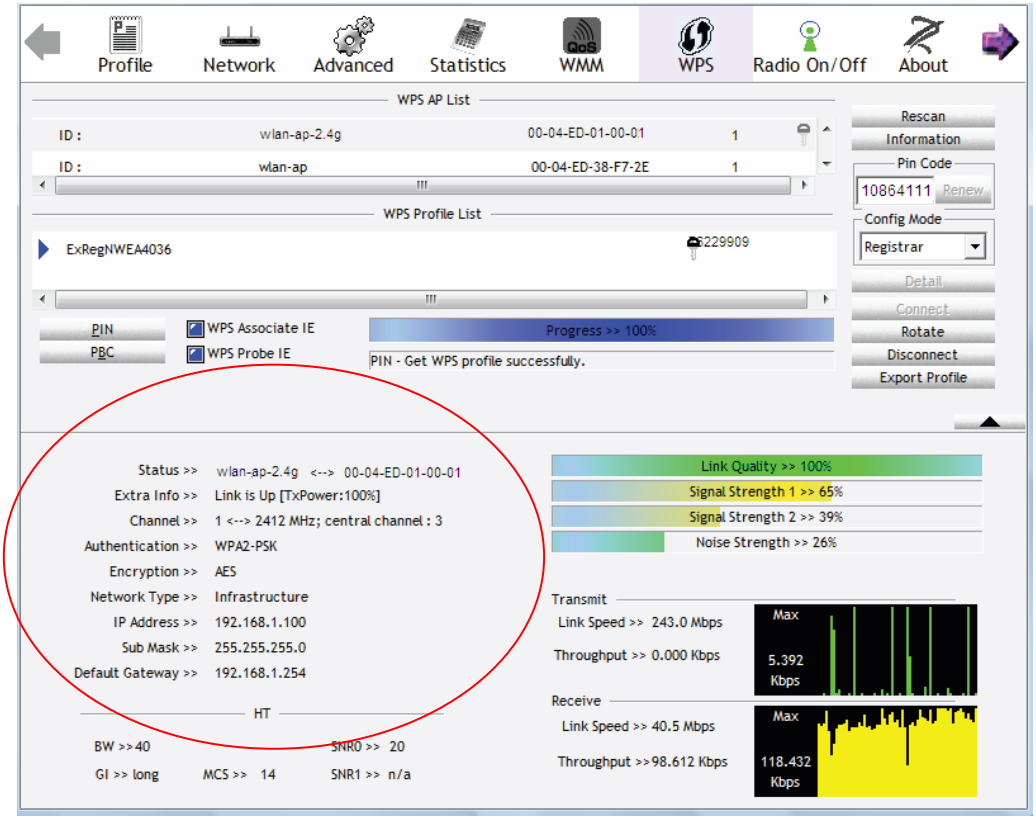


2. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as **Registrar**.

Enter the **PIN** number (13076542 (device) for example) in the PIN Code column then choose the correct AP (e.g. wlan-ap-2.4g) from the WPS AP List section before pressing the PIN button to run the scan.



3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



4. Refresh the GUI page to check new parameter settings after completing AP configuration changes.

MAC Filter

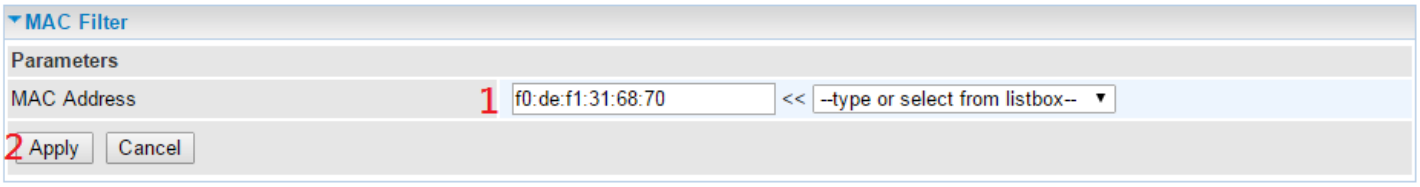
Select SSID: select the SSID you want this filter applies to.

MAC Restrict Mode:

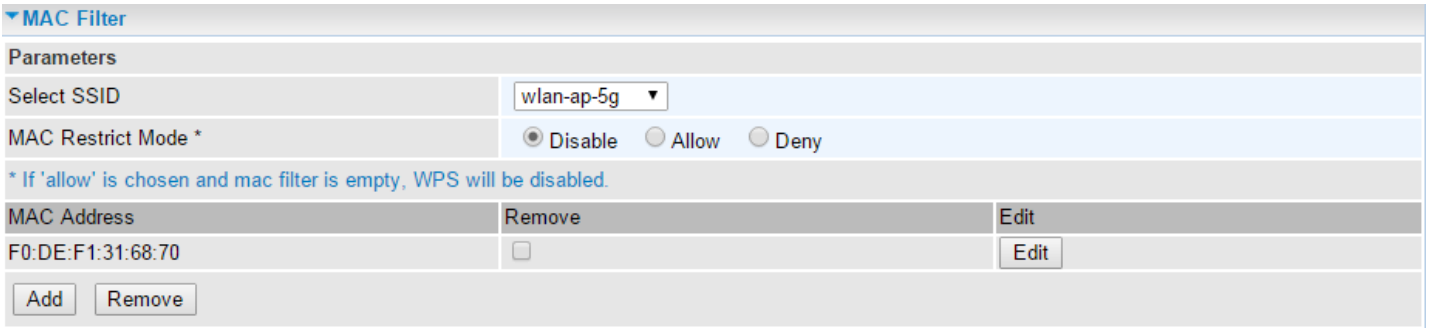
- **Disable:** disable the MAC Filter function.
- **Allow**: allow the hosts with the following listed MACs to access the wireless network.
- **Deny**: deny the hosts with the following listed MACs to access the wireless network.

Click **Add** to add a new MAC

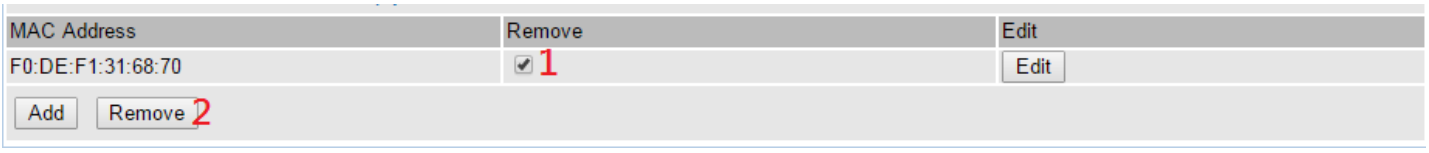
To add new MAC, enter MAC address of a device using one of these formats, xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.



Click **Apply** to apply your settings and the item will be listed under **MAC Filter** section



To delete entries, simply click the **checkbox** of the unwanted MAC address then click **Remove** to delete an entry.

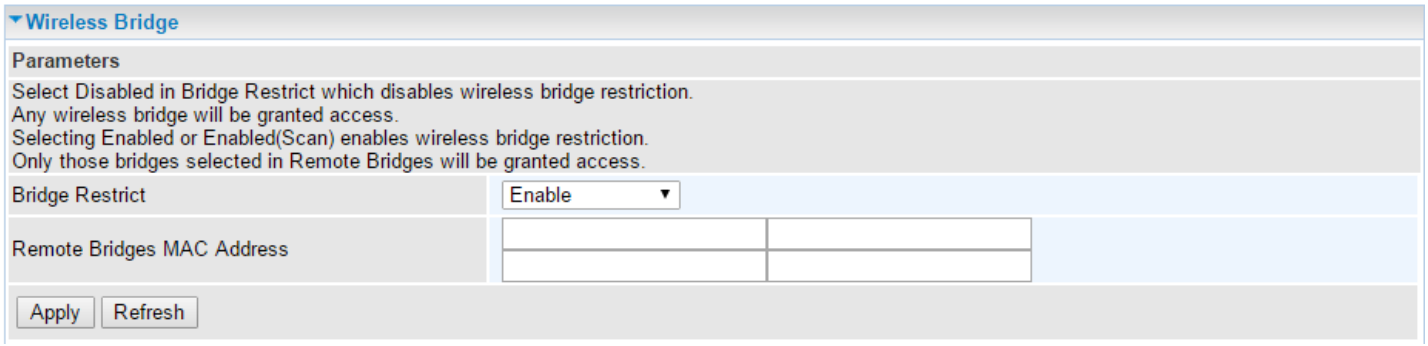


To make changes, click **Edit** of a MAC address to reconfigure the MAC as needed.

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

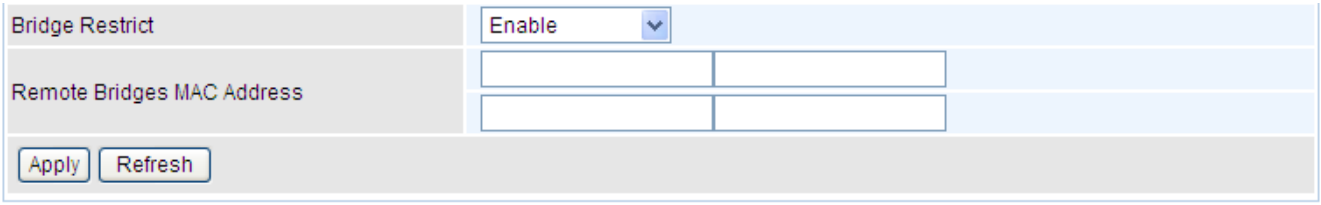
Here you can select what role the AP server has, AP or wireless bridge (WDS).



Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this determines whether the gateway will communicate with all other bridges or only specific ones:

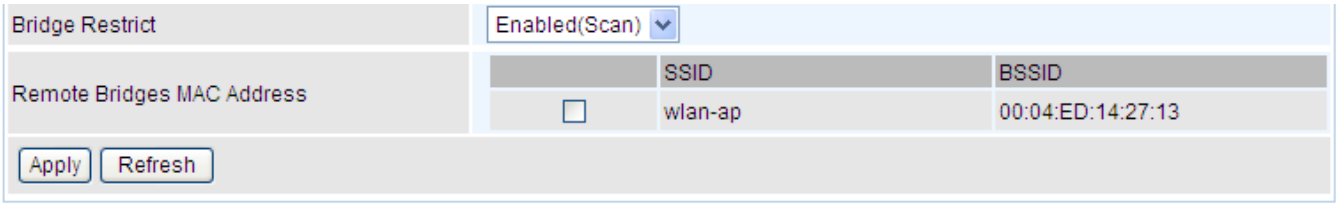
- **Enable:** to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.

  Remote Bridge MAC Address: enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

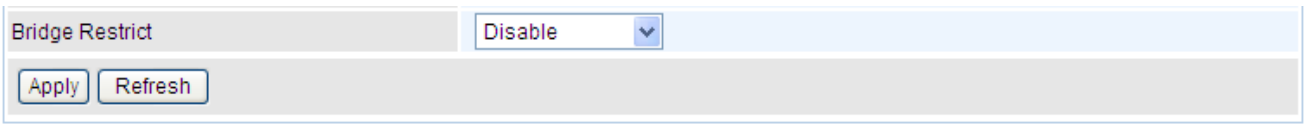


- **Enabled (Scan):** to enable wireless bridge restriction. Only those scanned by the gateway can communicate.

  Remote Bridge MAC Address: select the remote bridge MAC addresses.

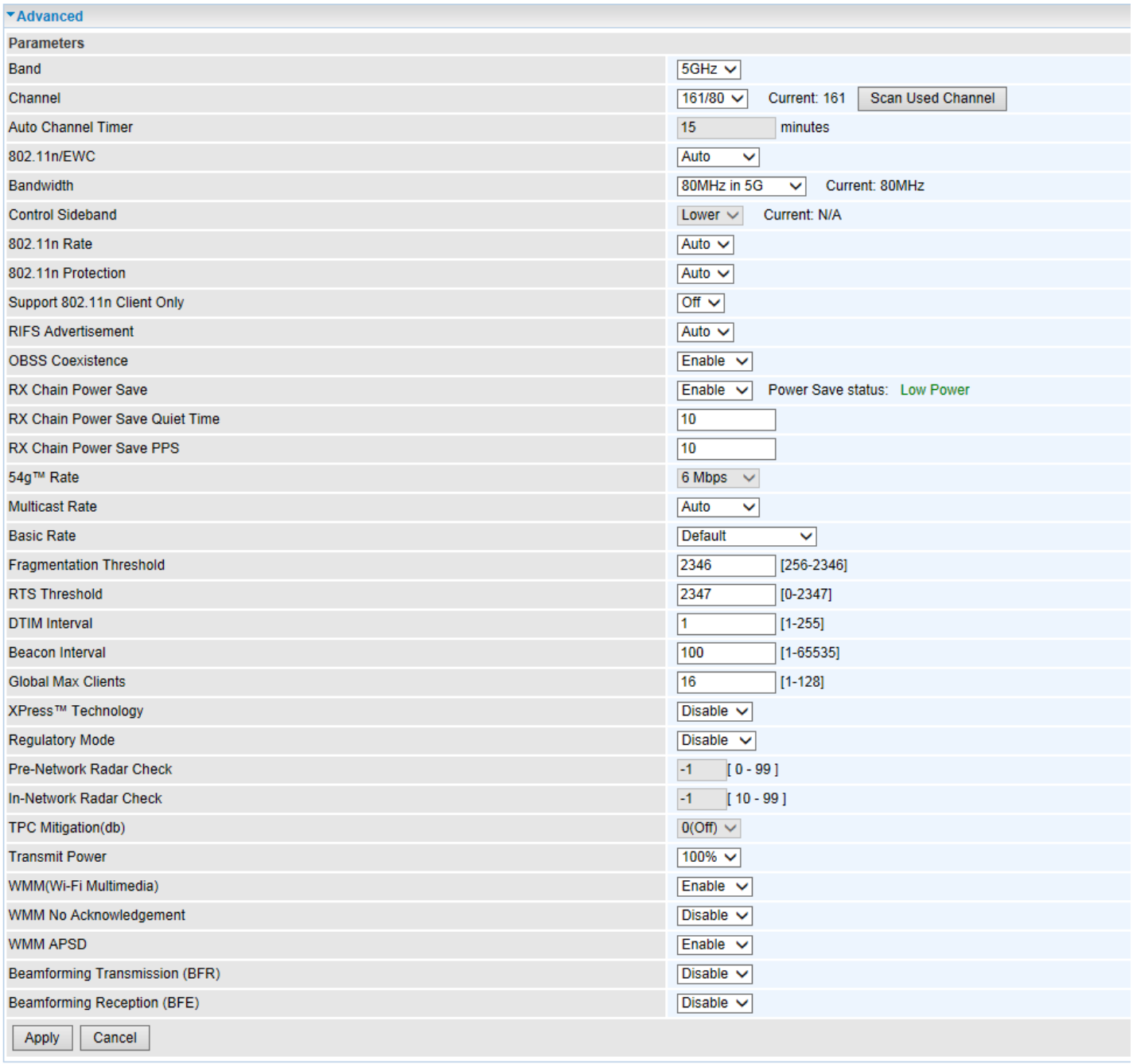


- **Disable:** Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.



Click **Apply** to apply your settings.

Advanced – 5GHz Wireless



Band: In the 5GHz radio frequency.

Channel: Choose a channel to use. Here is a list of available channels or select Auto mode instead.

- **Scan Used Channel:** Press the button to scan and list all channels being used.

Auto Channel Timer (min): Available when Auto Channel is selected. The auto channel times length it takes to scan in minutes.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: The higher the bandwidth the better the performance will be but greater interference with other wireless devices. Select **20MHz** for lessen radio interference.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower**

sideband) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: This allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximize throughput.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is an 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existence: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

RX Chain Power Save: Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

RX Chain Power Save Quiet Time: The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

RX Chain Power Save PPS: The maximum number of packets per seconds that can be processed by the WLAN interface for duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

54g™ Rate: Available after changing **802.11n Rate** to “Use 54g Rate” in **802.11n Rate**. It is used to limit 11n speed to a specific rate, e.g. 6M, 12M, 24M, 48, etc.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a specific kind of rate but a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Regulatory Mode: Select to deny any regulatory mode, which is only for **5GHz** band wireless. There are two regulatory modes:

- **802.11h:** The standard solves interference problems with e.g. satellites and radar using the same 5 GHz band as 802.11a or 802.11n dual-band access points.
- **802.11d:** This standard automatically adjusts its allowed frequencies, power levels and bandwidth accordingly to the country it's located in.

Pre-Network Radar Check (Used for 802.11h only): Specifies a period of time in seconds [0-99] to check for radar on a channel before the Access Point establishes a wireless network with the channel.

In-Network Radar Check (Used for 802.11h only): After the wireless network got established, specifies a period of time in seconds [10-99] to check for radar when switching to another non-radar channel.

TPC Mitigation (db): Known as Transmitter Power Control mitigation to reduce unnecessary transmitting power radio and possible radio interference to other users.

Transmit Power: select the transmitting power of your wireless signal.

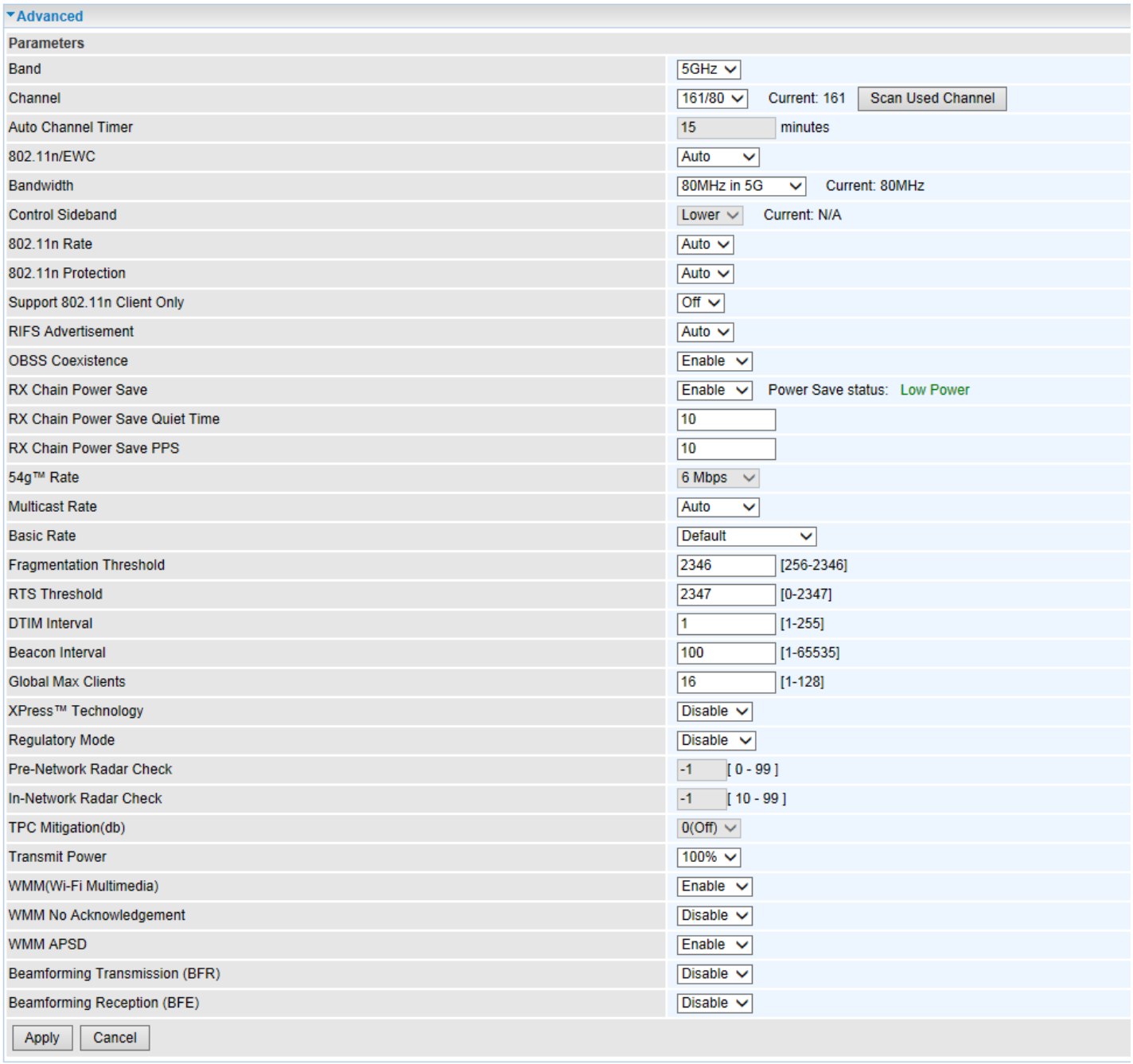
WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Beamforming Transmission (BFR) / Beamforming Reception (BFE): Enable to increase wireless speed by focusing and concentrating transmitted (send) and/or receive signals with a wireless client instead of broadcast signals in all directions. **Note**: Both router and client wireless must support beamforming technology.

Advanced – 2.4GHz Wireless



Band: In the 2.4 GHz radio frequency.

Channel: Choose a channel to use. Here is a list of available channels or select Auto mode instead.

- **Scan Used Channel:** Press the button to scan and list all channels being used.

Auto Channel Timer (min): Available when Auto Channel is selected. The auto channel times length it takes to scan in minutes.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: The higher the bandwidth the better the performance will be but greater interference with other wireless devices. Select **20MHz** for lessen radio interference.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower**

sideband) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: This allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximize throughput.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is an 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existence: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

RX Chain Power Save: Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

RX Chain Power Save Quiet Time: The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

RX Chain Power Save PPS: The maximum number of packets per seconds that can be processed by the WLAN interface for duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

54g™ Rate: Available after changing **802.11n Rate** to “Use 54g Rate” in **802.11n Rate**. It is used to limit 11n speed to a specific rate, e.g. 1M, 6M, 12M, 24M, 48M, etc.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a specific kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Transmit Power: select the transmitting power of your wireless signal.

WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

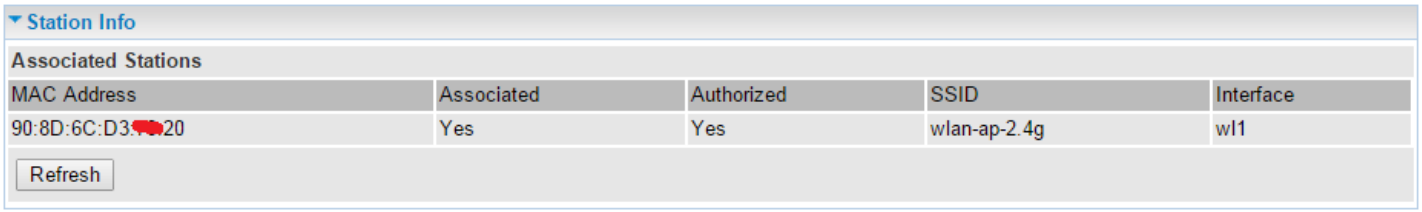
WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Beamforming Transmission (BFR) / Beamforming Reception (BFE): Enable to increase wireless speed by focusing and concentrating transmitted (send) and/or receive signals with a wireless client instead of broadcast signals in all directions. **Note**: Both router and client wireless must support beamforming technology.

Station Info

Here you can view information about the wireless clients.



MAC Address: The MAC address of the wireless clients.

Associated: List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access**.**

SSID: Show the current SSID of the client.

Interface: To show which interface the wireless client is connected to

- **wl0** : Refers to 5GHz Wireless Interface
- **wl1** : Refers to 2.4GHz Wireless Interface

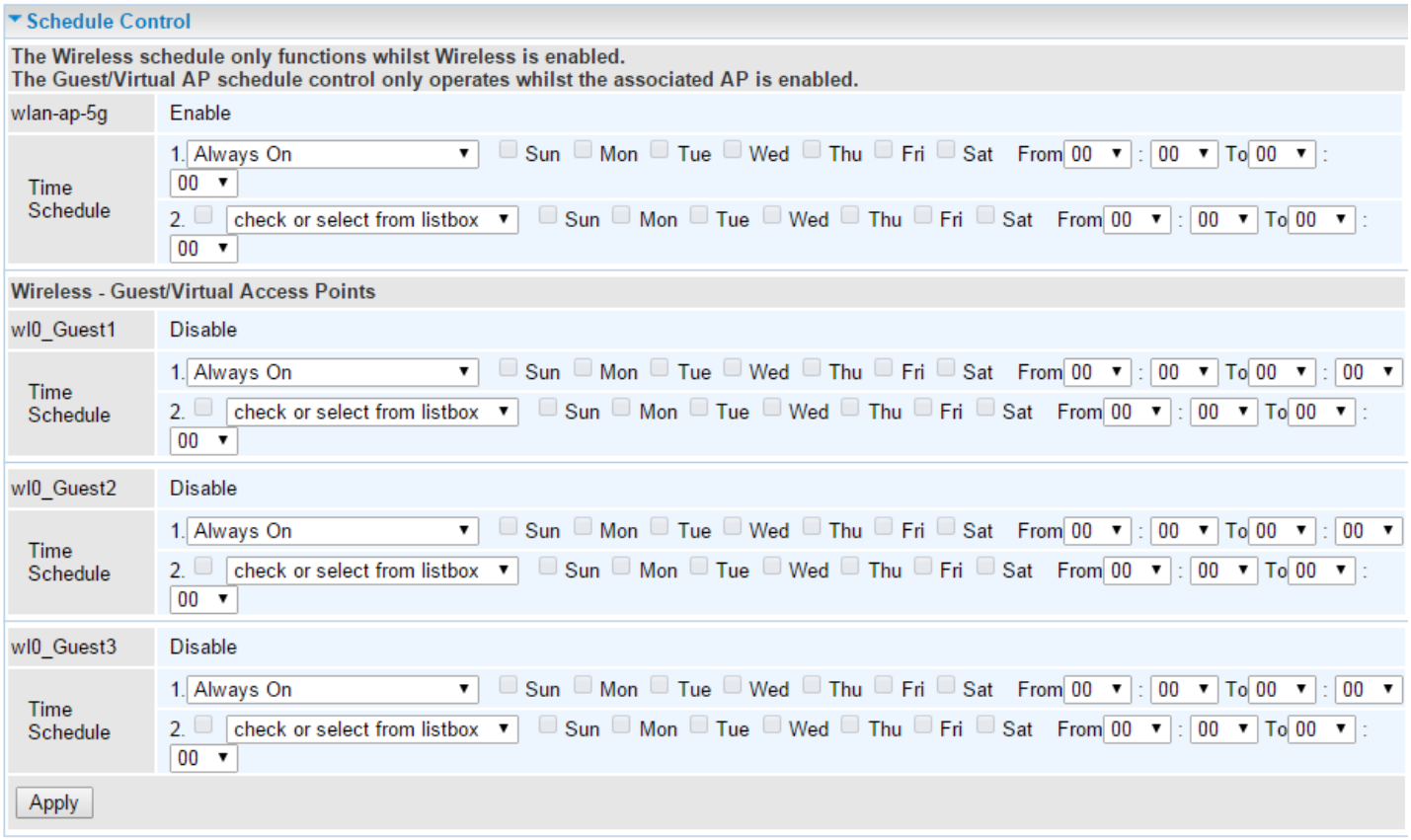
Refresh: To get the latest update.

Schedule Control

Schedule control is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access.

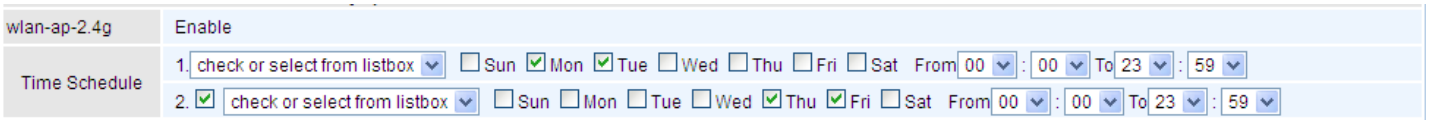
The Wireless schedule only functions whilst Wireless is enabled.
The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

For detail setting the timeslot, user can turn to Time Schedule .



Time Schedule: Set when the SSID works. If user wants the SSID works all the time, please select "Always On"; if not, please set or select the exact time your want the SSID works. Here user can set two separate intervals.

For example: user wants the SSID "*wlan-ap-2.4g*" to work on weekdays except for Wednesday, under this circumstance, user can set as shown below.



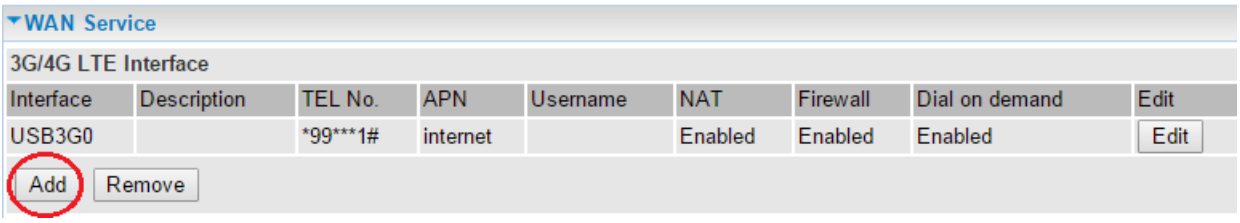
WAN - Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (e.g. Internet) that is used to connect LAN and other types of network systems.

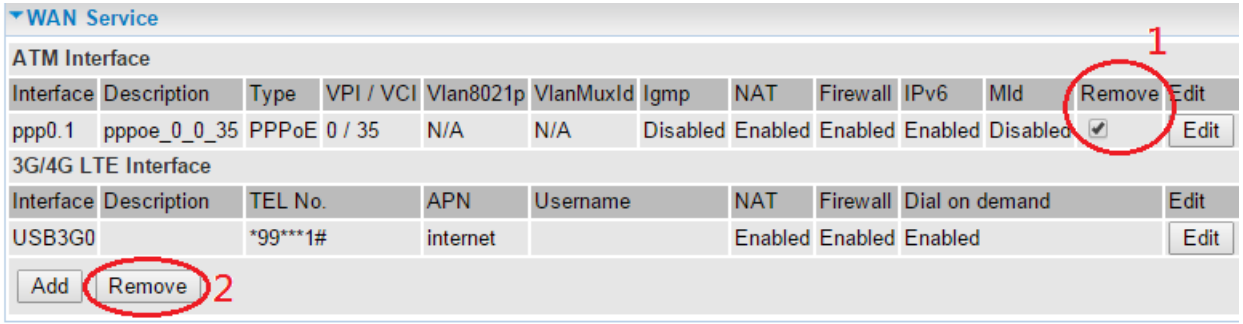
WAN Service

BEC 8920AC provides three different Internet interface for WAN connection, VDSL/ADSL, Ethernet WAN and 3G/4G_LTE via USB interface.

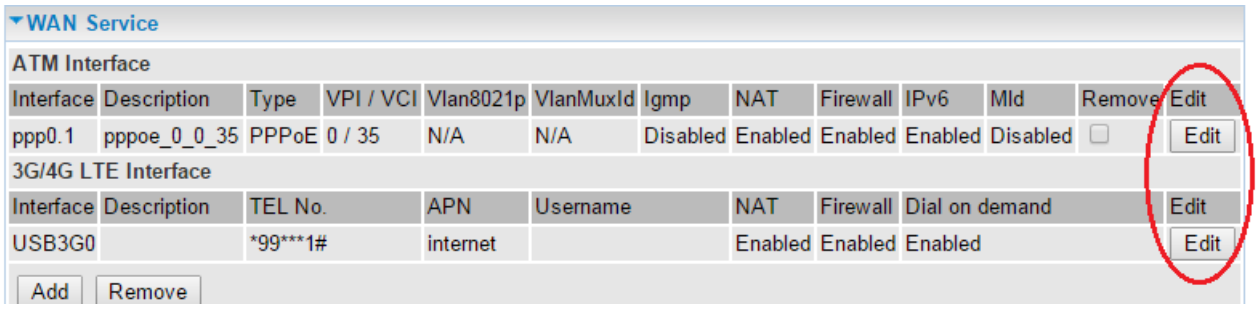
To add new entries, click **Add** to add a new WAN interface.



To delete entries, simply click the **checkbox** of the unwanted WAN interface then press **Remove** to delete an entry.



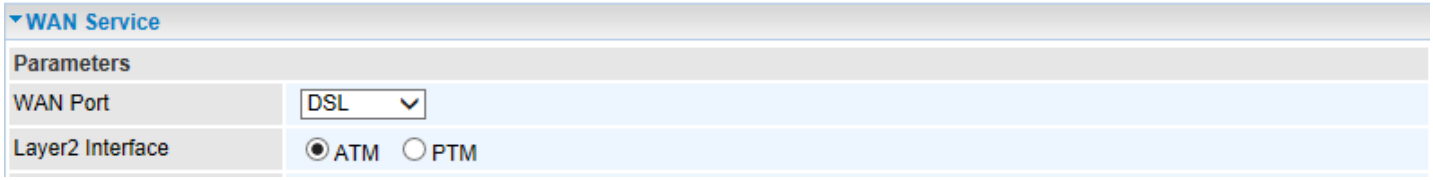
To make changes, click **Edit** button of a WAN entry to re-configure the settings.



To check WAN connection, go to **Status >WAN** or **Summary** to check and review your WAN connection status.

❖ VDSL / ADSL (xDSL) Connection Setup

In DSL mode, there are two transfer modes for you to configure for WAN connection, namely ATM and PTM, configuration of PTM mode is similar as ATM mode, here take ATM mode WAN configuration for example.



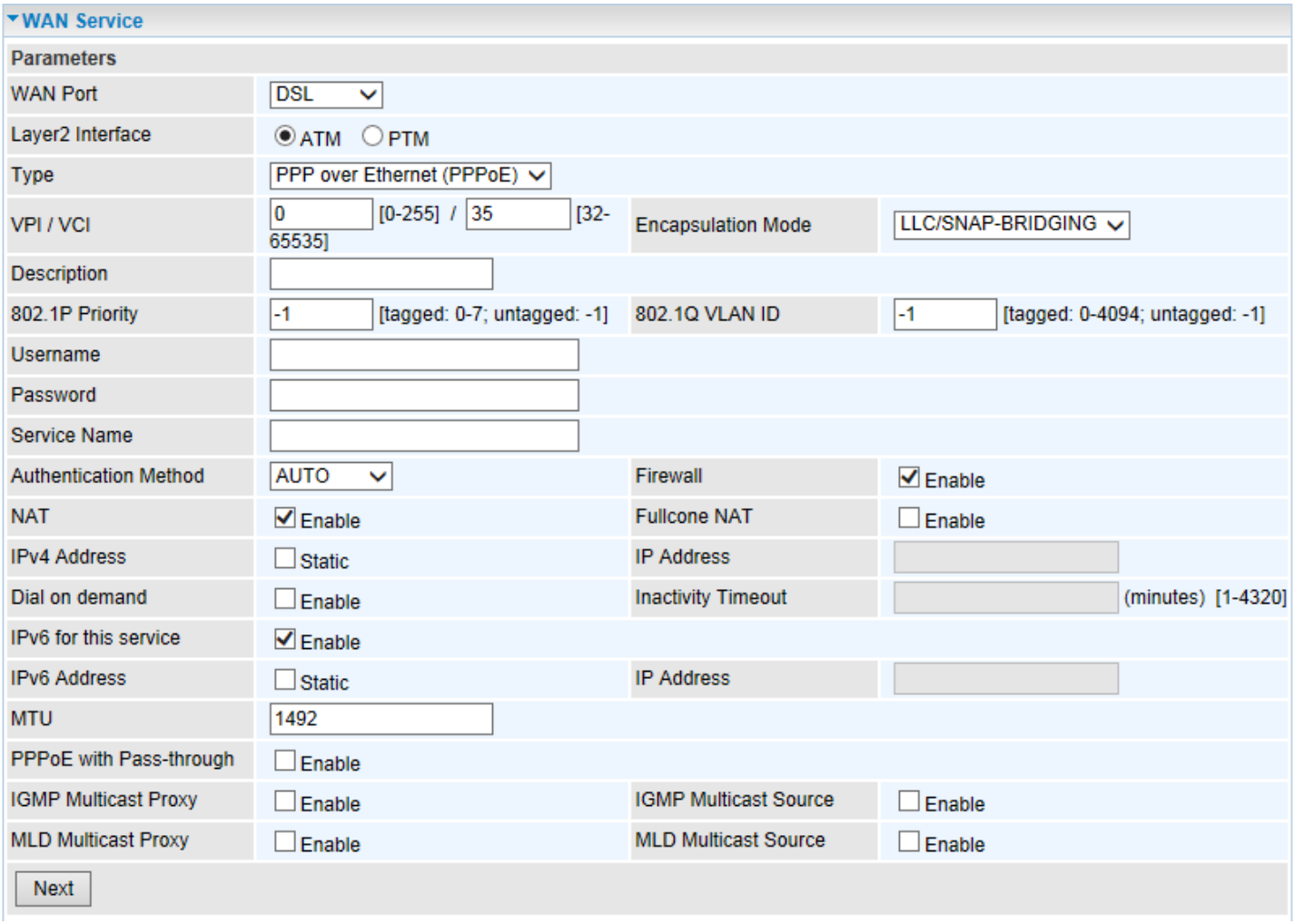
Layer2 Interface: There are two (2) transfer modes available, ATM and PTM. This information should be provided by your Internet Service Provider, please consult them for more information.

Type (Internet Protocols): Provides a list of Internet protocols. This information shall be provided by your Internet Service Provider, please consult them for more information.

Protocols in details are in the following pages.

xDSL Internet Protocol - PPPoE

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



VCP/VPI (For ATM Mode only): Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode (For ATM Mode only): Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged: -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purposes, user can define this.

Authentication Method: Default is set to **Auto**. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand; users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

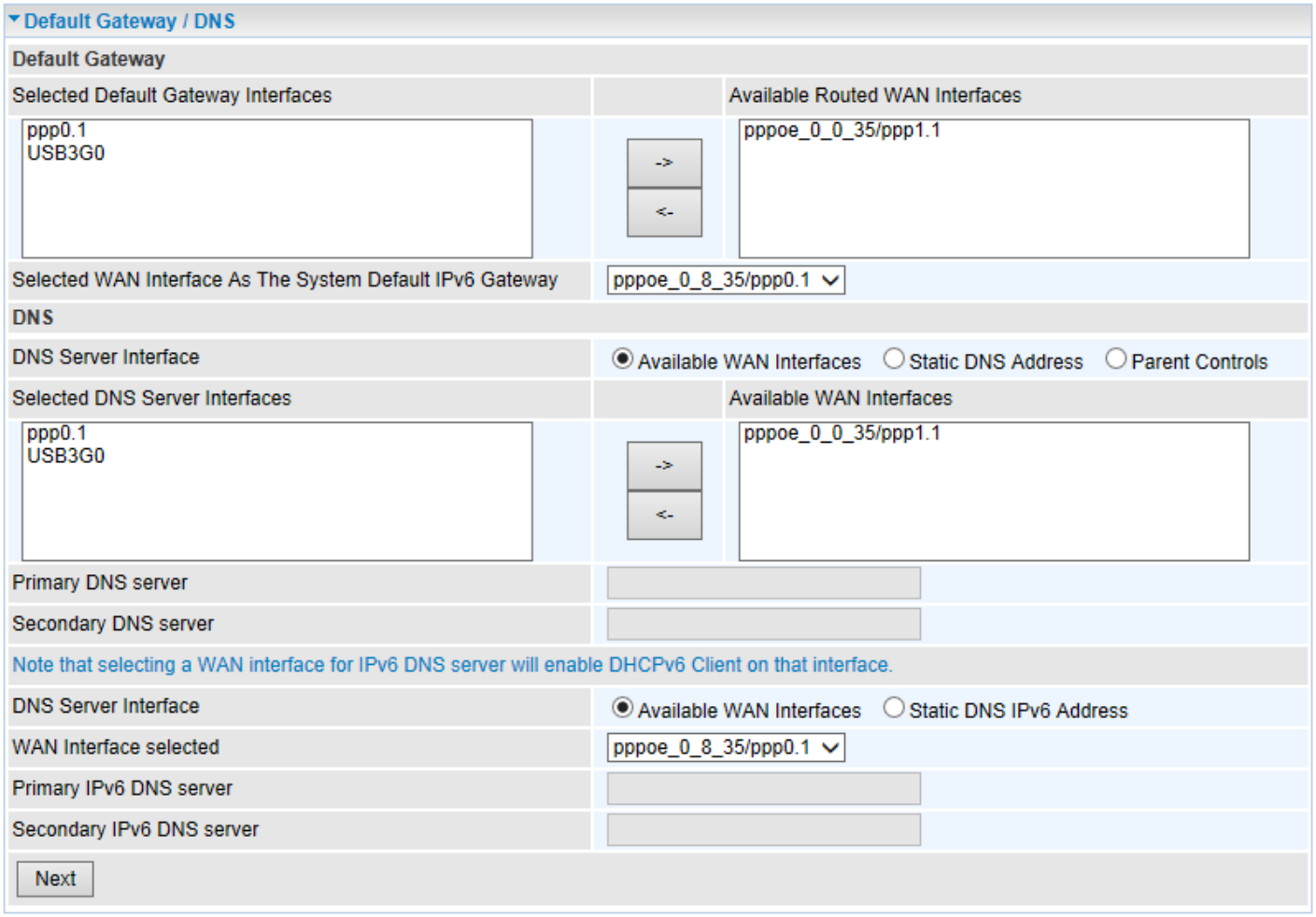
IGMP Multicast Proxy (for IPv4): Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the interested clients. (Only available in IGMPv3)

MLD Multicast Proxy (for IPv6): check whether to enable this function. MLD (**Multicast Listener Discovery Protocol**) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. It takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Default Gateway

- **IPv4**

Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

- **IPv6**

When enabling **IPv6** for external interface, please specify the default IPv6 gateway from **Selected WAN Interface as the System Default IPv6 Gateway.**

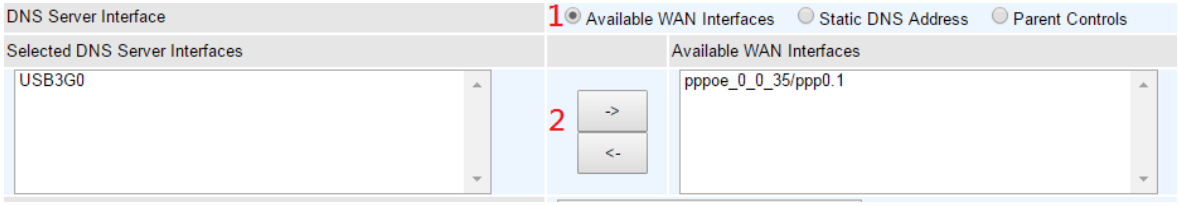
DNS

- **IPv4**

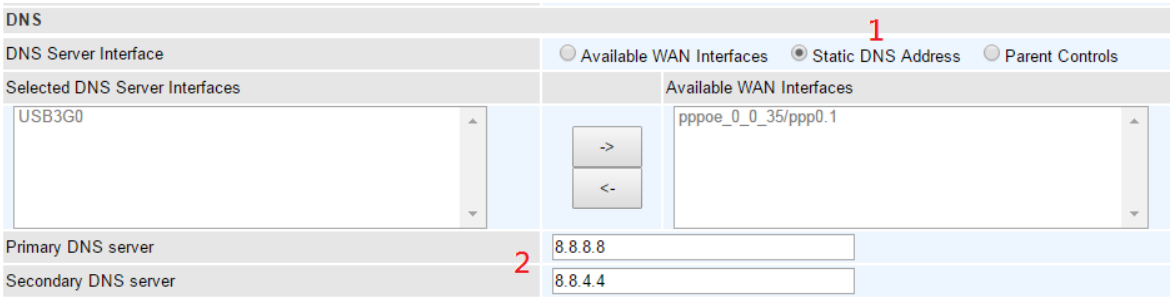
DNS Server Interfaces

1. **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

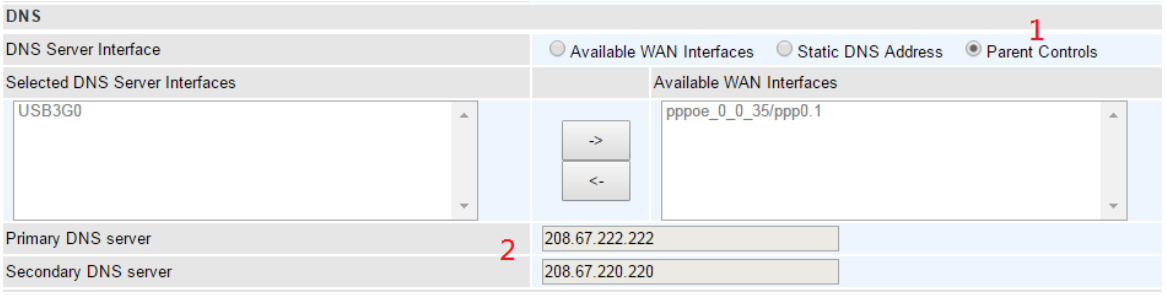
   To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



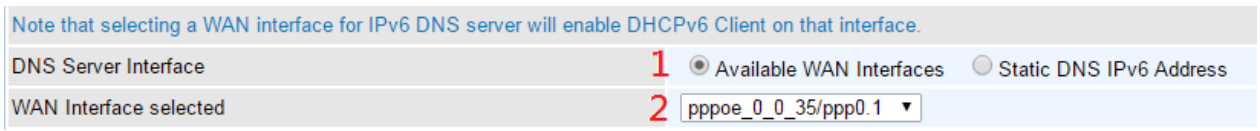
3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).



- **IPv6**

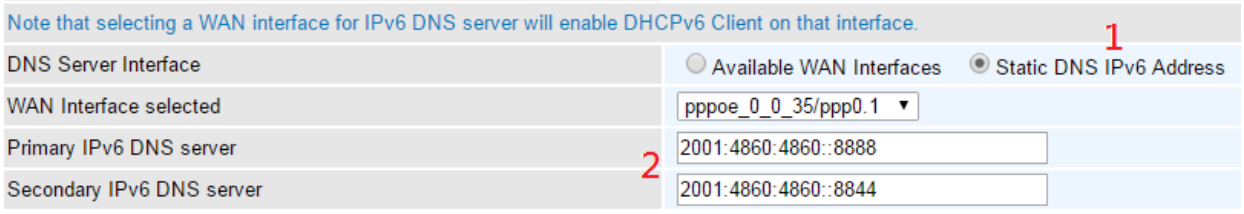
DNS Server Interfaces

1. **Available WAN interfaces:** If your Internet Service Provider assigns DNS server address along with the WAN connection, please select an appropriated Ipv6 WAN interface from **DNS Server Interface.**

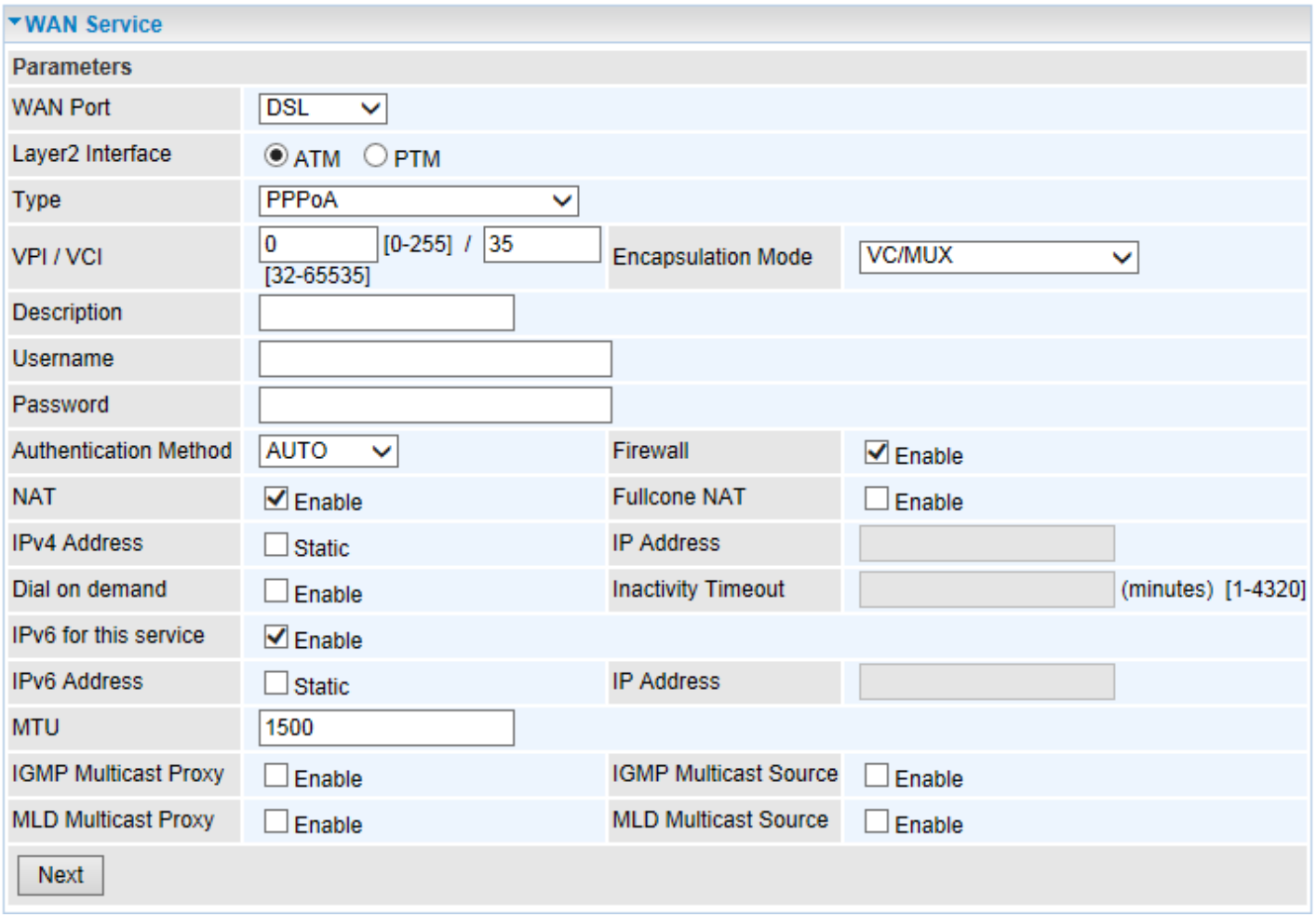


2. **Static DNS IPv6 Address:** If your Internet Service Provide does not provide or you wish to use other DNS servers for your network, simply manually enter other DNS server IP address here:

Primary / Secondary IPv6 DNS Server: Enter the specific primary and secondary IPv6 DNS Server address.



xDSL Internet Protocol - PPPoA



VCP/VPI: Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged: -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purposes, user can define this.

Authentication Method: Default is set to **Auto**. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own

public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If **Static** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand; users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If **Static** is enabled in the above field, enter the static IPv4 address.

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

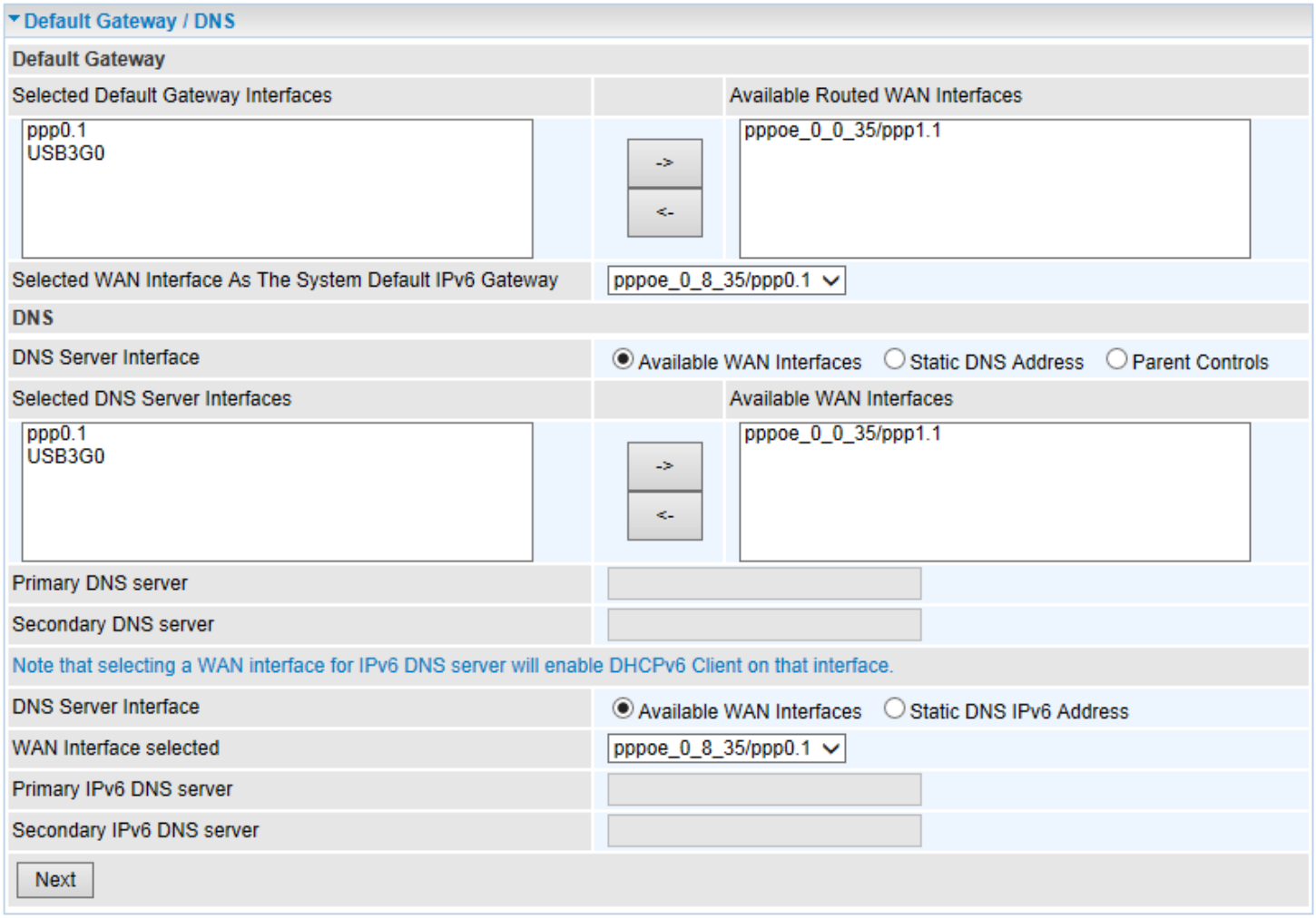
IGMP Multicast Proxy (for IPv4): Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the interested clients. (Only available in IGMPv3)

MLD Multicast Proxy (for IPv6): check whether to enable this function. MLD (**Multicast Listener Discovery Protocol**) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. It takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6



Default Gateway

- **IPv4**

Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

- **IPv6**

When enabling **IPv6** for external interface, please specify the default IPv6 gateway from **Selected WAN Interface as the System Default IPv6 Gateway.**

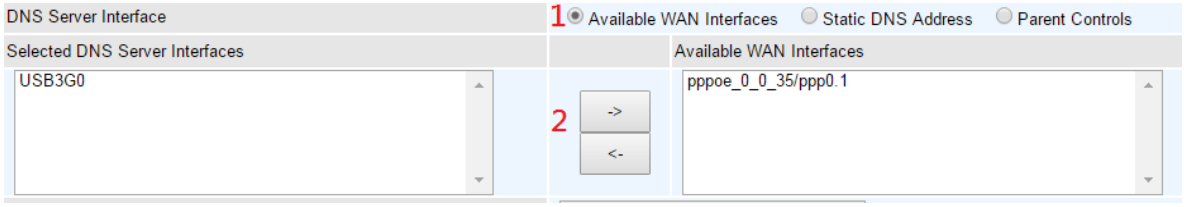
DNS

- **IPv4**

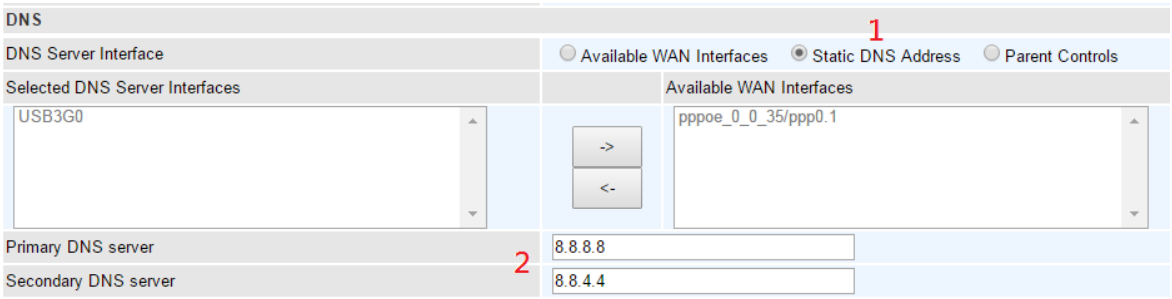
DNS Server Interfaces

1. **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

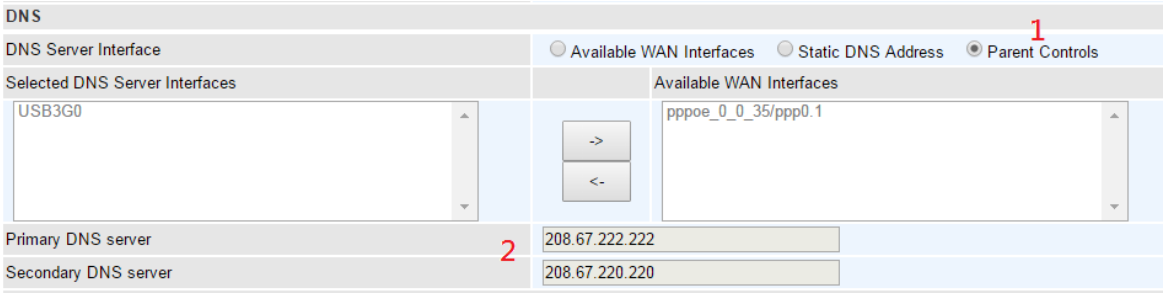
   To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



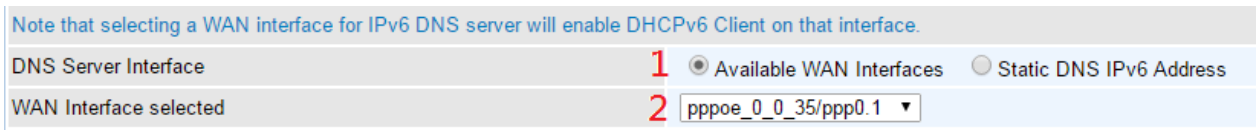
3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).



- **IPv6**

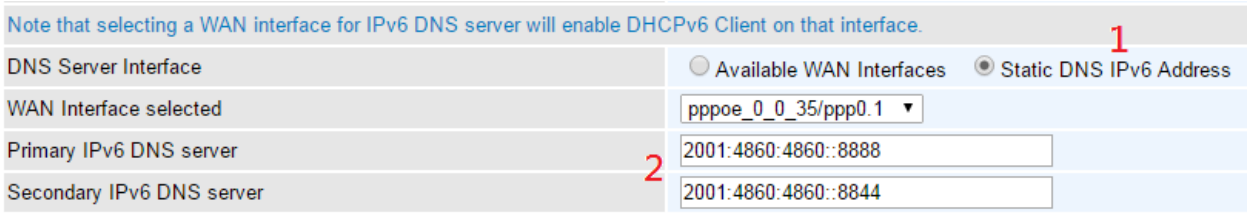
DNS Server Interfaces

1. **Available WAN interfaces:** If your Internet Service Provider assigns DNS server address along with the WAN connection, please select an appropriated Ipv6 WAN interface from **DNS Server Interface.**

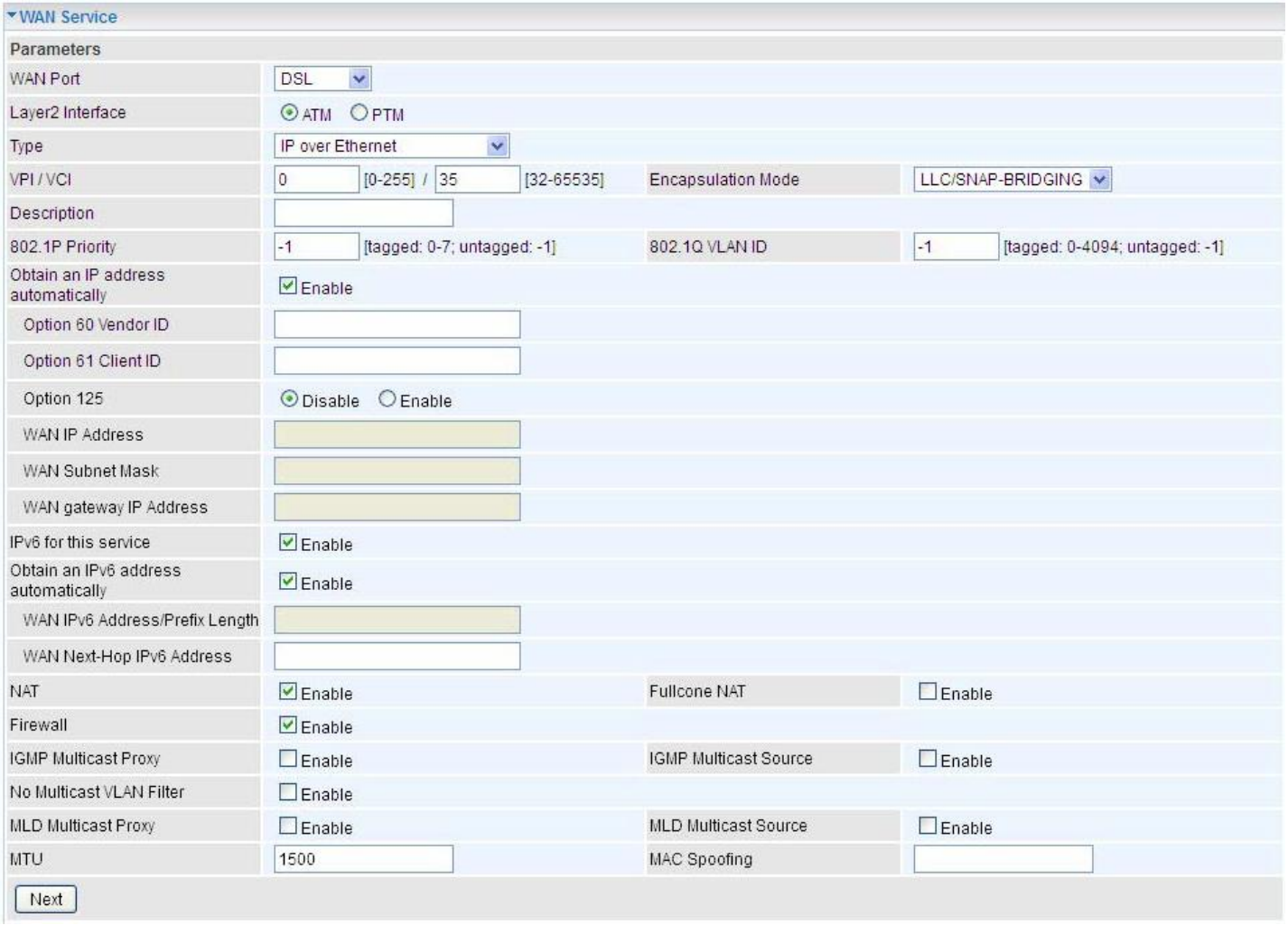


2. **Static DNS IPv6 Address:** If your Internet Service Provide does not provide or you wish to use other DNS servers for your network, simply manually enter other DNS server IP address here:

Primary / Secondary IPv6 DNS Server: Enter the specific primary and secondary IPv6 DNS Server address.



xDSL Internet Protocol - IP over Ethernet



VCP/VPI (For ATM Mode only): Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode (For ATM Mode only): Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged: -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

WAN IP Address

- **IPv4 – Automatic**

  Obtain an IP address automatically: Enable to receive a WAN (public) IP address from your Internet Service Provider. This information should be provided by your ISP, please consult them for more information.

(Option) Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

(Option) Option 61 ClientID: Enter the associated information provided by your ISP.

(Option) Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the pre-stored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is set to **Disable**.

NOTE: Leave them blink / disable unless you are instructed by your Internet Service Provider.

- **IPv4 – Manual Input**

  Manual Configure WAN IP Address: Specify your WAN (public) IPv4 address (xxx.xxx.xxx.xxx) to the device provided by your ISP.

  Manual Configure WAN Subnet Mask: Enter submask provided by your ISP.

  Manual Configure WAN Gateway IP: Enter gateway IP address provided by your ISP.

  IPv6 for this service: Enable to use IPv6 service.

- **IPv6 – Automatic**

  Obtain an IPv6 address automatically: Enable to receive an IPv6 WAN address from your Internet Service Provider. This information should be provided by your ISP, please consult them for more information.

- **IPv6 – Manual Input**

  WAN IPv6 Address/Prefix Length: Specify WAN IPv6 Address/Prefix Length. The information shall be provided by your ISP.

  WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast Proxy (for IPv4): Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the

interested clients. (Only available in IGMPv3)

No Multicast VLAN Filter: Enable to deactivate multicast filtering. All multicast packets will be forwarded to all ports in the relevant VLANs.

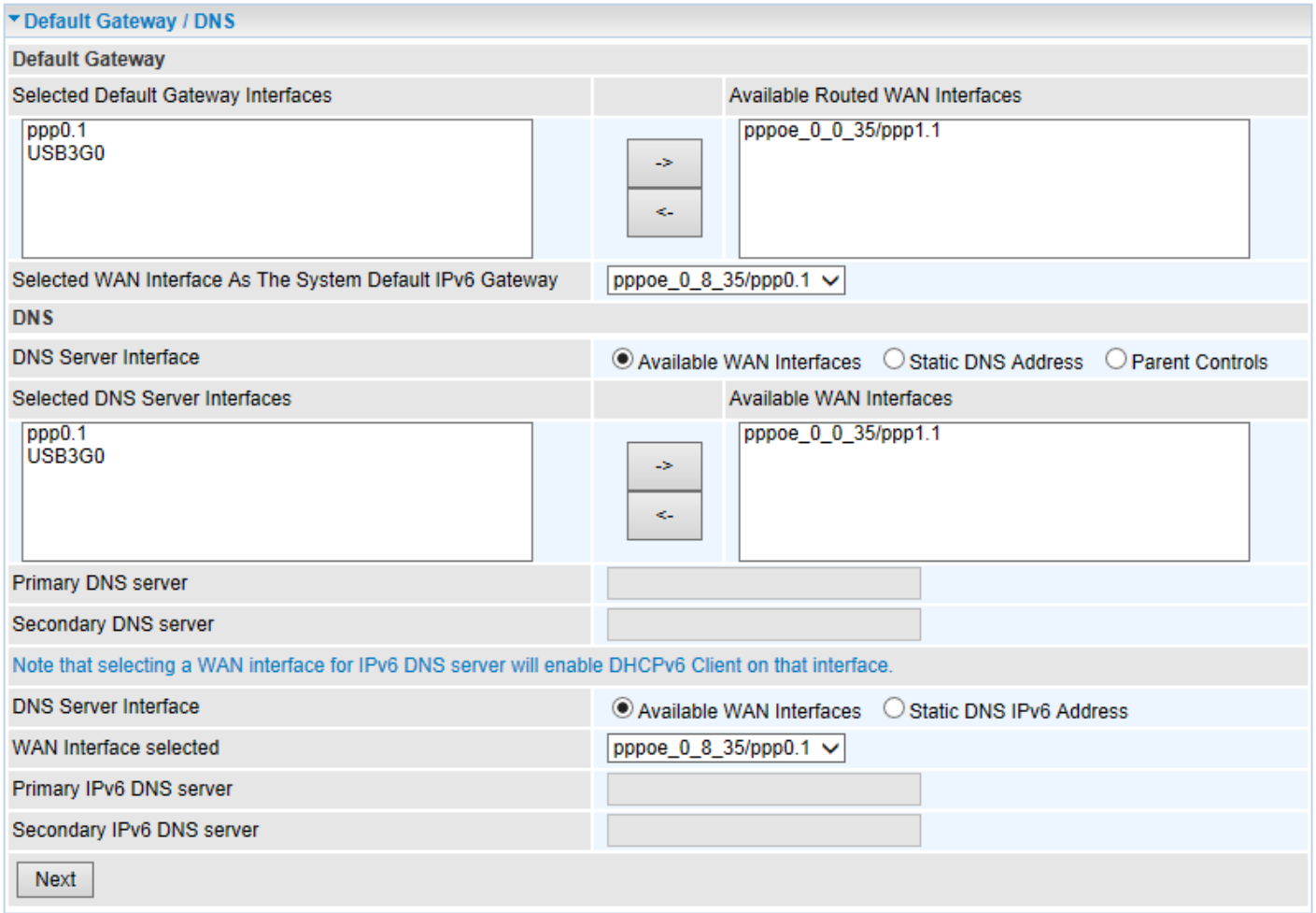
MLD Multicast Proxy (for IPv6): check whether to enable this function. MLD (**Multicast Listener Discovery Protocol**) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. It takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

MAC Spoofing: This option is required by some service providers specifying some specific MAC allowed for joining network. You must fill in the MAC address specified by your service provider when this information is required.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Default Gateway

- **IPv4**

Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway**

Interface box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

- **IPv6**

When enabling **IPv6** for external interface, please specify the default IPv6 gateway from **Selected WAN Interface as the System Default IPv6 Gateway.**

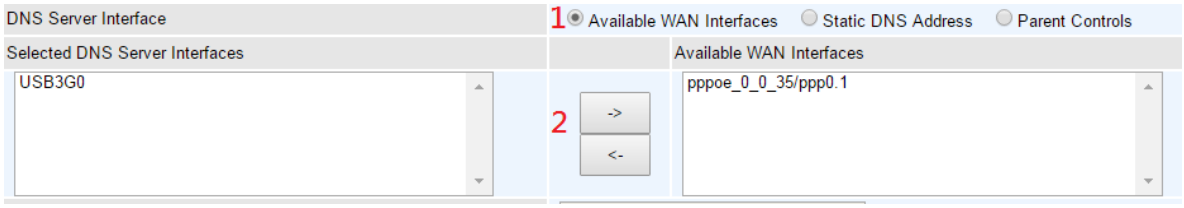
DNS

- **IPv4**

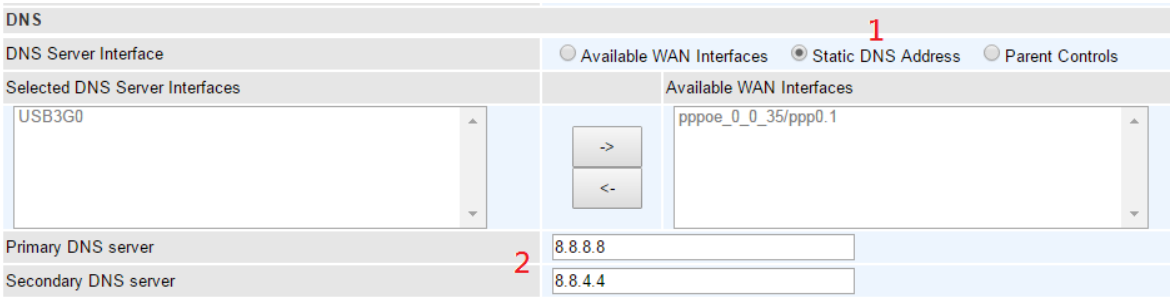
DNS Server Interfaces

1. **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

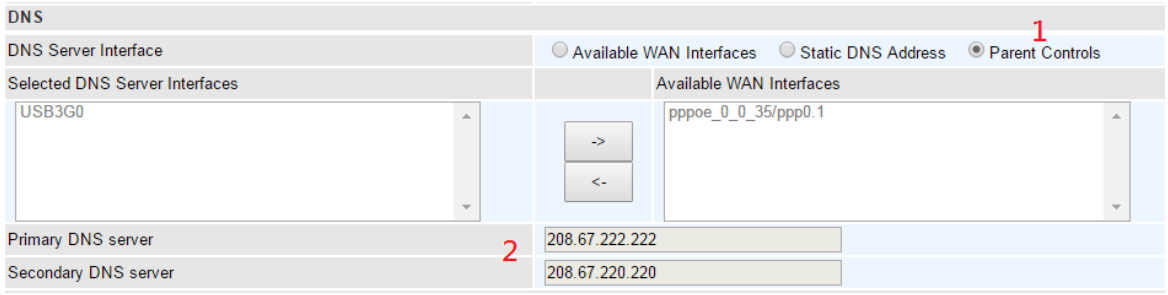
   To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

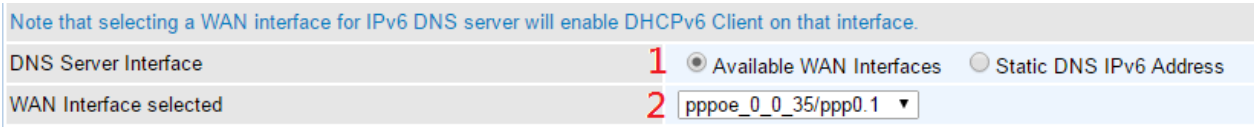


- **IPv6**

DNS Server Interfaces

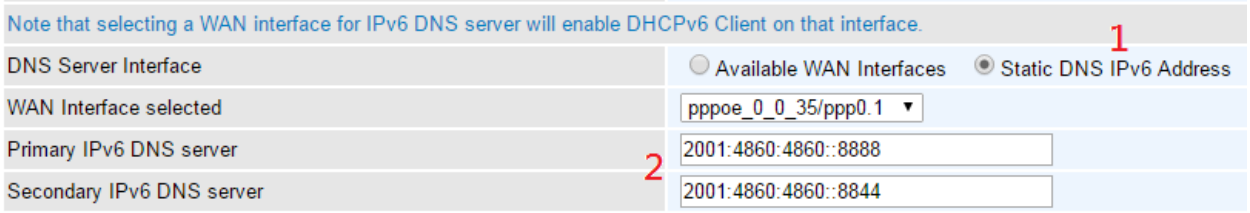
1. **Available WAN interfaces:** If your Internet Service Provider assigns DNS server address

along with the WAN connection, please select an appropriated Ipv6 WAN interface from **DNS Server Interface.**

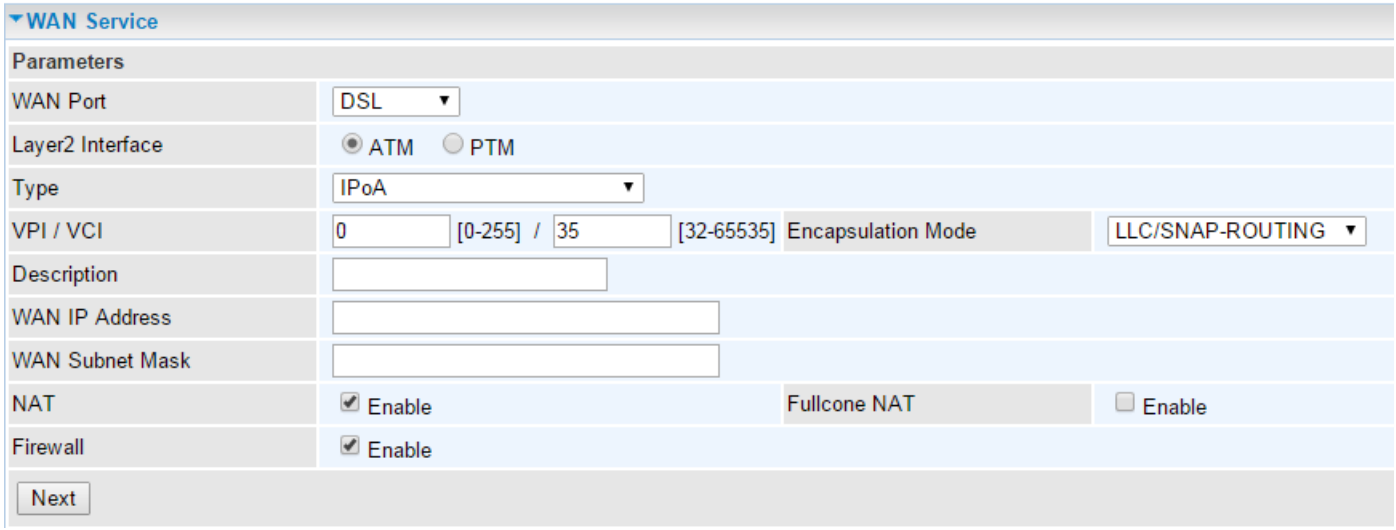


2. **Static DNS IPv6 Address:** If your Internet Service Provide does not provide or you wish to use other DNS servers for your network, simply manually enter other DNS server IP address here:

Primary / Secondary IPv6 DNS Server: Enter the specific primary and secondary IPv6 DNS Server address.



xDSL Internet Protocol - IPoA



VCP/VPI: Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

WAN IP Address: Specify your WAN (public) IPv4 address (xxx.xxx.xxx.xxx) to the device provided by your ISP.

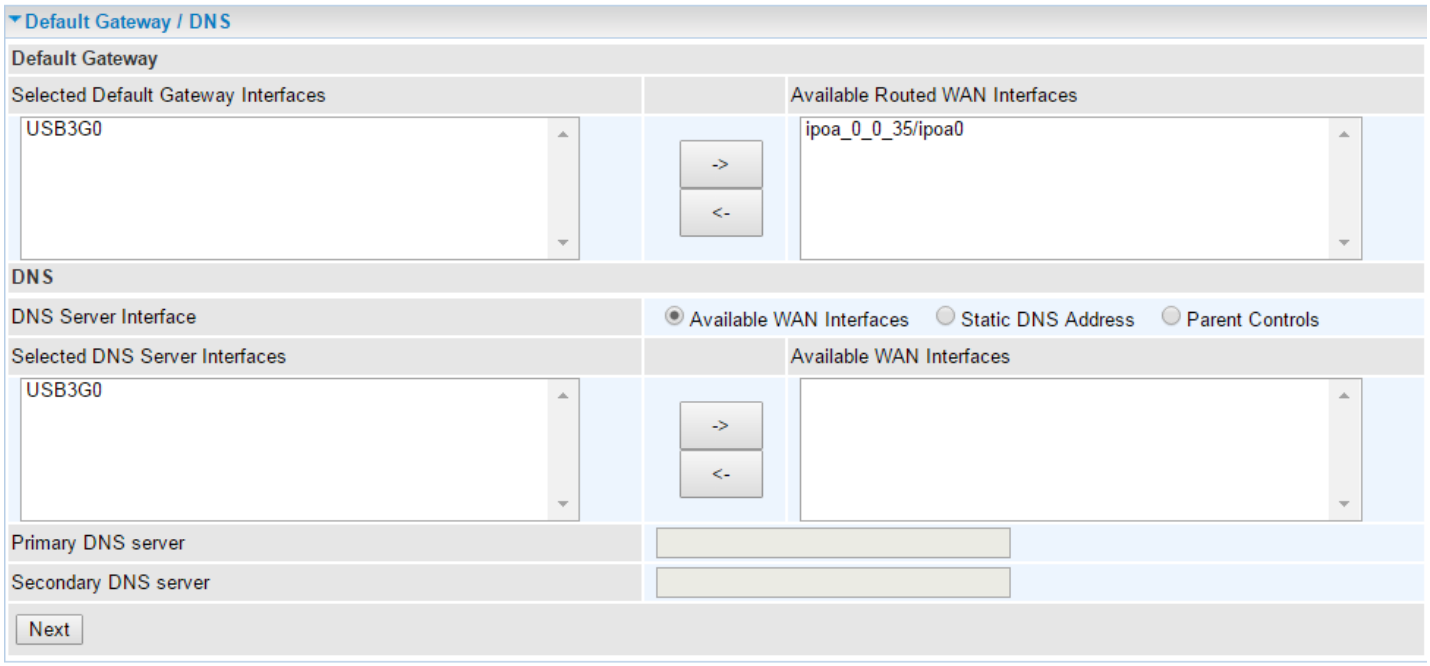
WAN Subnet Mask: Enter submask provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

Click **Next** to continue to set the default gateway and DNS IP address.



Default Gateway

Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

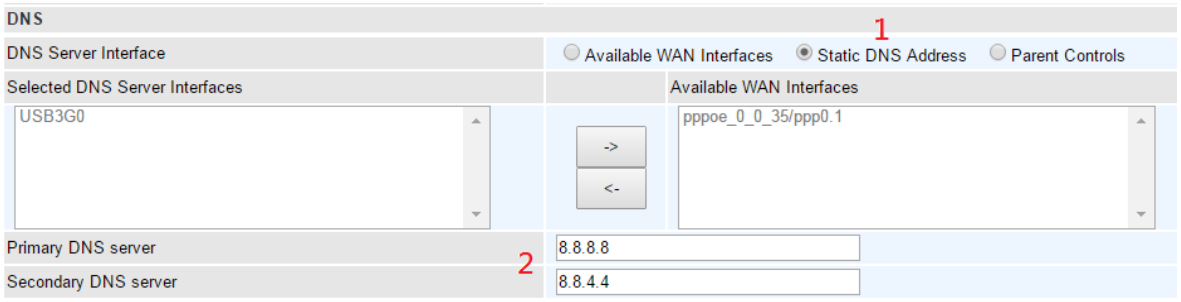
DNS

DNS Server Interfaces

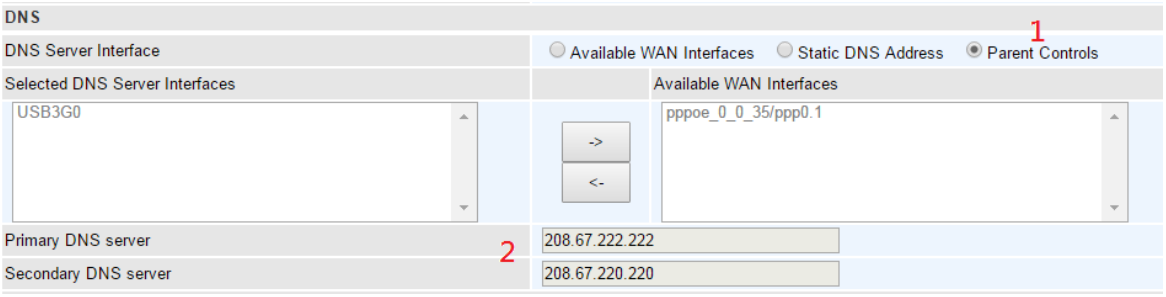
- **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

  To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

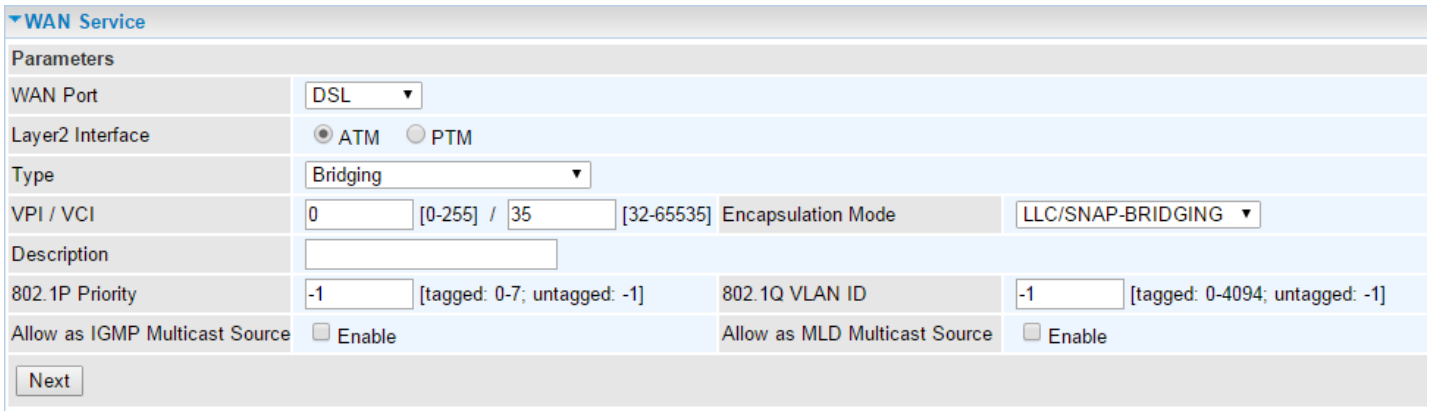
- **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



- **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).



xDSL Internet Protocol - Bridging



VCP/VPI (For ATM Mode only): Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode (For ATM Mode only): Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged: -1.

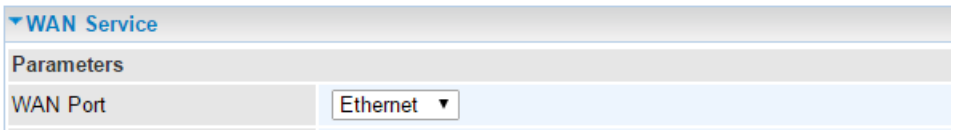
Allow as IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the interested clients. (Only available in IGMPv3)

Allow as MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

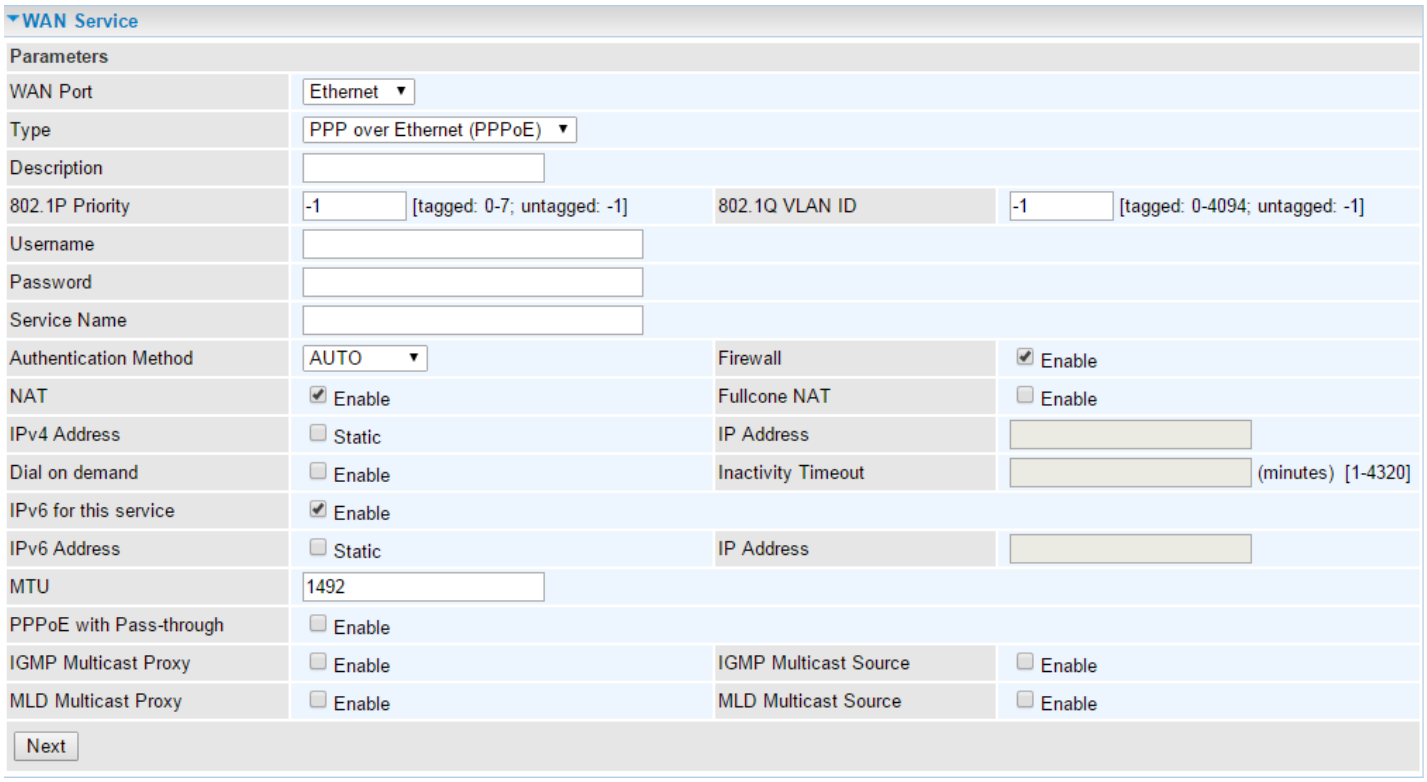
❖ Ethernet WAN (EWAN) Connection Setup

The Ethernet 5 is an interchangeable LAN/WAN port. Connect LAN5/EWAN port with a Fiber, Cable, or xDSL modem with a RJ-45 cable.

WAN Port: Select **Ethernet** to change LAN 5 port functionality.



EWAN Internet Protocol - PPPoE



Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purposes, user can define this.

Authentication Method: Default is set to ***Auto***. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet

through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand; users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If **Static** is enabled in the above field, enter the static IPv4 address.

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

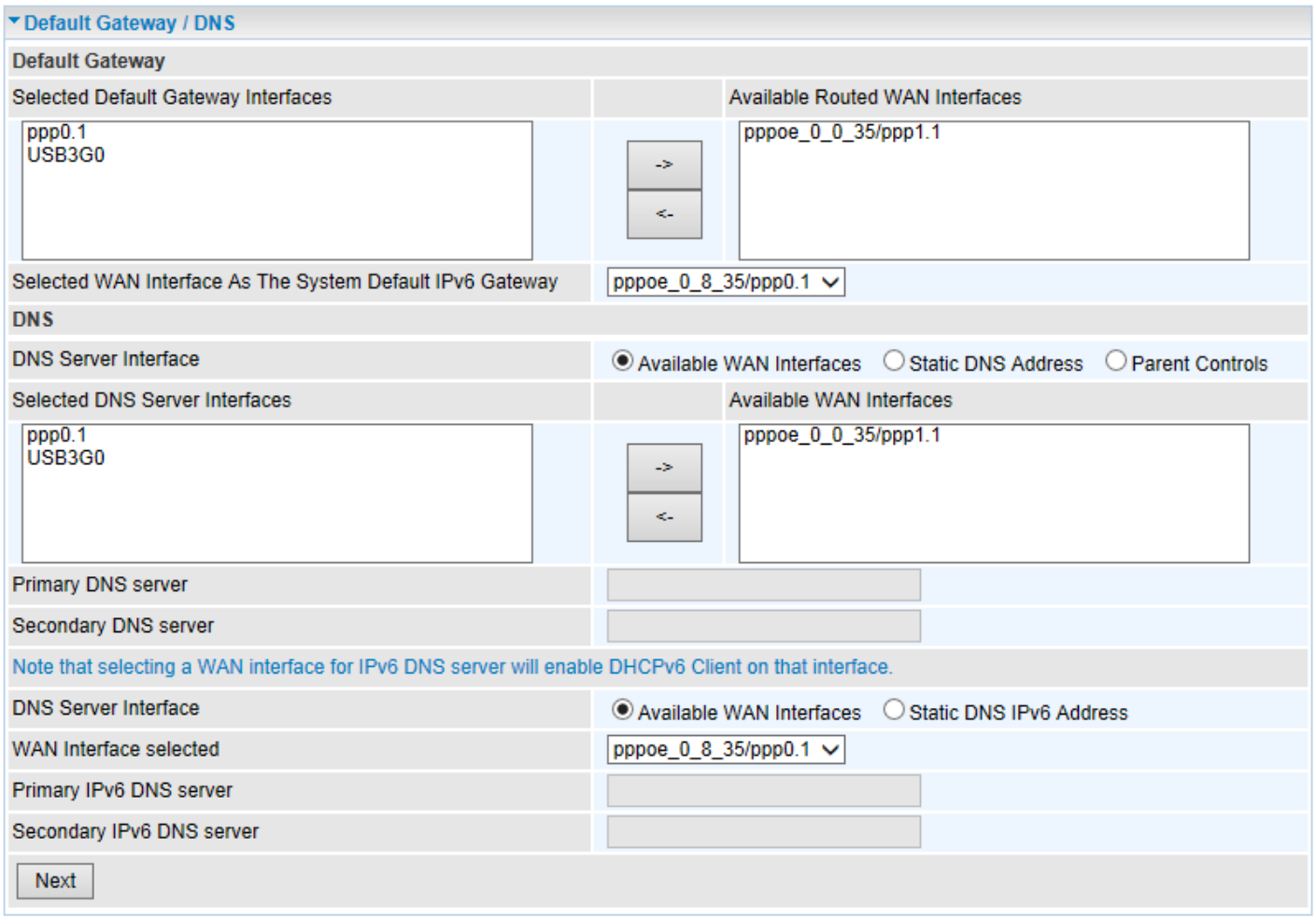
IGMP Multicast Proxy (for IPv4): Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the interested clients. (Only available in IGMPv3)

MLD Multicast Proxy (for IPv6): check whether to enable this function. MLD (**Multicast Listener Discovery Protocol**) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. It takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Default Gateway

- **IPv4**

Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

- **IPv6**

When enabling **IPv6** for external interface, please specify the default IPv6 gateway from **Selected WAN Interface as the System Default IPv6 Gateway.**

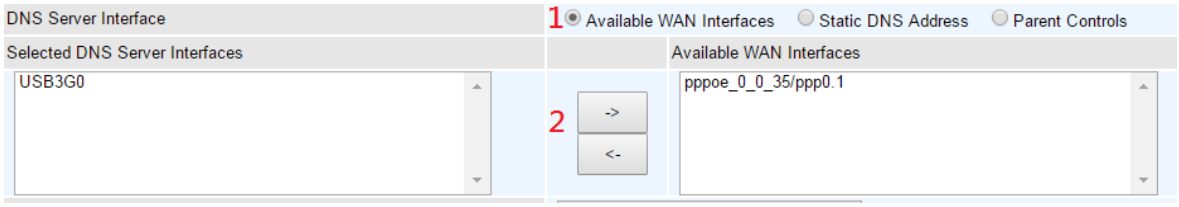
DNS

- **IPv4**

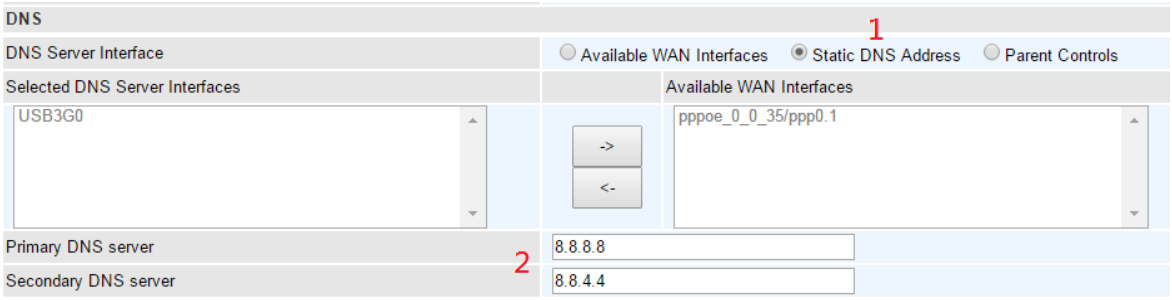
DNS Server Interfaces

1. **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

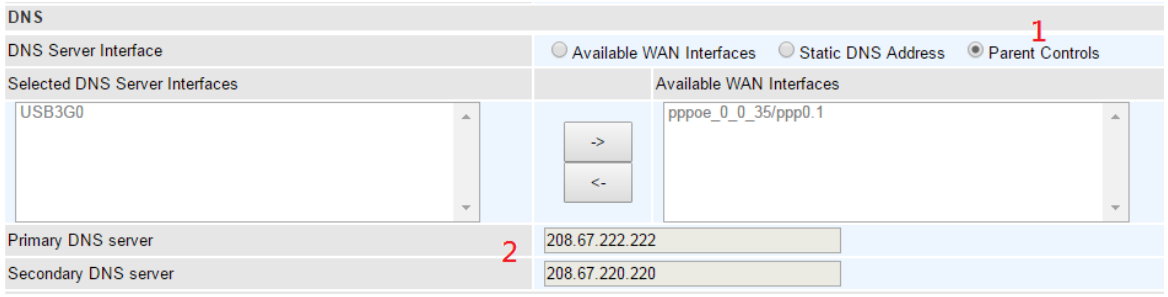
To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



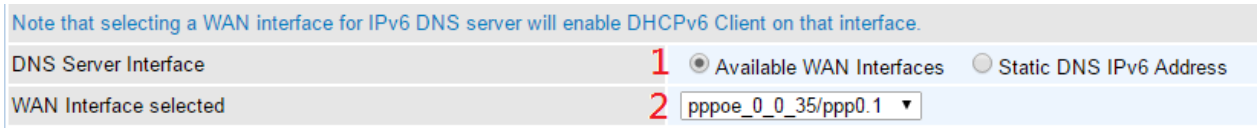
3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).



- **IPv6**

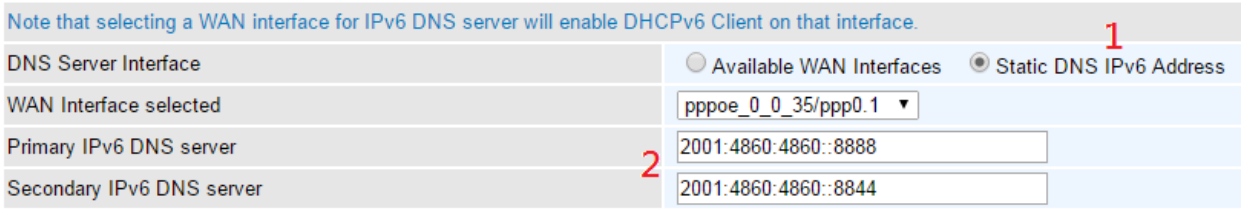
DNS Server Interfaces

1. **Available WAN interfaces:** If your Internet Service Provider assigns DNS server address along with the WAN connection, please select an appropriated Ipv6 WAN interface from **DNS Server Interface.**

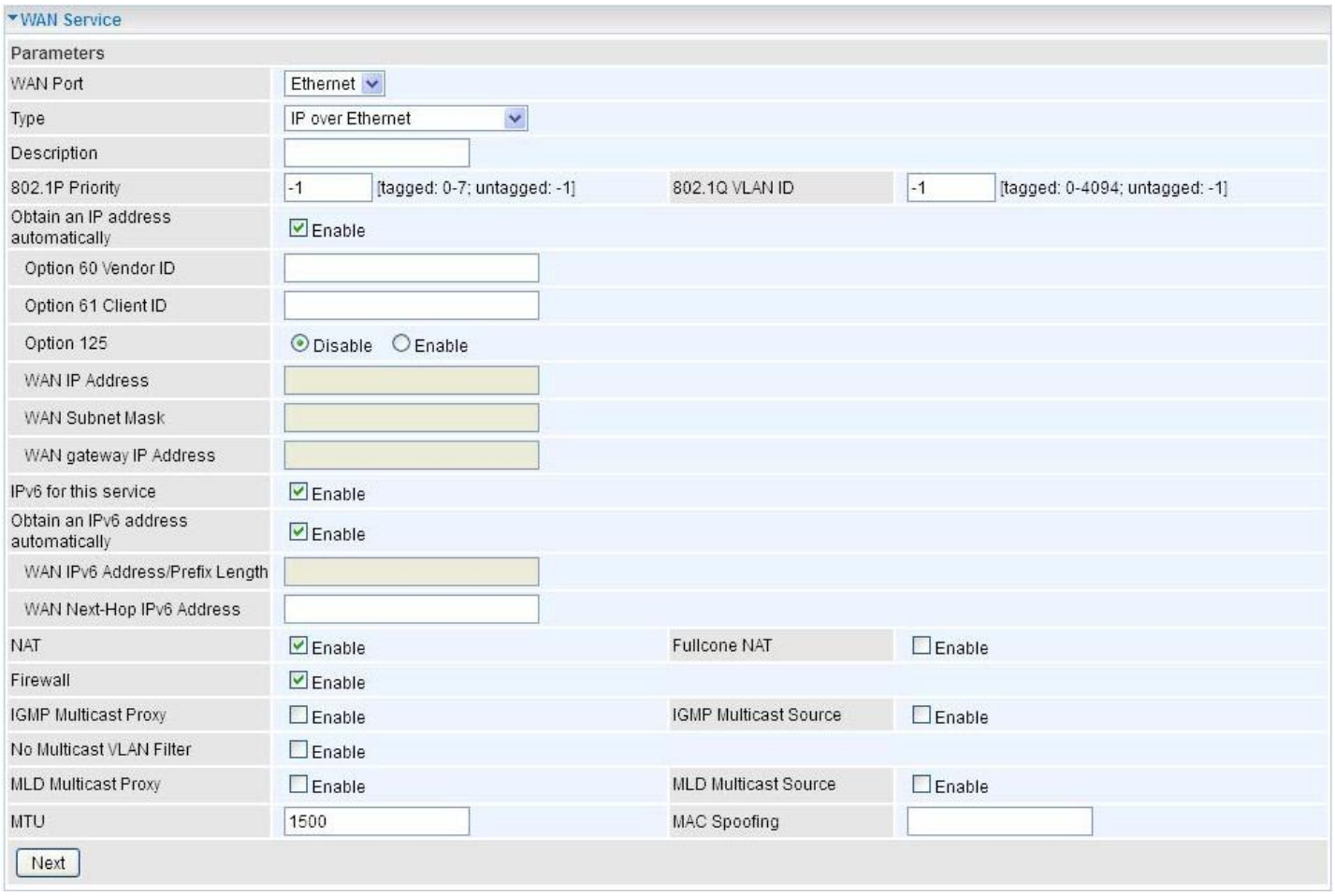


2. **Static DNS IPv6 Address:** If your Internet Service Provide does not provide or you wish to use other DNS servers for your network, simply manually enter other DNS server IP address here:

Primary / Secondary IPv6 DNS Server: Enter the specific primary and secondary IPv6 DNS Server address.



EWAN Internet Protocol - IP over Ethernet



VCP/VPI (For ATM Mode only): Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode (For ATM Mode only): Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged: -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

WAN IP Address

- **IPv4 – Automatic**

  Obtain an IP address automatically: Enable to receive a WAN (public) IP address from your Internet Service Provider. This information should be provided by your ISP, please consult them for more information.

  (Option) Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.

The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

(Option) Option 61 ClientID: Enter the associated information provided by your ISP.

(Option) Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the pre-stored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is set to **Disable**.

NOTE: Leave them blink / disable unless you are instructed by your Internet Service Provider.

- **IPv4 – Manual Input**

  Manual Configure WAN IP Address: Specify your WAN (public) IPv4 address (xxx.xxx.xxx.xxx) to the device provided by your ISP.

  Manual Configure WAN Subnet Mask: Enter submask provided by your ISP.

  Manual Configure WAN Gateway IP: Enter gateway IP address provided by your ISP.

  IPv6 for this service: Enable to use IPv6 service.

- **IPv6 – Automatic**

  Obtain an IPv6 address automatically: Enable to receive an IPv6 WAN address from your Internet Service Provider. This information should be provided by your ISP, please consult them for more information.

- **IPv6 – Manual Input**

  WAN IPv6 Address/Prefix Length: Specify WAN IPv6 Address/Prefix Length. The information shall be provided by your ISP.

  WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast Proxy (for IPv4): Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the interested clients. (Only available in IGMPv3)

No Multicast VLAN Filter: Enable to deactivate multicast filtering. All multicast packets will be forwarded to all ports in the relevant VLANs.

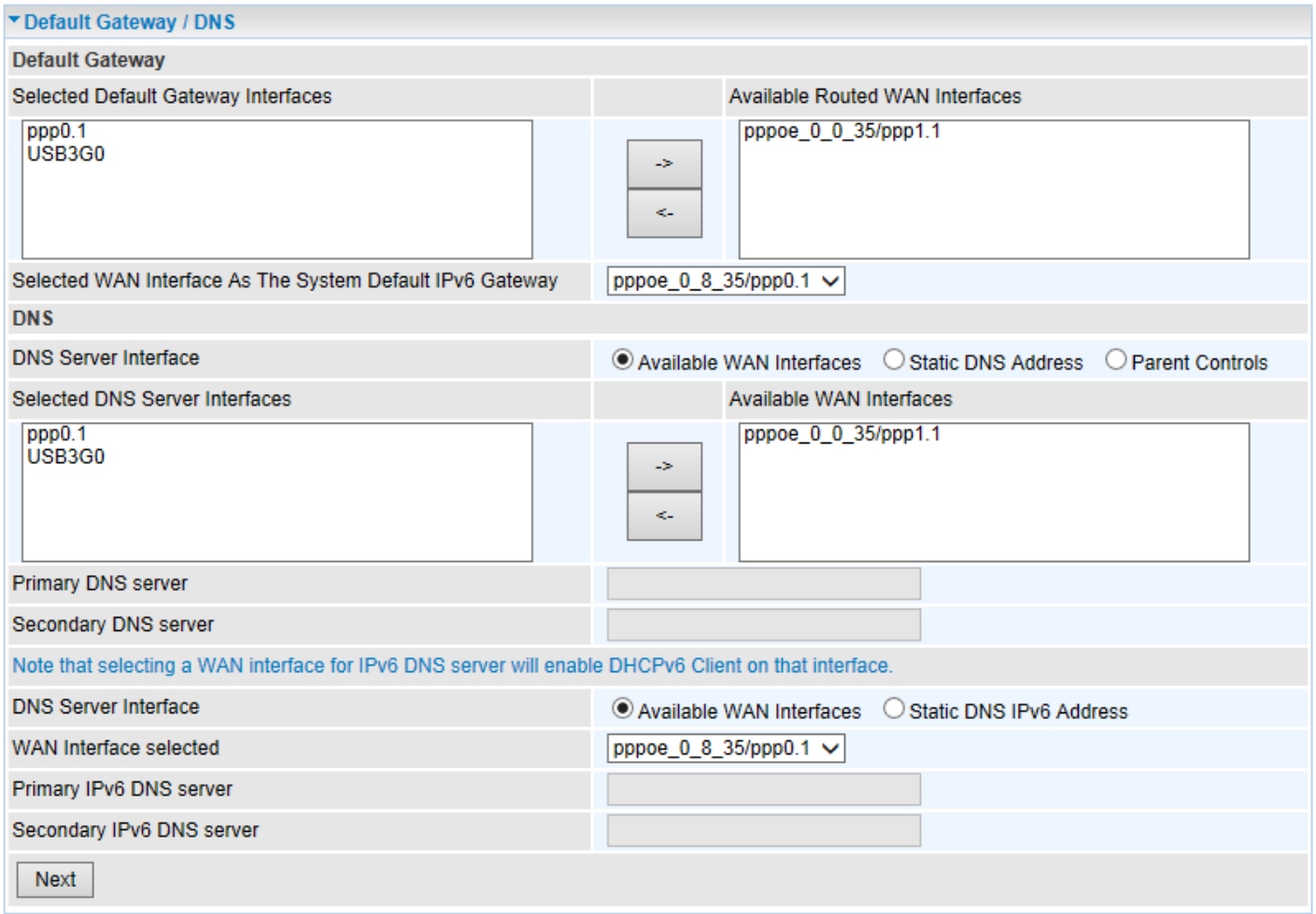
MLD Multicast Proxy (for IPv6): check whether to enable this function. MLD (**Multicast Listener Discovery Protocol**) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. It takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

MAC Spoofing: This option is required by some service providers specifying some specific MAC allowed for joining network. You must fill in the MAC address specified by your service provider when this information is required.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Default Gateway

- **IPv4**

Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

- **IPv6**

When enabling **IPv6** for external interface, please specify the default IPv6 gateway from **Selected WAN Interface as the System Default IPv6 Gateway.**

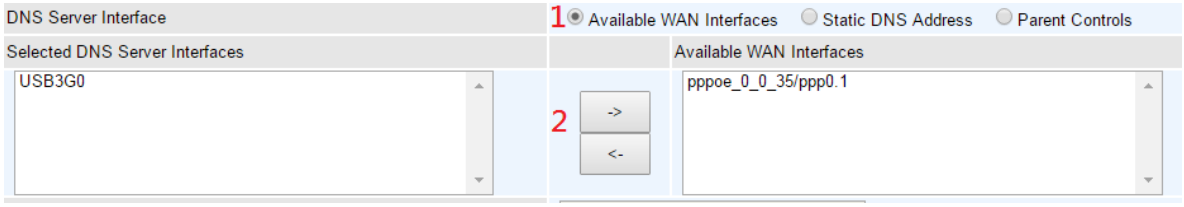
DNS

- **IPv4**

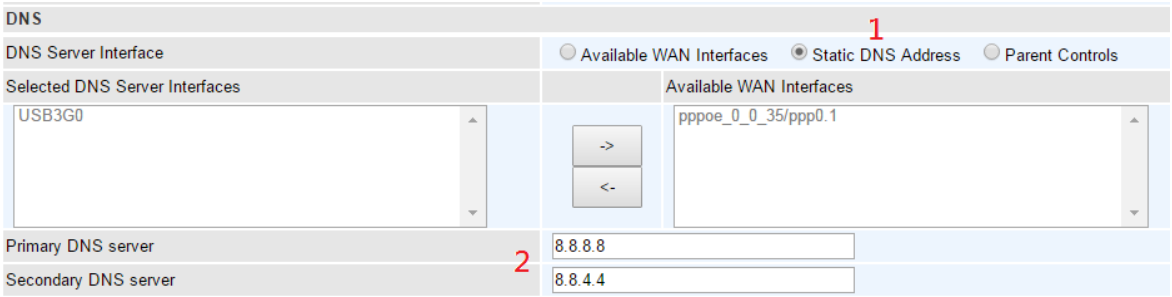
DNS Server Interfaces

1. **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

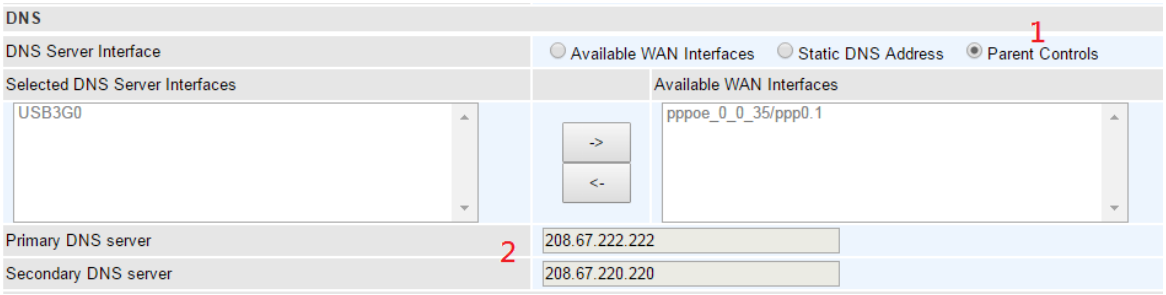
   To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

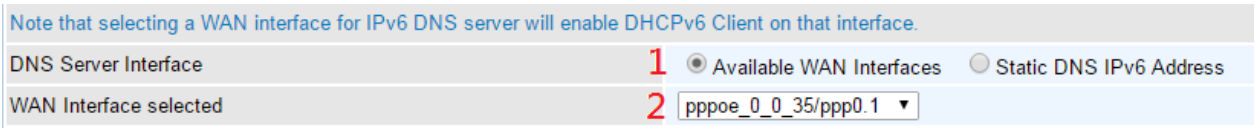


- **IPv6**

DNS Server Interfaces

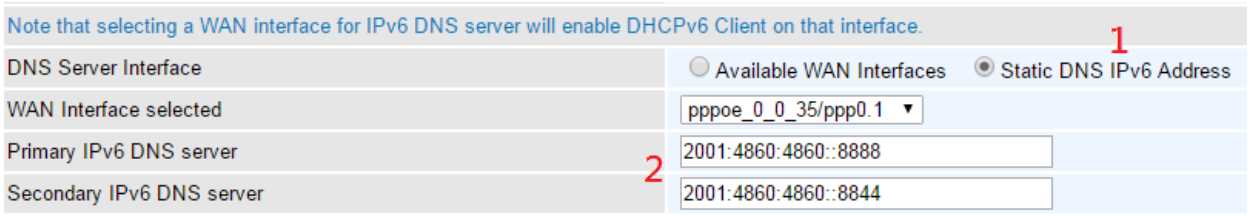
1. **Available WAN interfaces:** If your Internet Service Provider assigns DNS server address along with the WAN connection, please select an appropriated Ipv6 WAN interface from

DNS Server Interface.

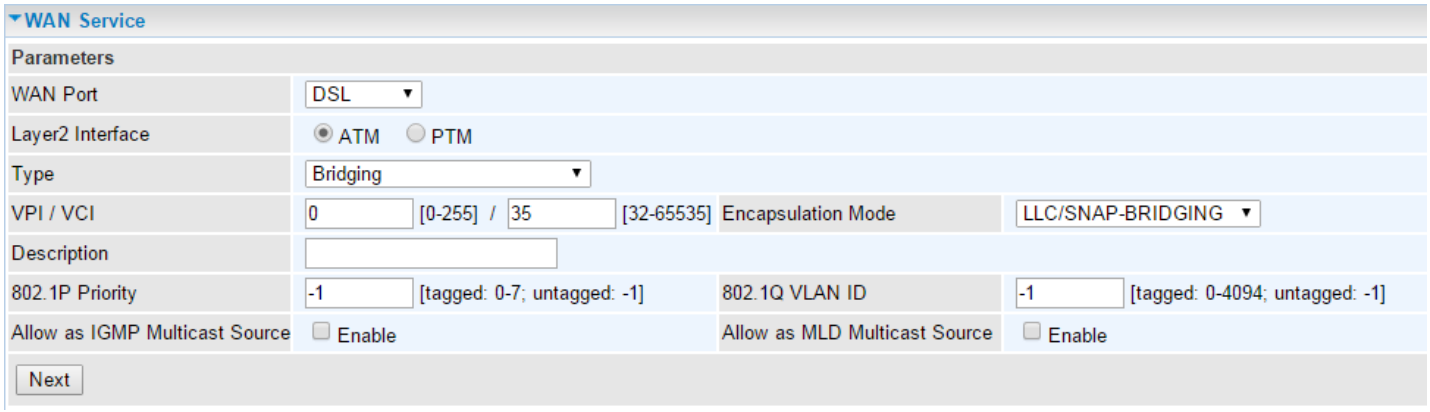


2. **Static DNS IPv6 Address:** If your Internet Service Provide does not provide or you wish to use other DNS servers for your network, simply manually enter other DNS server IP address here:

Primary / Secondary IPv6 DNS Server: Enter the specific primary and secondary IPv6 DNS Server address.



EWAN Internet Protocol - Bridging



VCP/VPI (For ATM Mode only): Enter the VCI/VPI from you Internet Service Provider (ISP). This information should be provided by your ISP, please consult them for more information.

Encapsulation Mode (For ATM Mode only): Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX. This information should be provided by your ISP, please consult them for more information.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

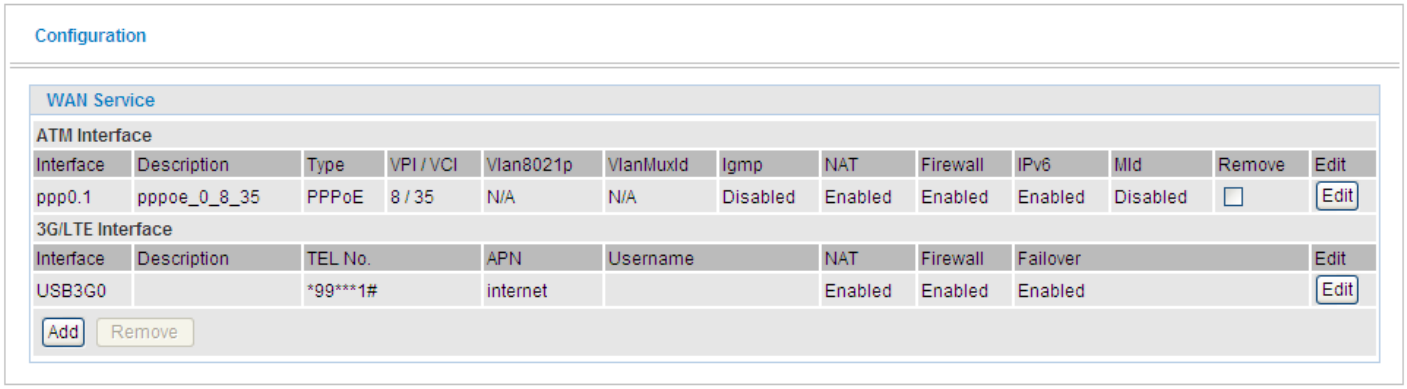
802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged: -1.

Allow as IGMP Multicast Source (for IPv4): Enable to deliver multicast packets from a specific source to the interested clients. (Only available in IGMPv3)

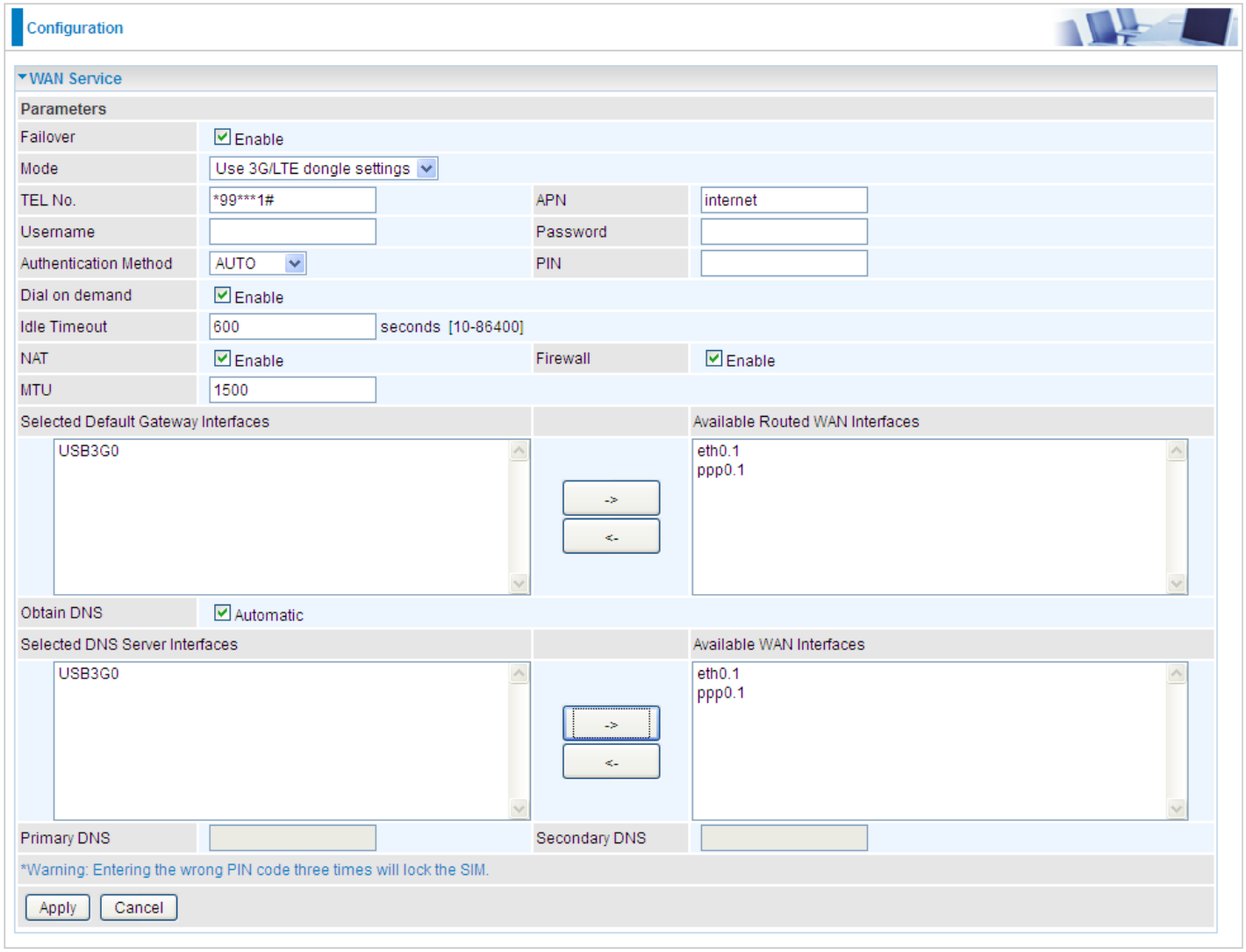
Allow as MLD Multicast Source (for IPv6): Enable to deliver multicast packets from a specific source to the interested clients. . (Only available in IGMPv3)

❖ 3G/4G LTE via USB Connection Setup

Select 3G/4G LTE to configure the route to enjoy the mobility. By default the 3G/4G LTE interface is on, user can edit the parameters to meet your own requirements.



Click **Edit** button to enter the 3G/4G LTE configuration page.



Failover: If enabled, the 3G/4G LTE will work in failover mode and be brought up only when there is no active default route. In this mode, 3G/4G LTE work as a backup for the WAN connectivity. While if disabled, 3G/4G LTE serves as a normal interface, and can only be brought up when it has been configured to achieve a mobile connectivity.

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G

preferred, UMTS 3G preferred, Automatic, and Use 3G/4G LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

TEL No.: The dial string to make a 3G/4G LTE user internetworking call. It may provide by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

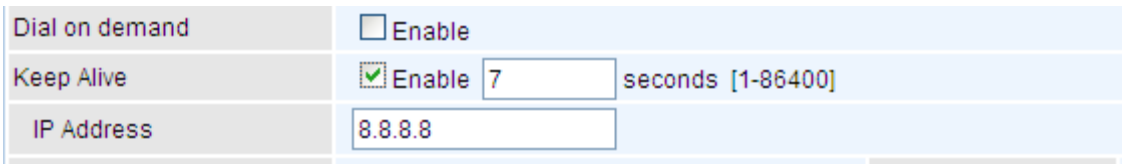
Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is set to Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/ service provider.

- **Connect on Demand:** If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.
- **Keep Alive:** Check Enable to allow the router to send message out every 7 seconds (can be changed base on need) to prevent the connection being dropped by ISP.

  IP Address: The IP address is used to "ping", and router will ping the IP to find whether the connection is still on.



MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.

NAT: Check to enable the NAT function.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

Default Gateway

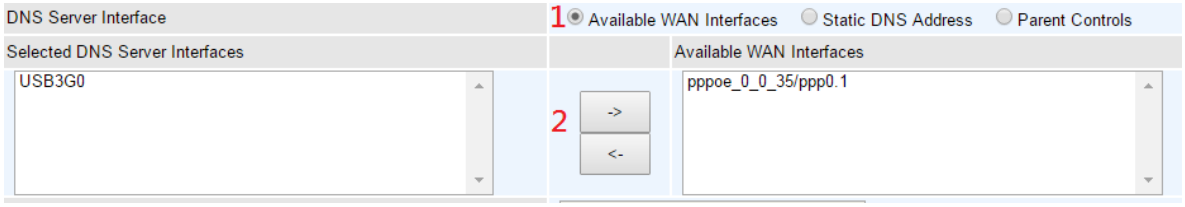
Click the appropriate default gateway interface for this WAN service from **Available Routed WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box.

To remove interface(s) from **Selected Default Gateway Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

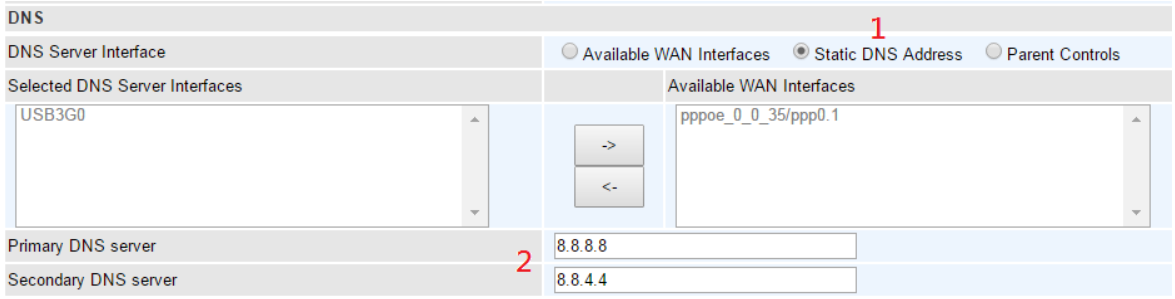
DNS

1. **Available WAN interfaces:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box

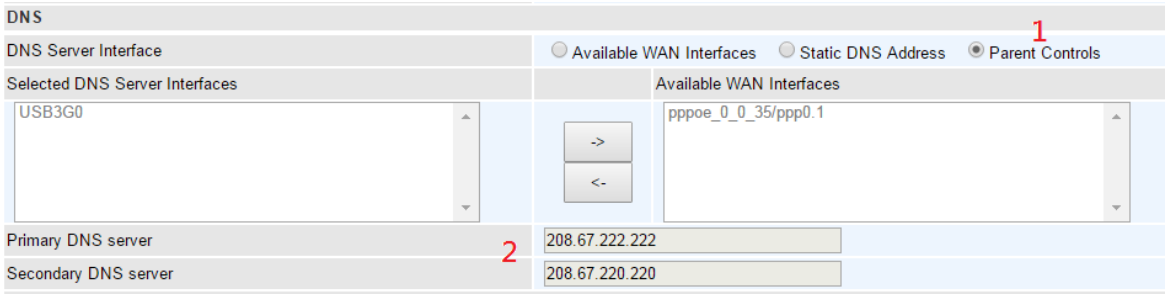
   To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

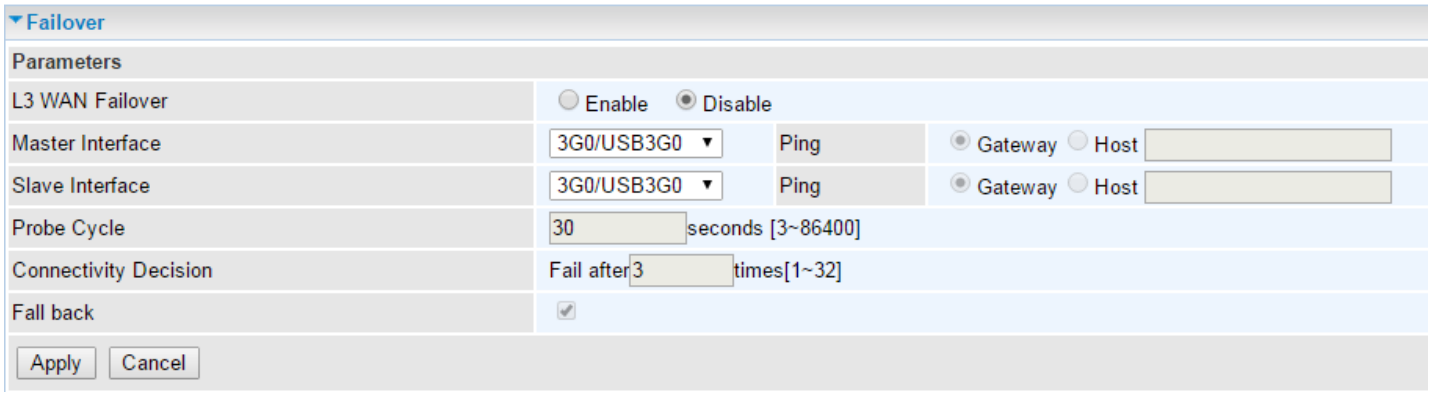


Click **Apply** to save the settings.

Failover

WAN Failover works in conjunction with two (2) WAN Interfaces and provides always-on Internet connectivity.

When BEC 8920AC detects WAN failure on Primary WAN link, seamlessly, all traffic will get routed to the Secondary WAN interface as backup WAN port.



L3 WAN Failover: Enable to activate the feature

Mater Interface (Primary WAN): Choose a primary WAN from the drop-down box which contains available WAN interfaces configured in the **WAN Service**

Slave Interface (Secondary WAN): Choose a secondary WAN link as a backup WAN.

Ping: Here are two test methods to check Internet connectivity.

- **Gateway:** System sends ping packet to gateway and wait for response from the gateway in every “Probe Cycle” in seconds.
- **Host:** Specify a host IP address in the given space. The system pings the specified host and wait for its response in every “Probe Cycle” in seconds.

Probe Cycle: Specify failover interval in seconds.

Connectivity Decision: Specify Ping failure threshold in every Probe Cycle to switch to backup WAN link.

Fallback: Enable to automatically reconnect to the primary WAN link when connectivity is restored.

Automatically WAN Failover Rule:

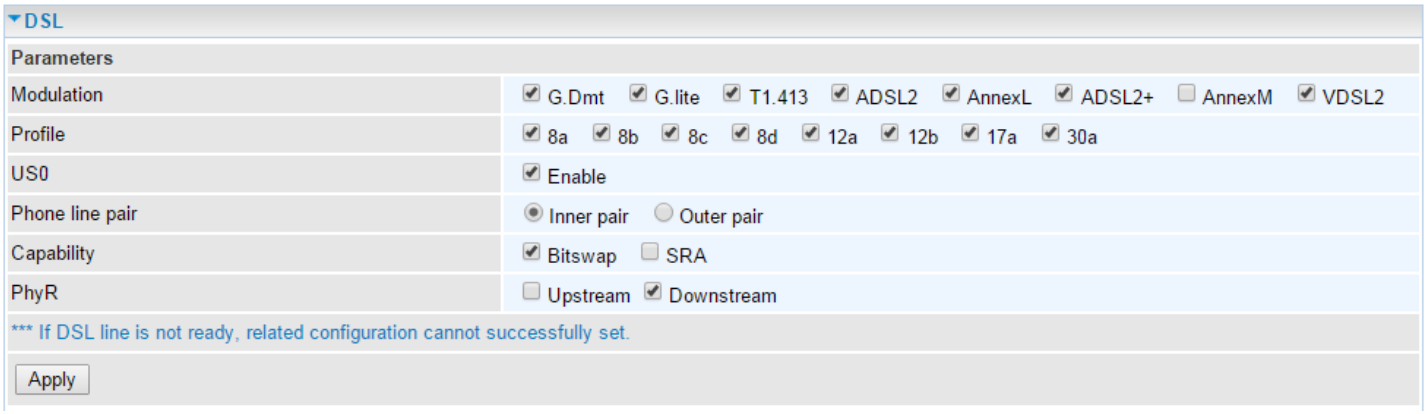
Rule 1: ADSL or VDSL connection fail

Rule 2: Ping Fail when exceed the number of consecutive failures in specific failover interval.

Example: If Ping to either the gateway or host IP with no responses in 30 seconds (Probe Cycle) for 3 consecutive times (Connectivity Decision), 8920AC will assume primary link is down then switch to secondary WAN link as backup interface.

DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.



Modulation: There are 8 modes available, “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, ”ADSL2+”,“AnnexM”, and “VDSL” to choose from. Please consult with your Internet Service Provider if you don’t what mode to choose.

Profile: VDSL profiles up to 30a.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

US0: Enable to improve rate performance and extend the reach distance of VDSL2.

Capability: There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- **Bitswap:** Enable to activate bitswaping function.
- **SRA:** Enable to activate seamless rate adaptation.

PhyR: A new technology to control impulse and noise to improve the BER and DSL data quality.

Click **Apply** to save settings.

DSL Bonding

This feature allows you to double your ADSL or VDSL data rate. Contact your ISP to see if you can upgrade your Internet service in order to use this feature

xDSL Bonding Capability: To enable or disable the xDSL bonding feature.

- **Enable**: The device will attempt to make connection in two-pair xDSL bonding mode.
- **Disable**: The device will only make a connection in single-pair xDSL mode.

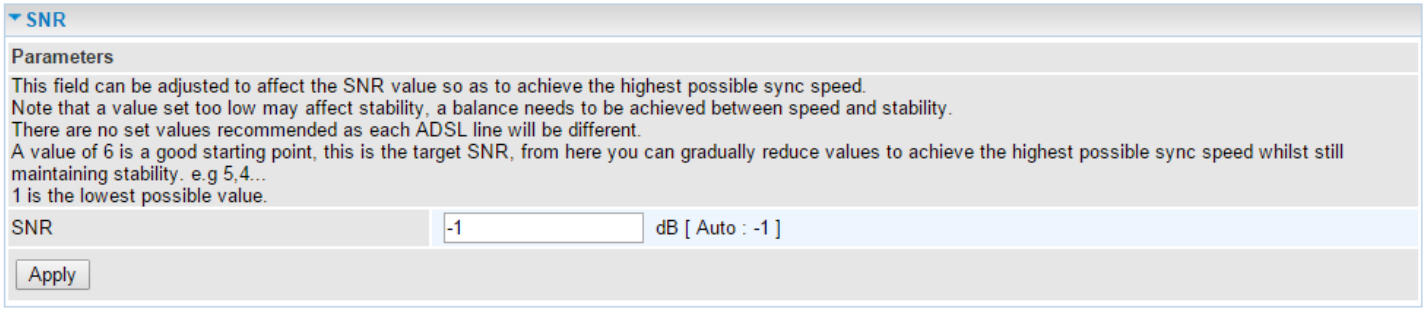
Current WAN xDSL Mode: This displays your current xDSL connection mode on the DSLAM/ISP.

- **Bonded**: two-pair xDSL bonding is available.
- **Non-Bonded:** single-pair xDSL is available.

Click **Apply/Reboot** to save settings then reboot the system to activate the changes.

SNR

Signal-to-noise ratio (often abbreviated **SNR** or **S/N**) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.



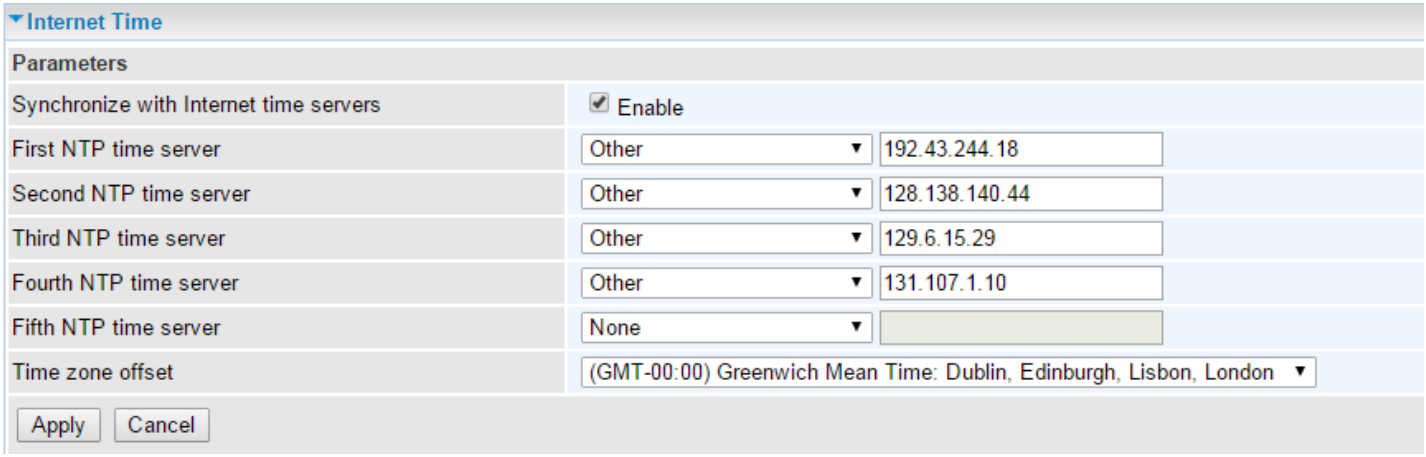
SNR: Change the value to adjust the DSL link rate, more suitable for an advanced user.

System

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.



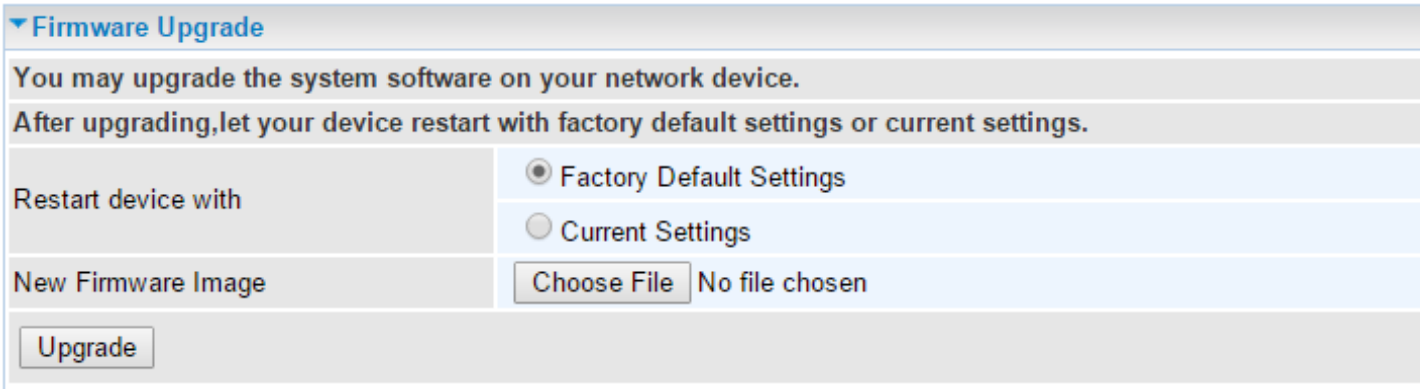
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click **Apply** to save your settings.

Firmware Upgrade

Software upgrading lets you experience new and integral functions of your router.



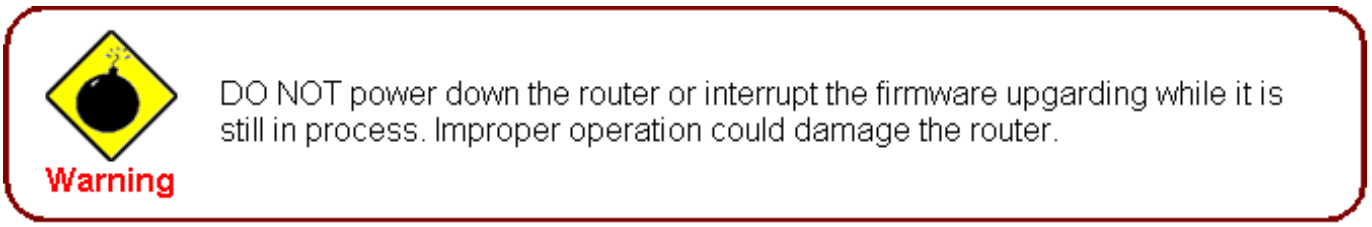
Restart device with:

- **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.
- **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.

Your router's "firmware" is the software that allows it to operate and provides all its functionality.

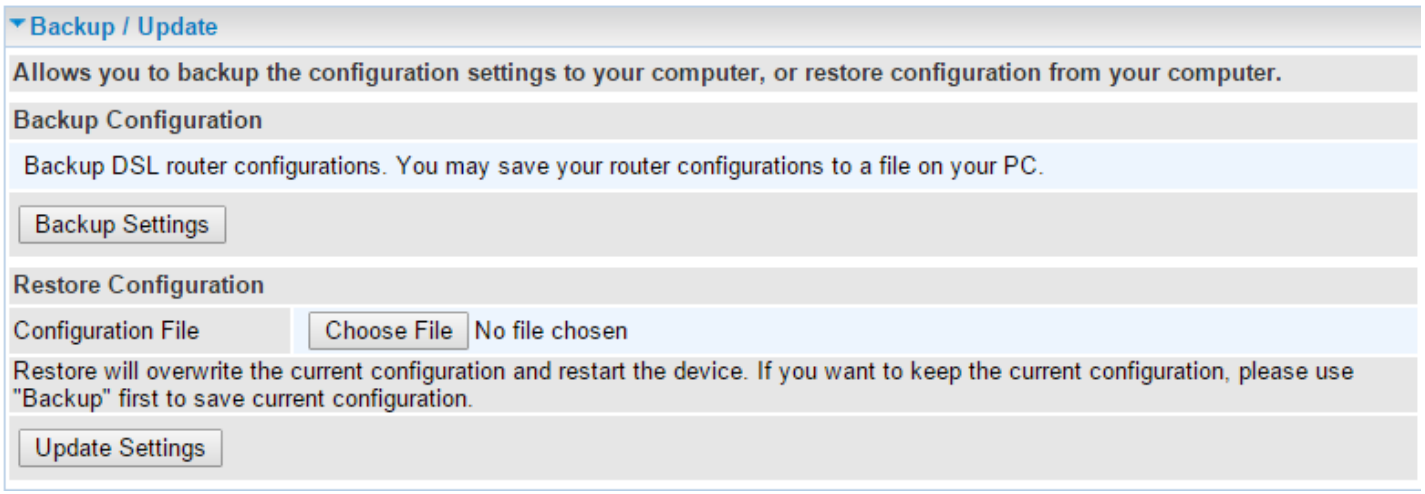
Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click **Upgrade** to update the firmware in your router.



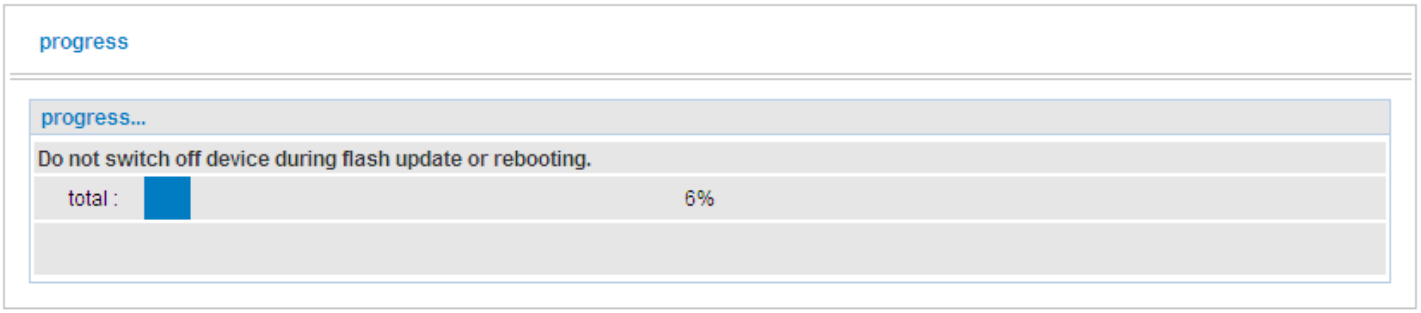
Backup / Update

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore from a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.



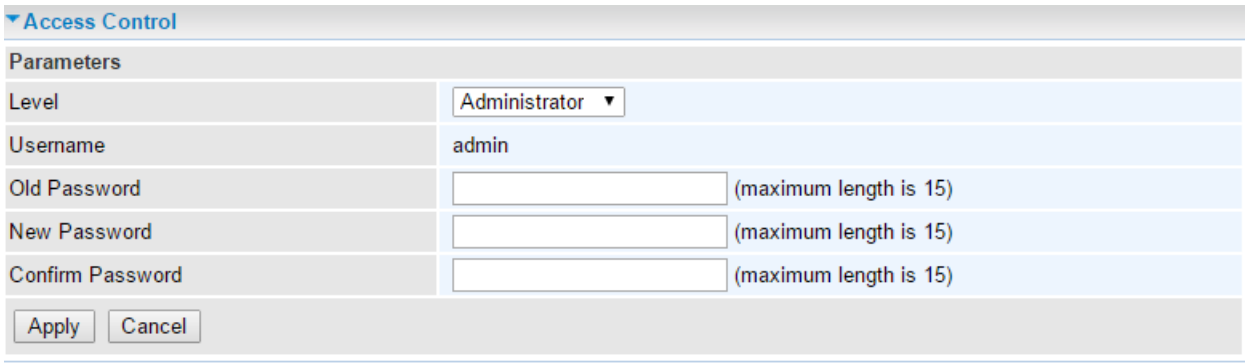
Click **Backup Settings**, a window appears, click save, then browse the location where you want to save the backup file.

Click **Browse** and browse to the location where your backup file is saved, the click **Open.** Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.



Access Control

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.



Level: select which level you want to change password to. There are three default levels.

- **Administrator:** Root account with ability to control and manage all features.

  Username: admin

  Password: admin
- **Advanced:** Normal user account. With limited ability to control and manage the device

  Username: advanced

  Password: advanced
- **User:** Guest account to view Status and manage Wireless section only.

  Username: user

  Password: user

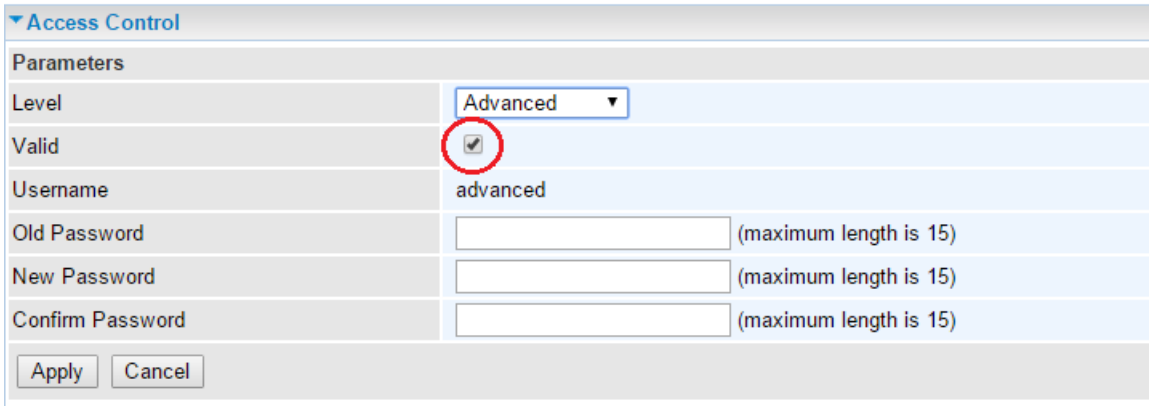
Username: the default username for each user access level.

Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Re-enter the new password to confirm.

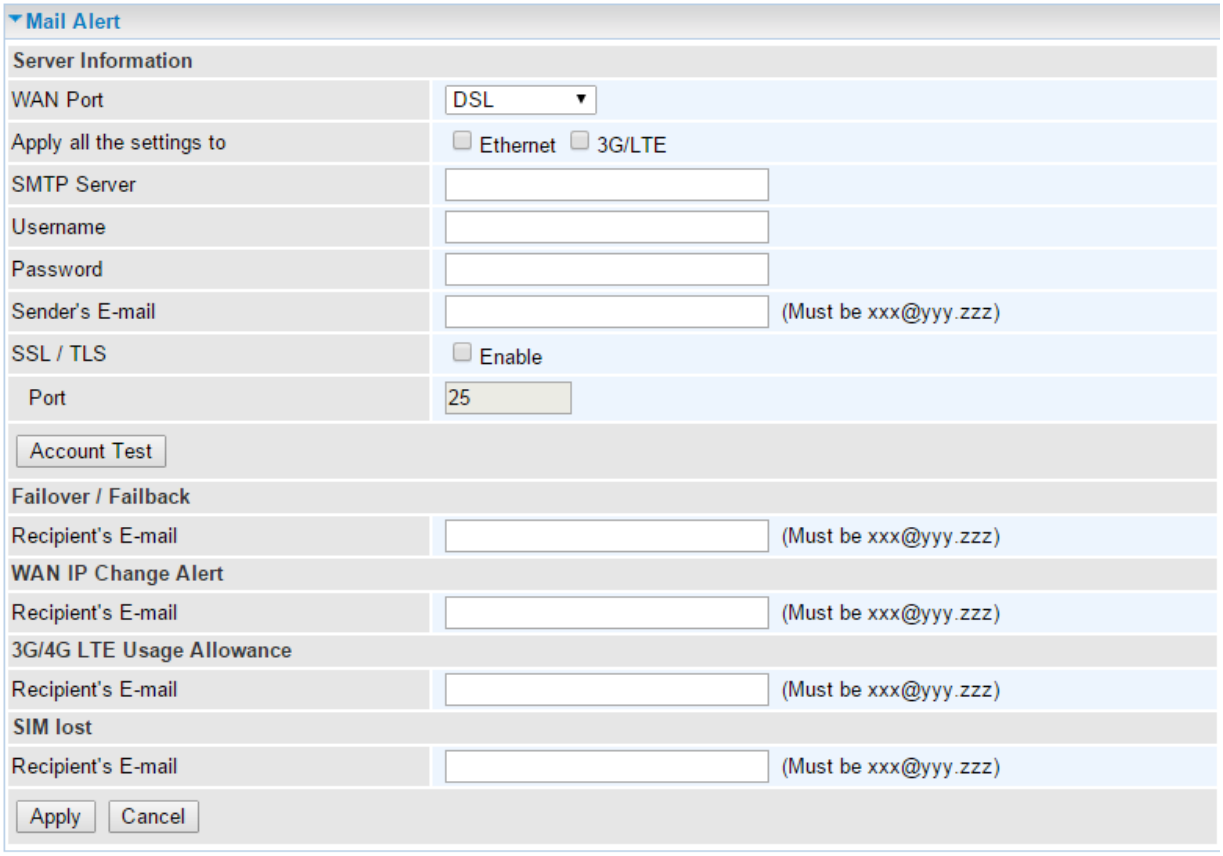
Note: By default, the **Advanced** and **User** accounts are inactivated. Use Admin account to activate each account by clicking the **Valid** check-box.



Click **Apply** to apply your new settings.

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



WAN Port: Mail Alert feature can be applicable to every WAN mode: xDSL, EWAN, and 3G/4G LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

Apply all settings to: check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL / TLS: Check to whether to enable SSL / TLS encryption feature.

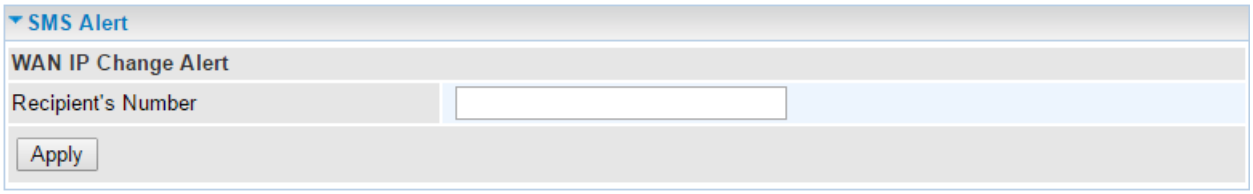
Port: the port, default is 25.

Account Test: Press to test the connectivity and feasibility to your sender's e-mail.

Recipient's Email (WAN IP Change Alert): Enter a valid e-mail address to receive a message when WAN Failover / Failback occurs, WAN IP changed, SIM card removed, and 3G/4G LTE usage allowance update

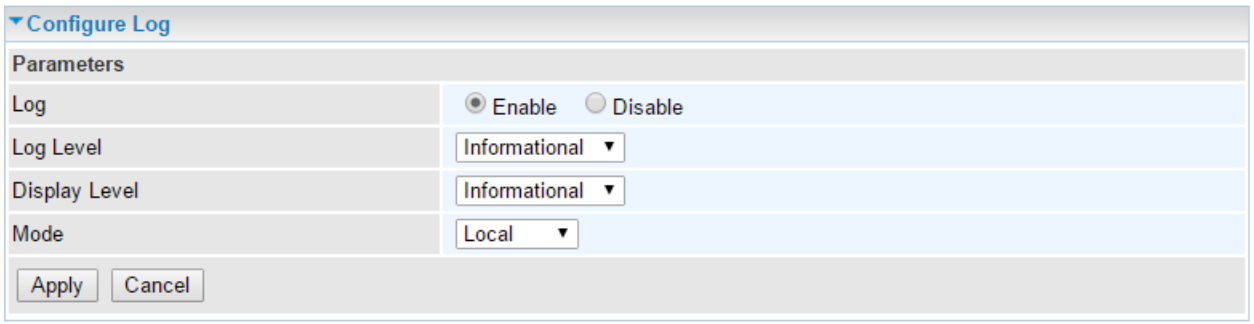
SMS Alert

SMS, Short Message Service, is to inform clients the information clients subscribe. The BEC 8920AC offers SMS alert sending clients alert messages when a WAN IP change is detected.



Recipient's Number (WAN IP Change Alert): Enter the Recipient's number that will receive the alert message once a WAN IP change has been detected.

Configure Log



Log: Enable or disable this function.

Log level: Select your log level. The log level allows you to configure which types of events are logged. There are eight log levels from high to low are displayed below:

- **Emergency** = system is unusable
- **Alert** = action must be taken immediately
- **Critical** = critical conditions
- **Error** = error conditions
- **Warning** = warning conditions
- **Notice** = normal but significant conditions
- **Informational** = information events
- **Debugging** = debug-level messages

The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

Display Level: Display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: Select the mode the system log adopted. Three modes: local, Remote and Both.

- **Local**: Select this mode to store the logs in the router's local memory.
- **Remote**: Select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- **Both**: Logs stored adopting above two ways.

Click **Apply** to save your settings.

IP Tunnel

IP Tunnel is an Internet Protocol (IP) network communication channels between two networks of different protocols. It is used to transport another network protocol by encapsulation of its packets.

IP Tunnels are often used to connect two disjoint IP networks that do not have a native routing path to each other, via an underlying routable protocol across an intermediate transport network, like VPN.

Another prominent use of IP Tunnel is to connect islands of IPv6 installations across the IPv4 Internet.

IPv6-in-IPv4 (6RD)

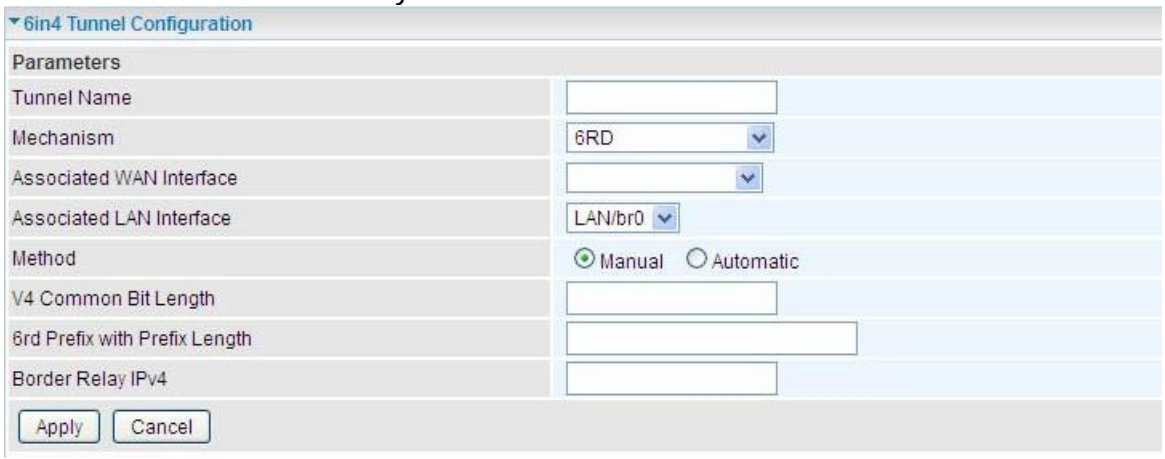
6in4 is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 links. The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP Protocol number set to 41. This protocol number is specifically designated for IPv6 capsulation.

6RD

6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of Internet Service Providers (ISPs).

It is derived from 6to4, a preexisting mechanism to transporting IPv6 packets over IPv4 infrastructure network, with the significant change that it operates entirely within the end user's ISP network, thus avoiding the major architectural problems inherent in the original design of 6to4.

Click **Add** button to manually add the 6in4 rules.



Tunnel Name: User-defined name.

Mechanism: Here only 6RD.

Associated WAN Interface: The applied WAN interface with the set tunnel, thus when there are 148 packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Set the linked LAN interface with the tunnel.

Method: There are two 6rd operation mechanisms

- **Automatically:** 6rd parameters will be configured by the system.
- **Manually:** Fill out the following 6rd parameters:

  V4 Common Bit Length: Specify the length of IPv4 address carried in IPv6 prefix.

  For example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

  6rd Prefix with Prefix Length: Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP (The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

  Border Relay IPv4 Address: The IPv4 address of the border relay. The relay is to un-wrap capsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

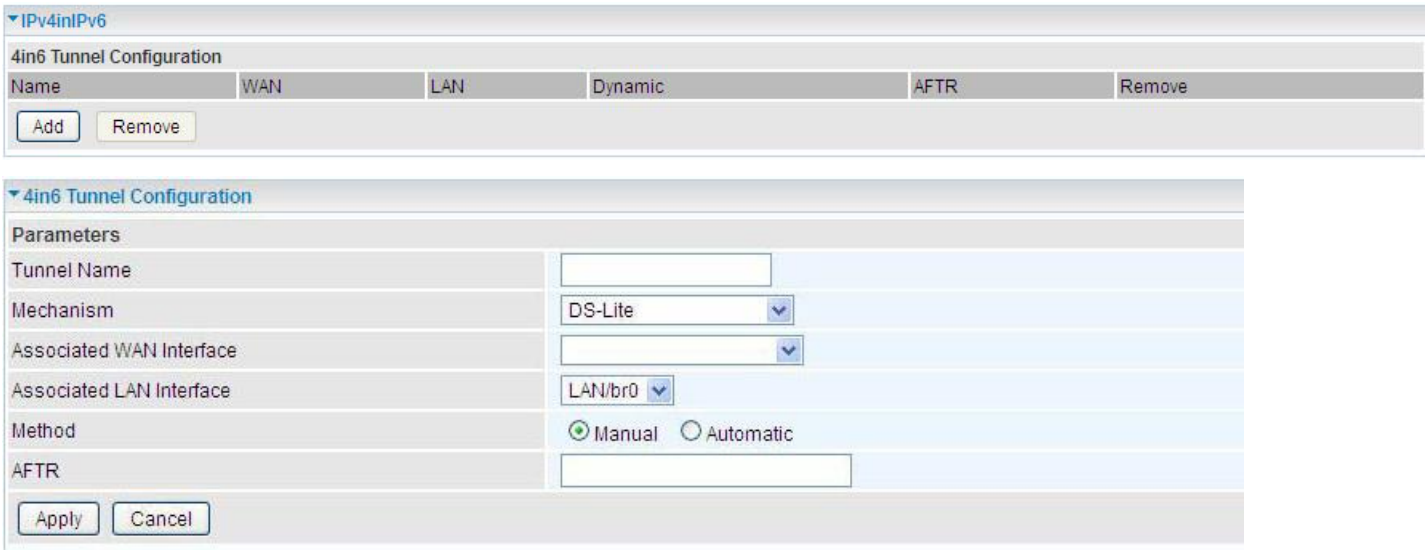
IPv4-in-IPv6 (DS-Lite)

DS-Lite

DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.

Click **Add** button to manually add the 4in6 rules.



Tunnel Name: User-defined tunnel name.

Mechanism: It is the 4in6 tunnel operation technology. Please select DS-Lite.

Associated WAN Interface: The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Specify the linked LAN interface with the tunnel.

Method: Manually to specify the AFTP (Address Family Transition Router) address or Automatic.

AFTR: Specify the address of AFTP (Address Family Transition Router) from your ISP.

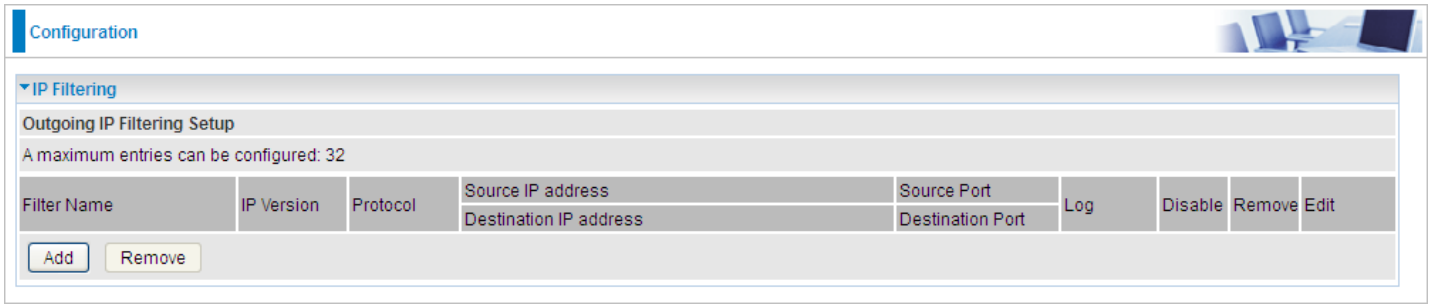
Security

IP Filtering Outgoing

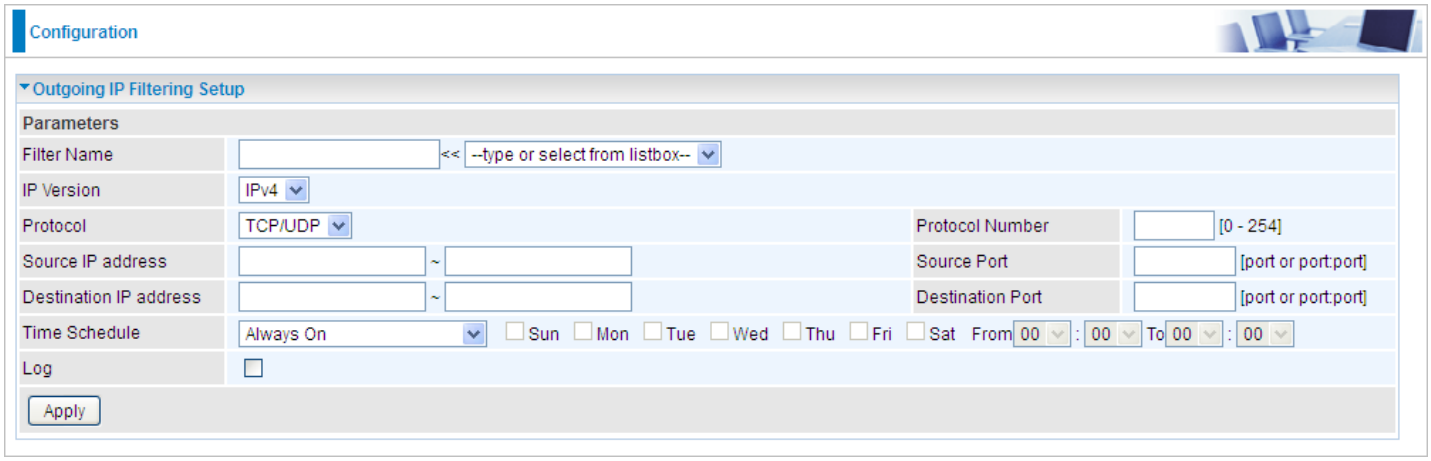
IP filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Outbound IP Filtering by default is set to **forward** all outgoing traffic from LAN to go through the router, but user can set rules to **block** the specific outgoing traffic.

Note: The maximum number of entries: 32.



Click **Add** button to enter the exact rule setting page.



Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

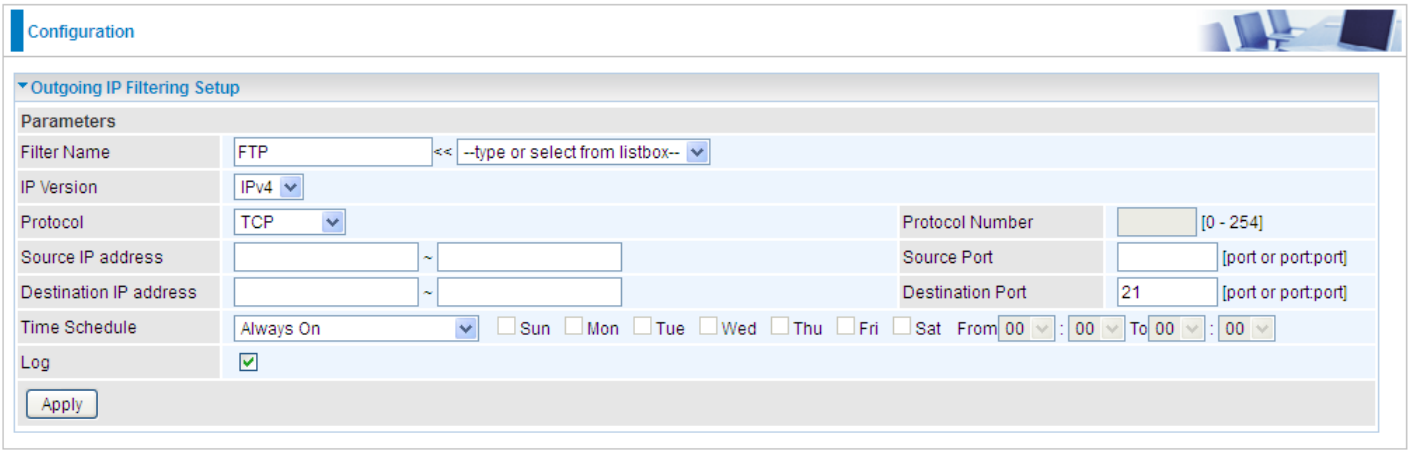
Destination Port [port or port: port]: Traffic with the particular set destination port or port in the set

port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535.

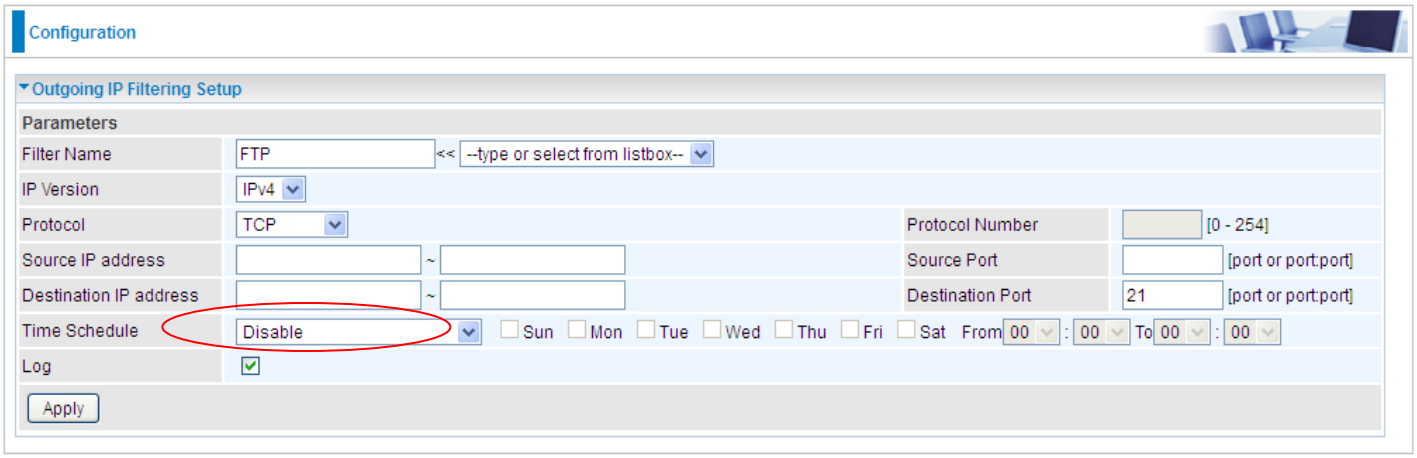
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 of Sun to 19:00 of Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon” ” in list table indicating the rule is inactive. See Time Schedule.

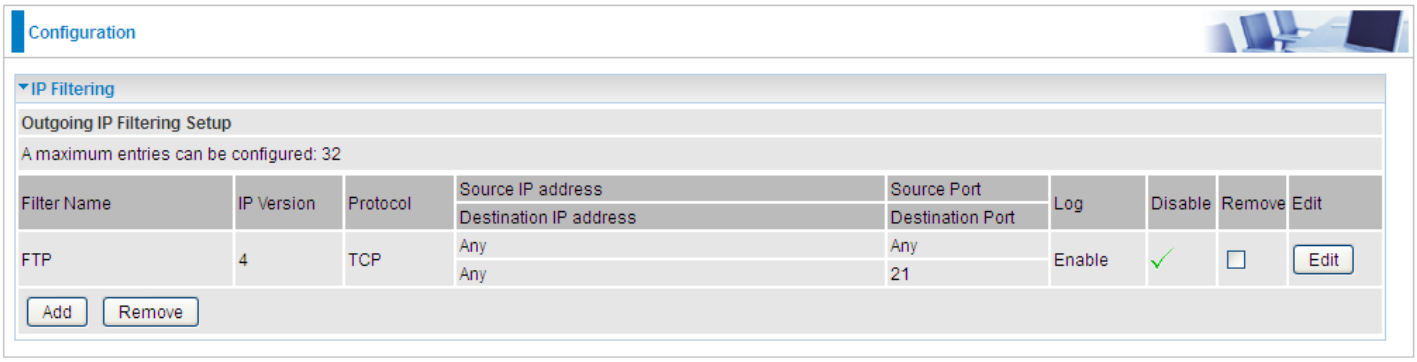
Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

Example: For example, if there is an outgoing rule set as follows, then the 21 application between source IP and destination IP will be blocked. Or exactly in the rule below, all traffic trying to access FTP will be blocked.



(The rule is active; disable field shows the status of the rule, active or inactive)





(Rule inactive)

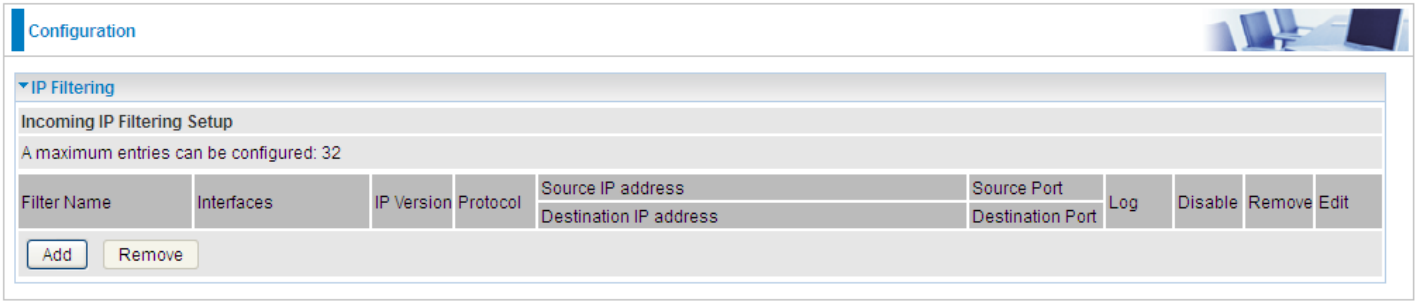
IP Filtering Incoming

Incoming IP Filtering is set by default to **block** all incoming traffic, but user can set rules to **forward** the specific incoming traffic.

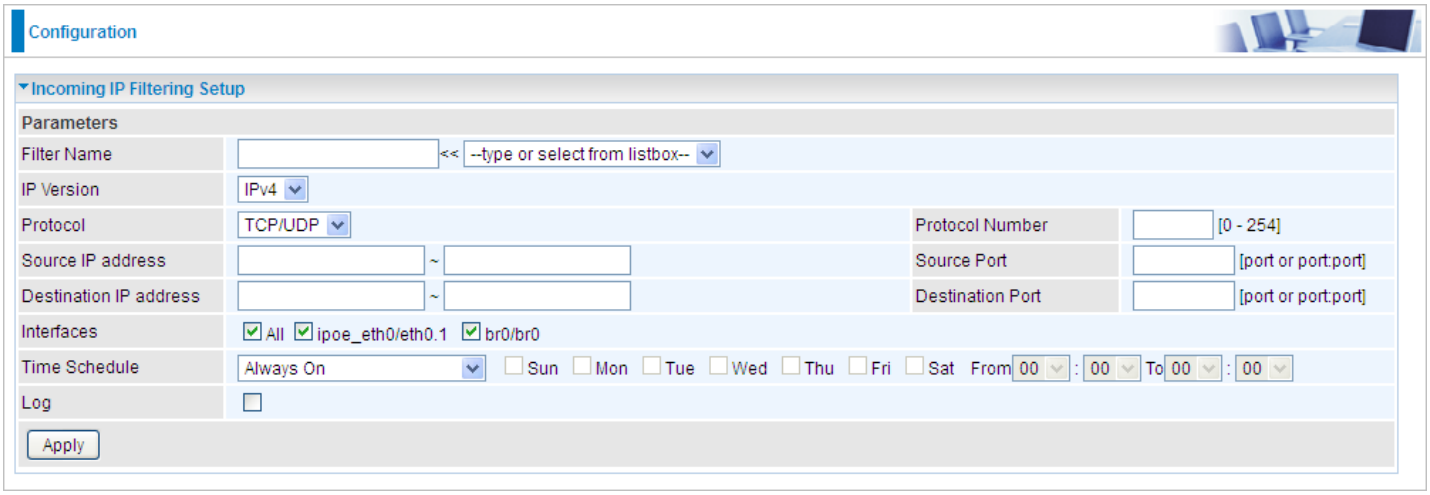
Note:

1. The maximum number of entries: 32.

2. When LAN side firewall or firewall in WAN interface(s) is enabled, user can move here to add allowing rules to pass through the firewall.



Click **Add** button to enter the exact rule setting page.



Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, and ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range.. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port : port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535

Interfaces: Check if the filter rule applies to all interfaces. User can base on need select interfaces to

make the rule take effect with those interfaces.

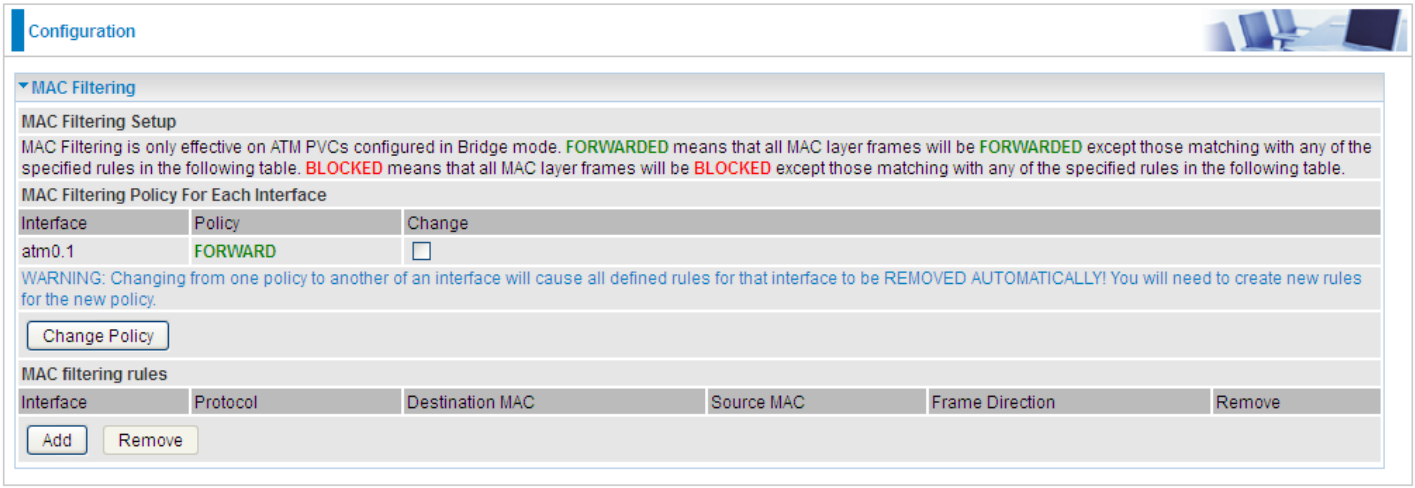
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 of Sun to 19:00 of Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”  ” in the list table indicating the rule is inactive. See Time Schedule.

Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

MAC Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

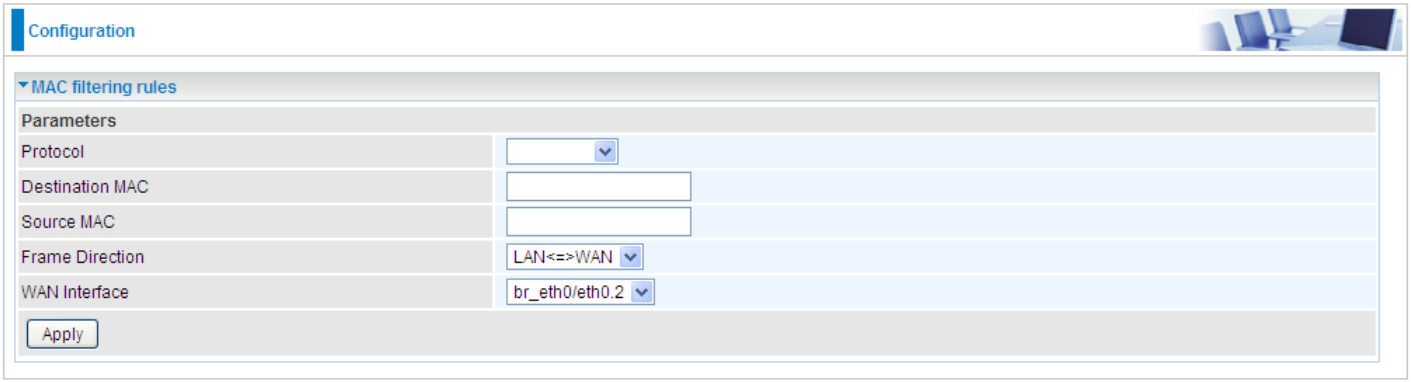
- **FORWARDED:** All MAC layer frames will be **forwarded** except those matching with any of the specified rules in the following table.
- **BLOCKED:** All MAC layer frames will be **blocked** except those matching with any of the specified rules in the following table.



By default, all MAC frames of the interface in Bridge Mode will be **forwarded**; you can check **Change** checkbox and then press **Change Policy** to change the settings to the interface.

For example, from above, the interface atm0.1 is of bridge mode and all the MAC layer frames will be **forward**, but you can set some rules to let some item matched the rules to be **blocked**.

Click **Add** button to add the rules.



Protocol type: Select from the drop-down menu the protocol that applies to this rule.

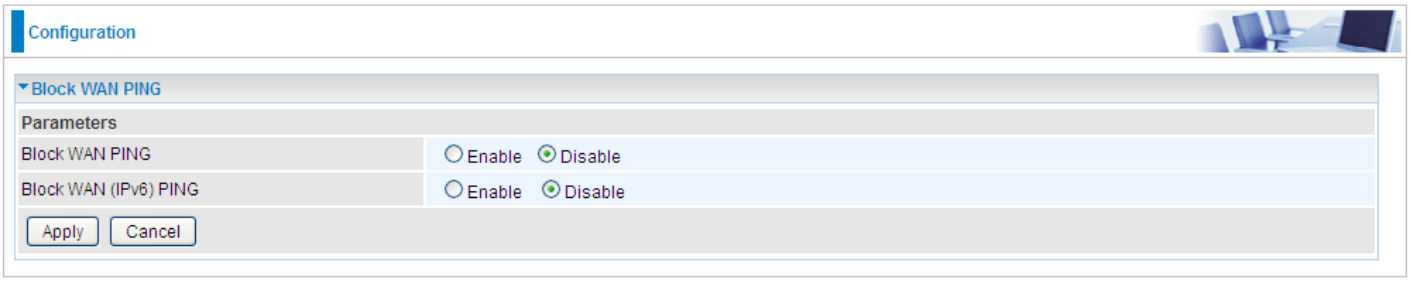
Destination /Source MAC Address: Enter the destination/source address.

Frame Direction: Select the frame direction this rule applies, both LAN and WAN: LAN <=>WAN, only LAN to WAN: LAN=>WAN, only WAN to LAN: WAN=>LAN.

WAN Interfaces: Select the interfaces configured in Bridge mode.

Blocking WAN PING

This feature is enabled to let your router not respond to any ping command when someone others “Ping” your WAN IP.

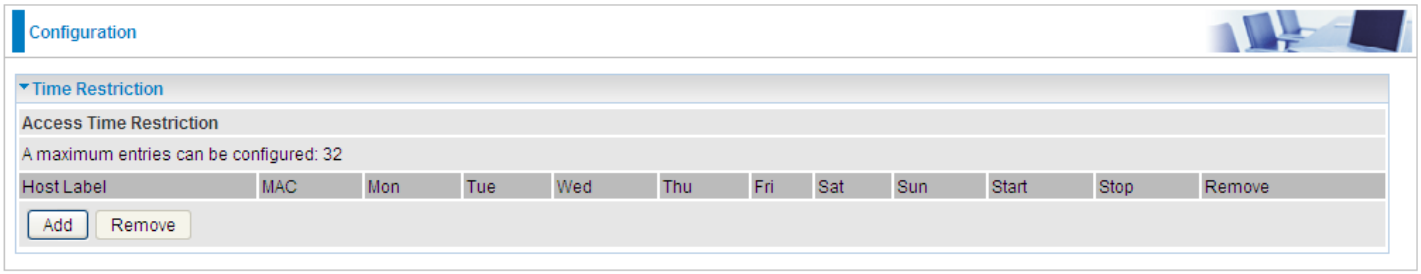


Time Restriction

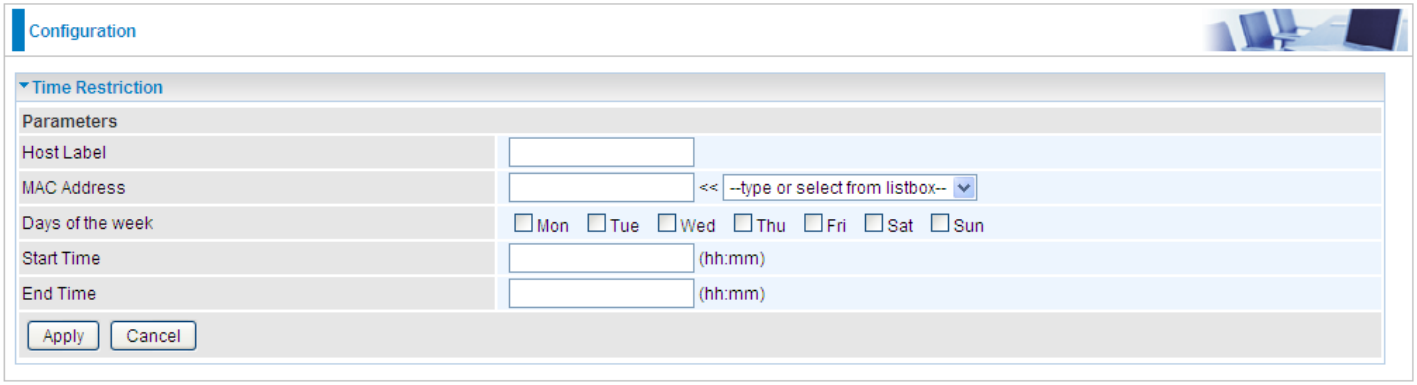
A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN during the specified time.

This page adds time of day restriction to a special LAN device connected to the router. To **Restrict** LAN device(s), please click Add button to add the device(s) from accessing internet under some set time. To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.



Click **Add** to add the rules.



Host Label: User-defined name.

MAC Address: Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. For convenience, user can select from the list box.

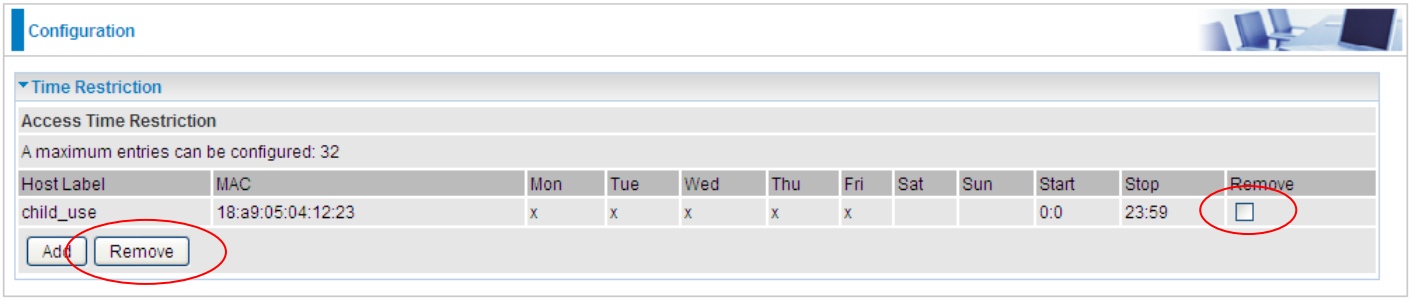
Days of the week: Select the days of a week the rule takes efforts.

Start Time: Enter the start time of each day in hh:mm format. Leaving it empty means 00:00.

End Time: Enter the end time of each day in hh:mm format. Leaving it empty means 23:59.

Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.

Example:



Here you can see that the user “child_use” with a MAC of 18:a9:05:04:12:23 is blocked to access the router from 00:00 to 23:59 Monday through Friday.

If you needn’t this rule, you can check the box, press Remove, it will be OK.

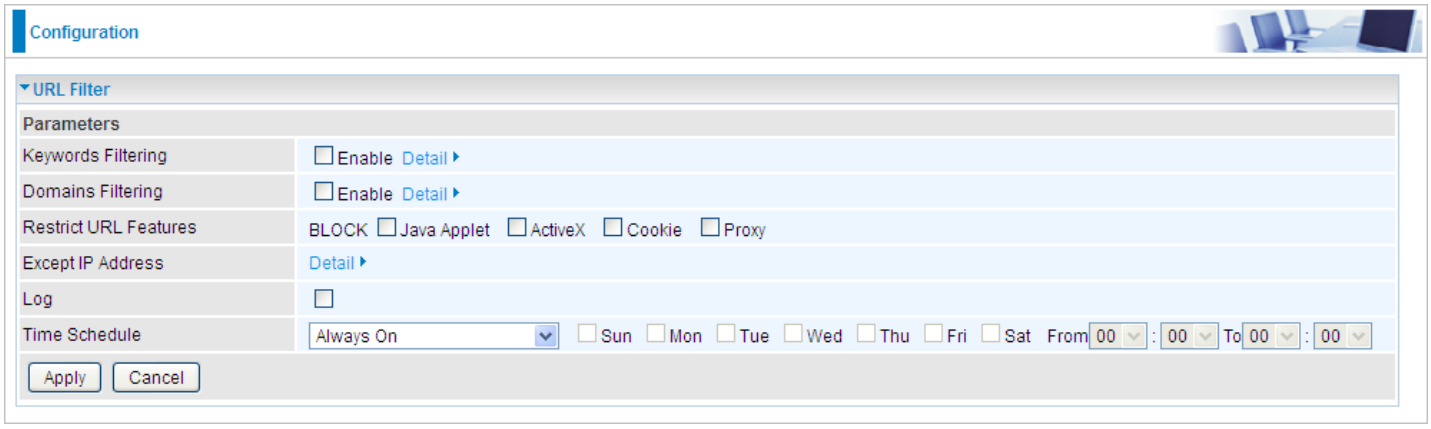
URL Filtering

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

Note:

1) URL Filter rules apply to both IPv4 and IPv6 sources.

2) But in **Exception IP Address** part, user can click Detail ▸ to set the exception IP address(es) for IPv4 and IPv6 respectively.

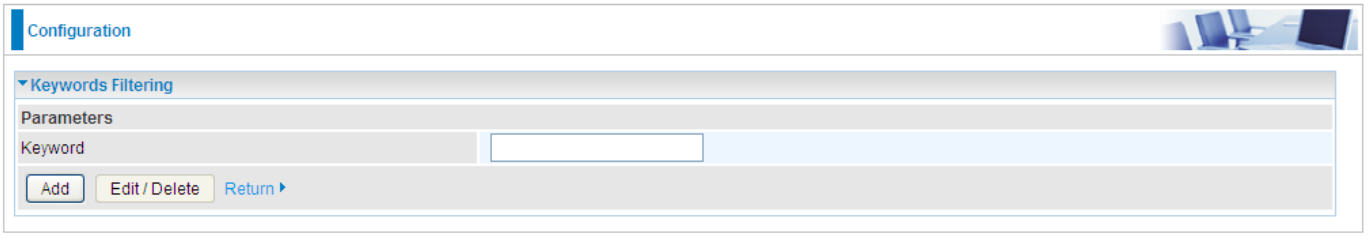


Keywords Filtering: Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g.to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

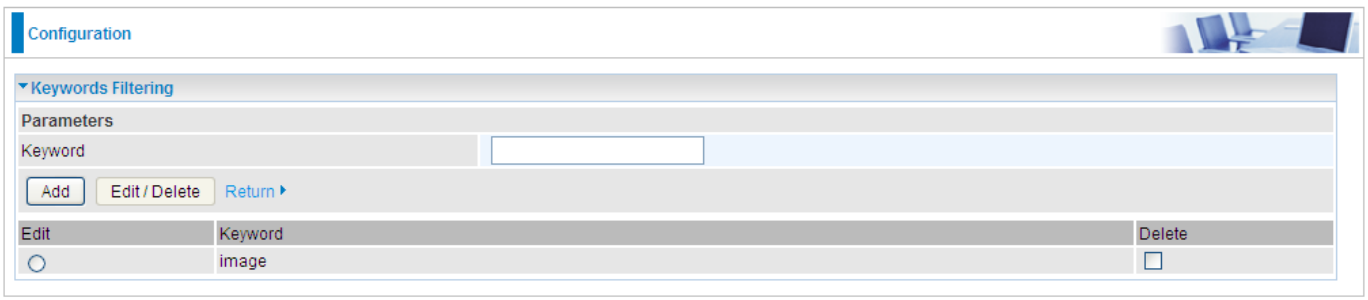
Detail >>

Note: Maximum number of entries: 32.

Click Detail ▸ to add the keywords.



Enter the Keyword, for example image, and then click **Add.**



You can add other keywords like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the

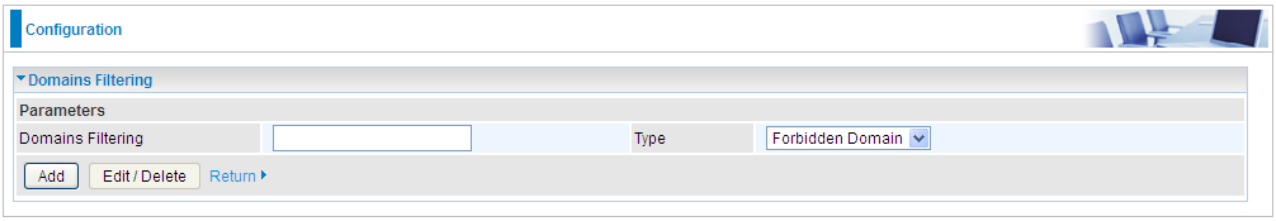
Keyword field, edit, and then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Detail >>

Note: Maximum number of entries: 32.

Click Detail to add Domains.



Domain Filtering: enter the domain you want this filter to apply.

Type: select the action this filter deals with the Domain.

- **Forbidden Domain:** The domain is forbidden access.
- **Trusted Domain:** The domain is trusted and allowed access.

Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to **Keywords Filtering** section in this manual**.**

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components.

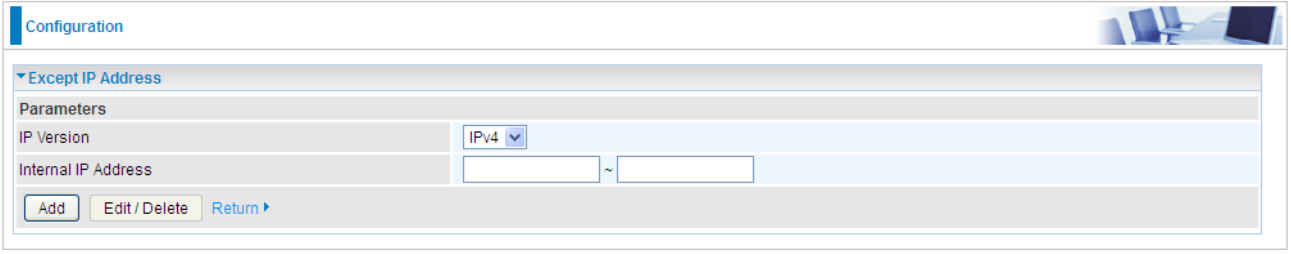
Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

Exception IP Address: You can input a list of IP addresses as the exception list for URL filtering; those IP addresses will not be covered by the URL rules.

Detail >>

In the section, users can set the exception IP respectively for IPv4 and IPv6.

Click Detail to add the IP Addresses.



Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the ***Exception List***, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords Filtering** section in this manual**.**

For example, users can set IPv4 client 192.168.1.103 in your network as a exception address that is not limited to the rules set in URL filter (or IPv4 clients (or in a range)). And also an IPv6 client

(2000:1211:1002:6ba4:d160:5adb:9009:87ae) or IPv6 clients can be the exceptions from the URL rules.

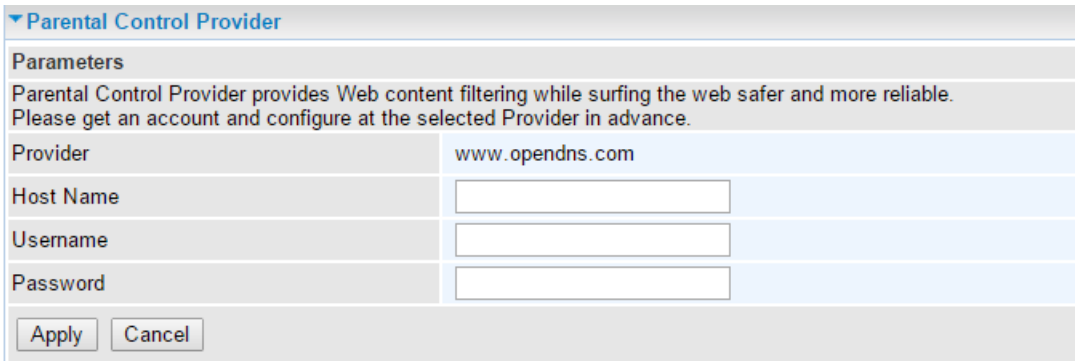
At the URL Filter page, press **Apply** to confirm your settings.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 of Sun to 19:00 of Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled. See Time Schedule.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy. To check the log, users can turn to Security Log.

Parental Control Provider

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.



To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

Parent Control Provider: Hosted by www.opendns.com

Host Name: It is the domain name of your OpenDNS. If you don't have one, please leave it blink.

Username / Password: Put down your OpenDNS account username and password

QoS - Quality of Service

Quality of Service

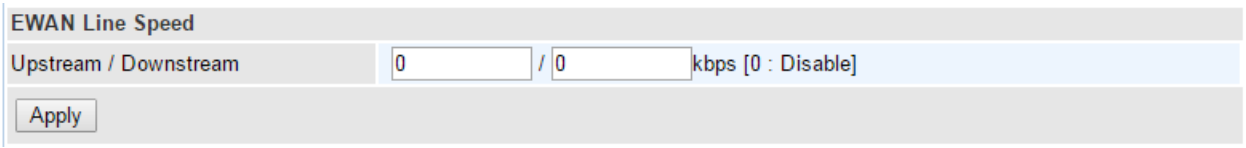
QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). This feature allows you to control the quality and speed of throughput for each application when the system is running with full upstream load.

EWAN Line Speed

Upstream / Downstream: Specify the upstream and downstream rate of the EWAN interface.

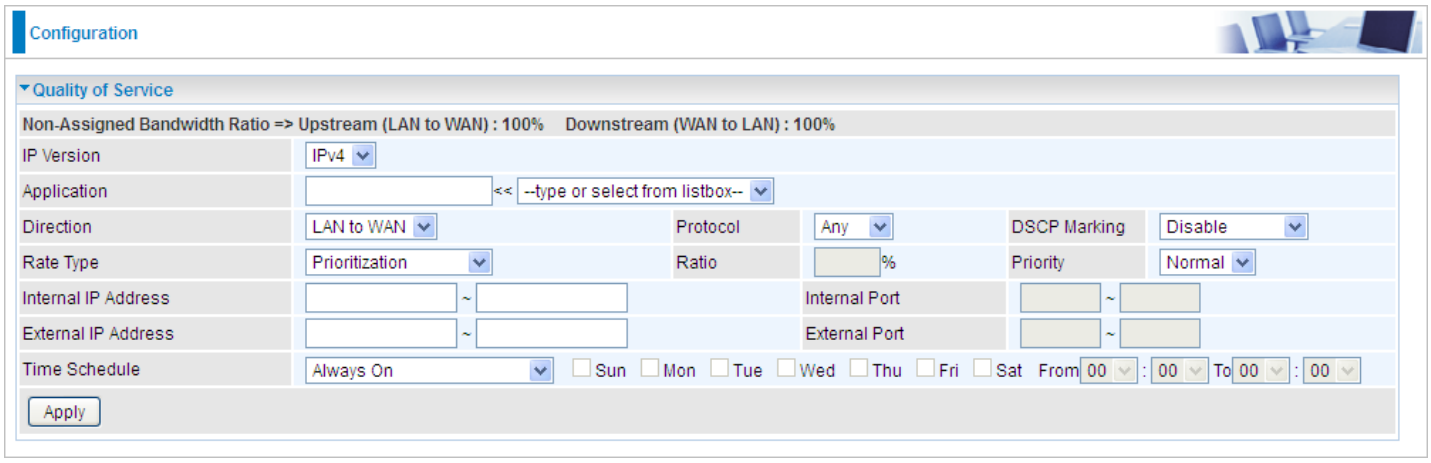
Note: ADSL line speed is based on the ADSL sync rate.

Click **Apply** to save the EWAN rate settings.



Add New QoS Rules

Click **Add** to create a QoS rule.



IP Version: Select either IPv4 or IPv6 base on need.

Application: Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

Direction: Shows the direction mode of the QoS application.

- **LAN to WAN:** You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application.

  Example: If you have a FTP server inside the local network and want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.

- **WAN to LAN:** Control traffic from WAN to LAN (Downstream).

Protocol: Select the supported protocol from the drop down list.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP

Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

IP Precedence and DSCP Mapping Table

Mapping Table	
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP offers three levels of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four levels of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Rate Type: You can choose ***Limited*** or ***Prioritization***.

- **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximum rate for this policy. When you choose ***Limited***, type the ***Ratio*** proportion. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- **Prioritization:** Specify the rate type control for the rule to use. If you choose ***Prioritization*** for the rule, you parameter ***Priority*** would be available, you can set the priority for this rule.

- **Set DSCP Marking:** When select ***Set DSCP Marking***, the packets matching the rule will be forwarded according to the pre-set DSCP marking.

Ratio: The rate percent of each application/policy compared to total traffic on the interface with limited rate type. For example, we want to only allow 20% of the total data for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps rate, the estimated data rate, in kbps, for this rule is 20%*256*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8)

Priority: Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

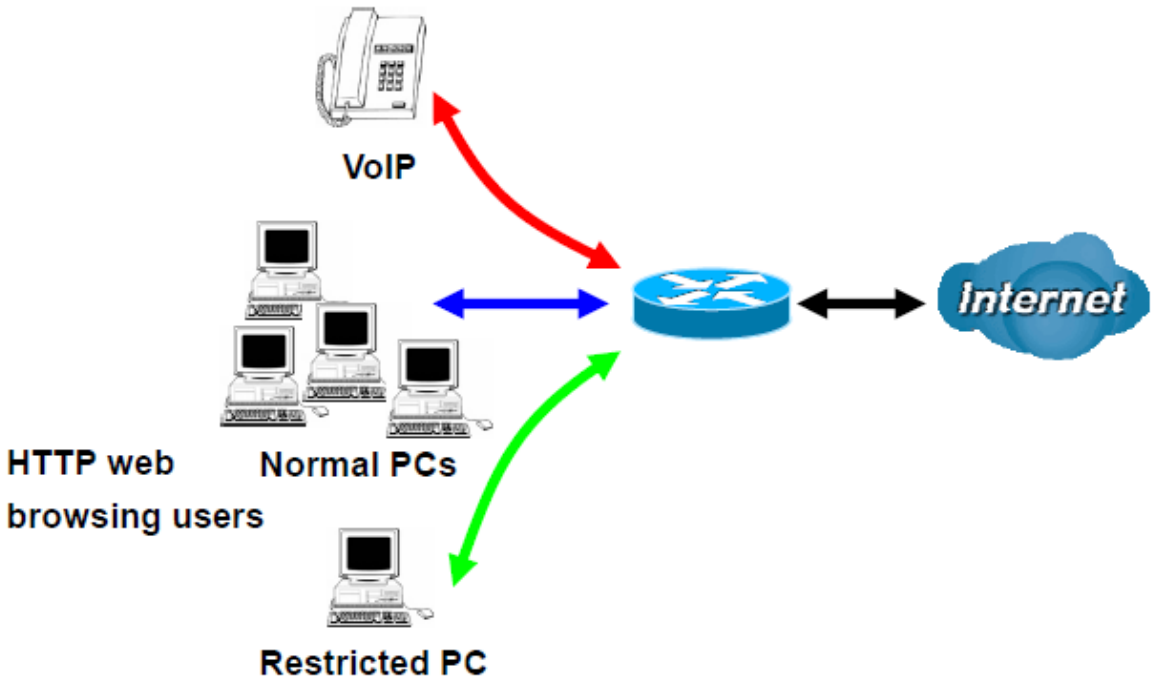
Internal Port: The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

External Port: The Port number on the remote / WAN side.

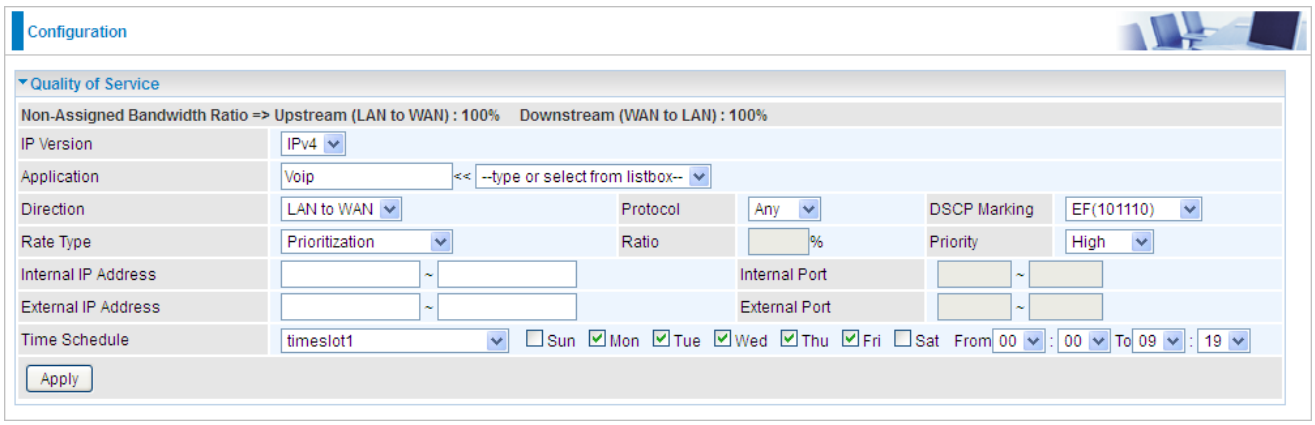
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 of Sun to 19:00 of Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”  ” indicating the rule is inactive. See Time Schedule.

Example:

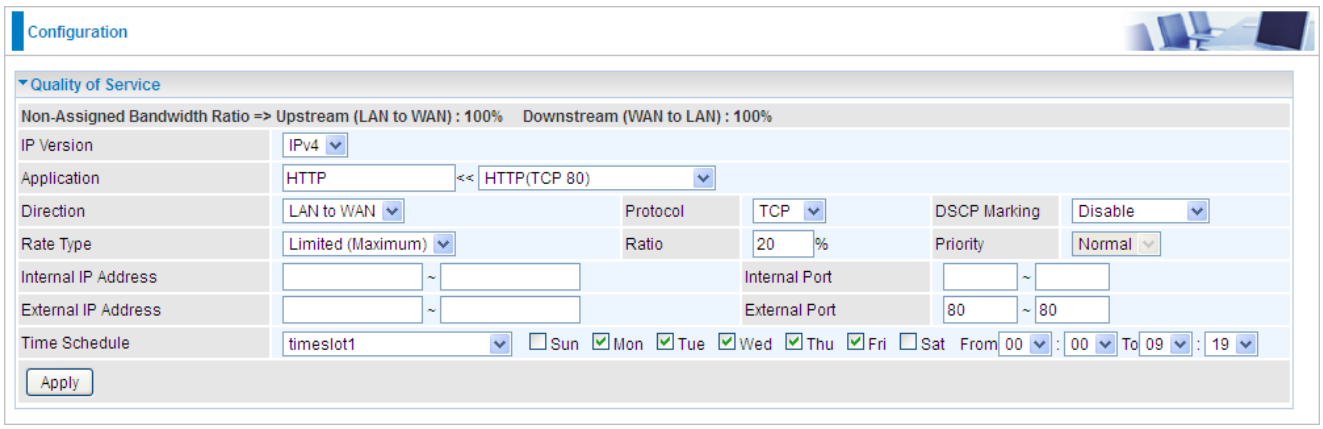


1. Assign high priority to outgoing VoIP traffic.

The default queue priority is normal, so if you have VoIP users in your local network, you can set a higher priority to the outgoing VoIP traffic.

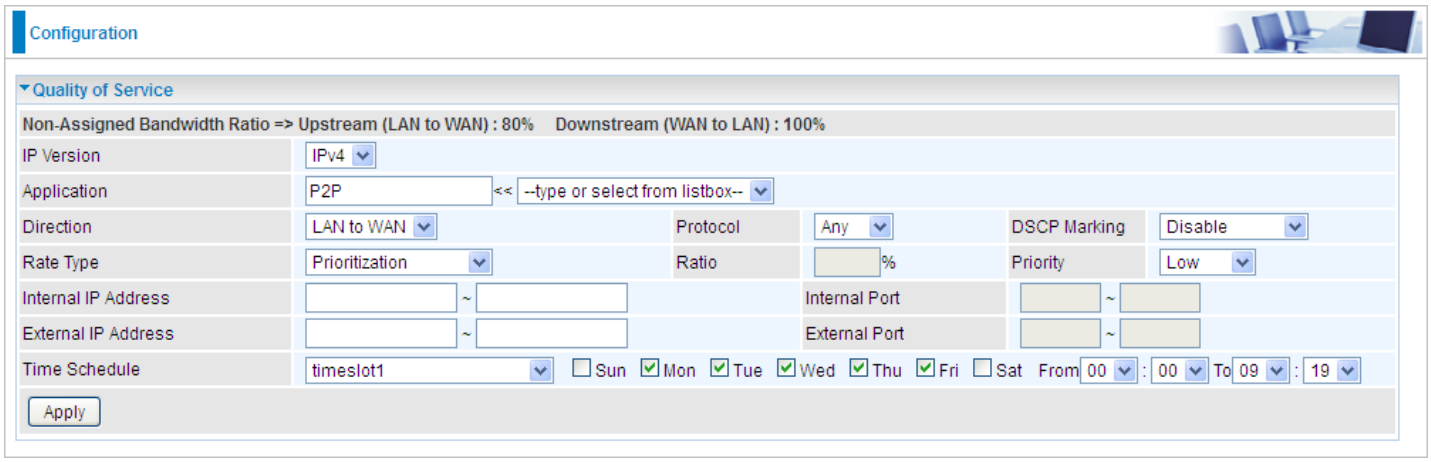


2. Limit bandwidth for HTTP access



3. If you are actively engaged in P2P and are afraid of slowing down internet access for other users

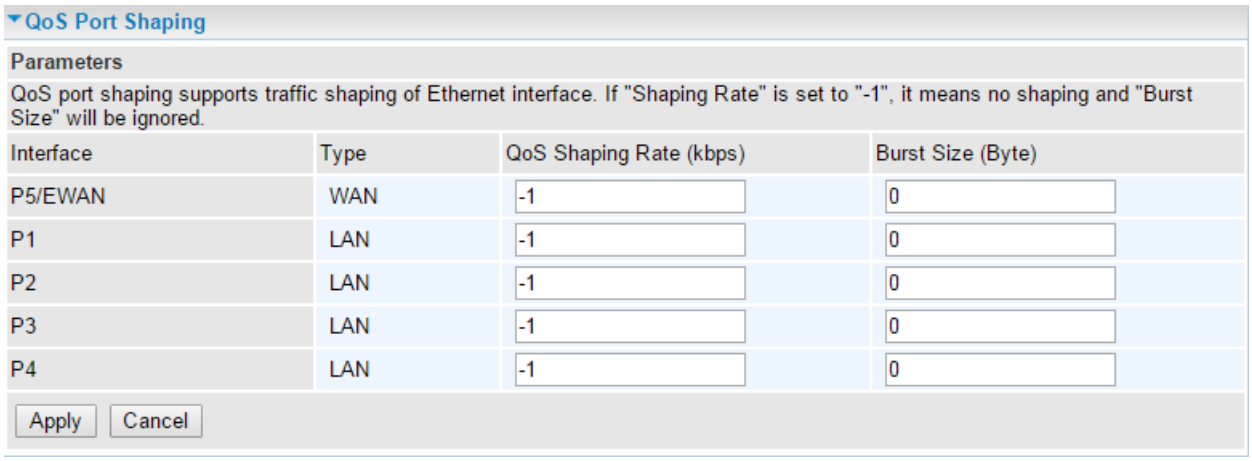
within your network, you can then use QoS to set a rule that has low priority. In this way, P2P application will not congest the data transmission with other applications.



You can also use QoS to limit bandwidth or set priority for applications such as FTP, Mail access, etc., based on your requirement.

QoS Port Shaping

QoS port shaping supports traffic shaping of Ethernet interfaces. It forcefully maximizes the throughput of the Ethernet interface. When “Shaping Rate” is set to “-1”, no shaping will be in place and the “Burst Size” is to be ignored.



Interface: P1-P4. P4 used as EWAN also covered.

Type: All LAN when P4 is LAN port; P4 used as EWAN, type WAN and all others LAN.

QoS Shaping Rate (Kbps): Set the forcefully maximum rate.

Burst Size (Bytes): Set the forcefully Burst Size.

NAT

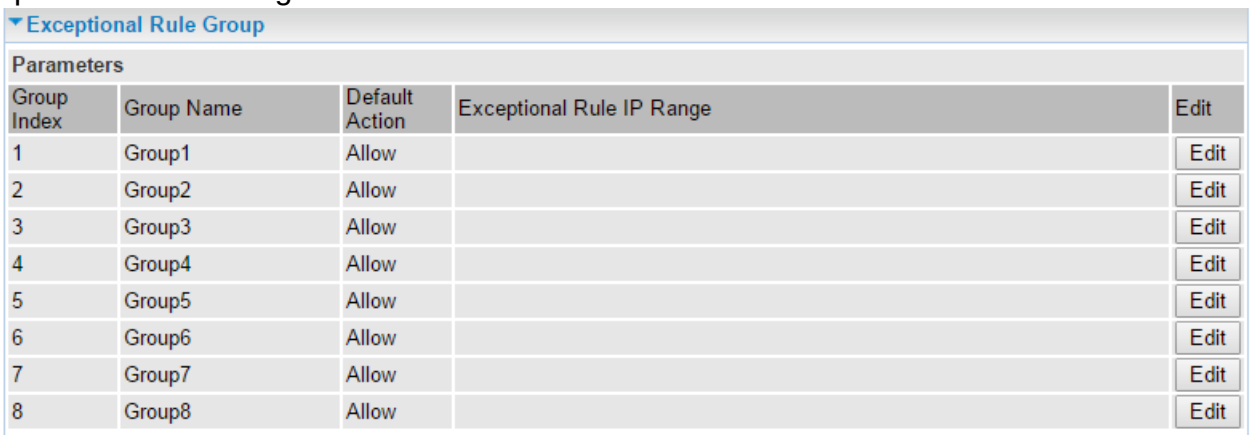
NOTE: This feature disables automatically if WAN connection is in BRIDGE mode.

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

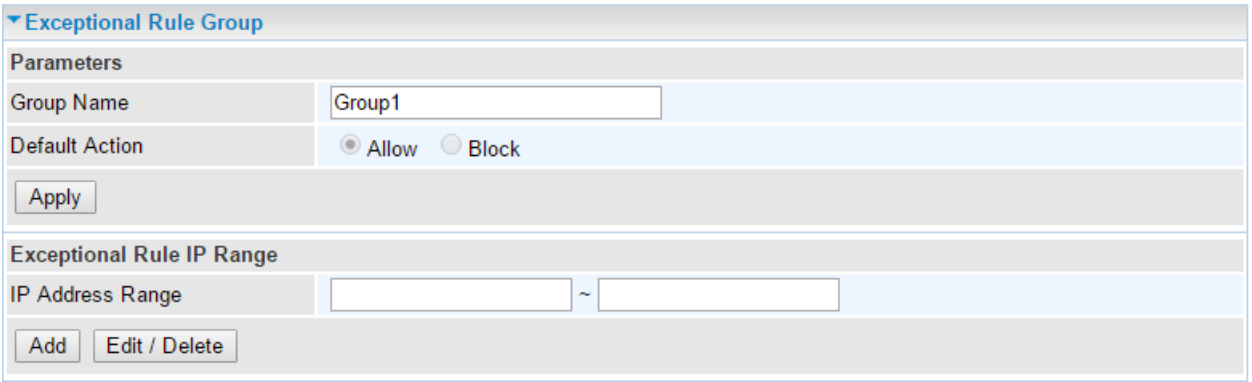
Exceptional Rule Group

Exceptional Rule is dedicated to giving or blocking NAT/DMZ access to some specific IP or IPs(range).

Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



Click **Edit** to configure the group.



Parameters

Group Name: Assign a name to this group

Default Action

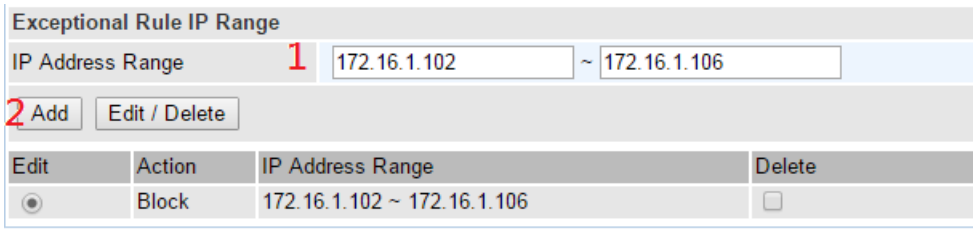
- **Allow** to grant access to the listed IP or IPs to Virtual Server and DMZ Host.
- **Block** to ban the listed IP or IPs to access the Virtual Server and DMZ Host.

Click **Apply** to save the settings

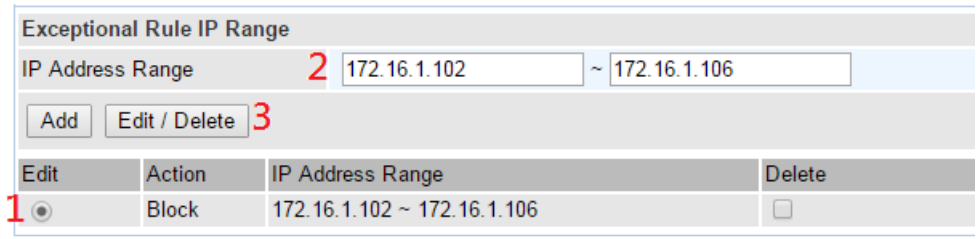
Exceptional Rule Range

IP Address Range: Specify the IP address range; IPv4 address range can be supported.

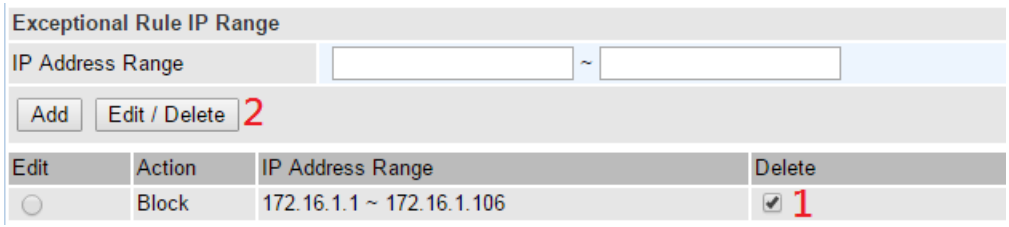
To **Add** a new entry: Click **Add** to create a new IP or IP Range.



To **Edit** an existing entry: Click **Edit** radio button of the entry you want to edit, then click **Edit / Delete** button to make changes



To **Delete** an existing entry: Click **Delete** check-box of the entry you want to delete, then click **Edit / Delete** to remove it.



Virtual Servers

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

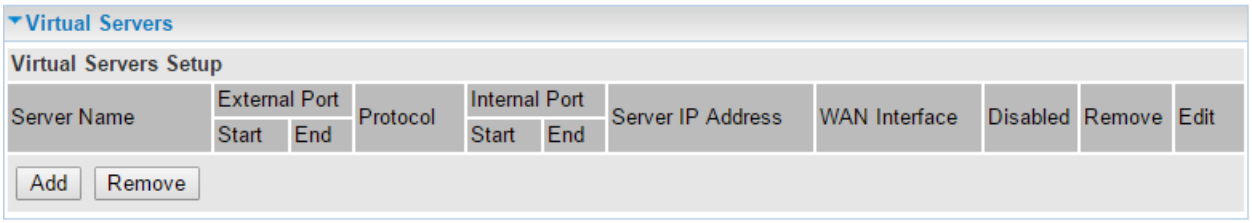
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

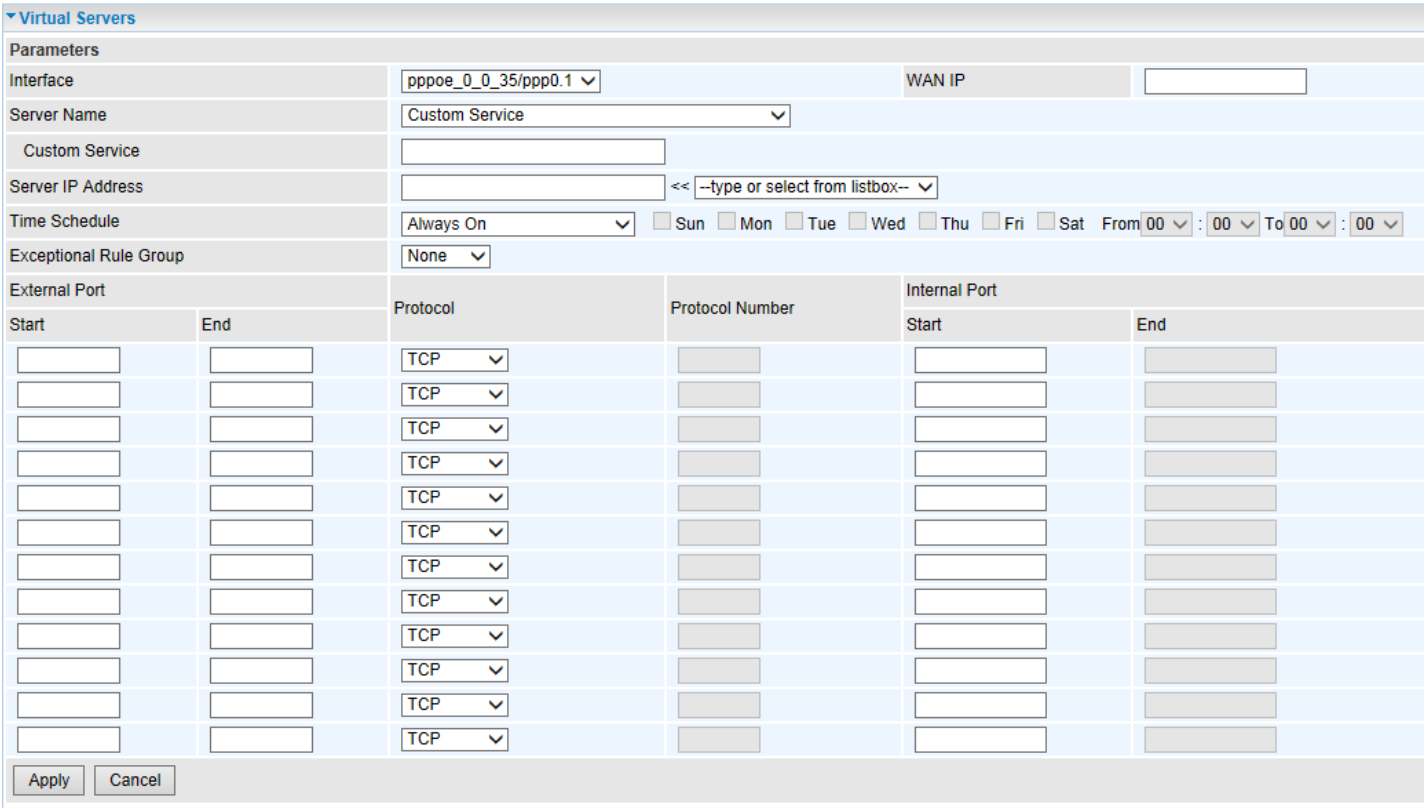
The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

This part is only available when NAT is enabled.

Note: The maximum number of entries: 64.



It is virtual server listing table as you see, Click **Add** to create a new Virtual Server entry.



Interface (WAN): select from the drop-down menu the interface you want the virtual server(s) to apply to.

WAN IP: When there are multiple external/WAN IP addresses are available on the WAN interface; specify the WAN IP address for this virtual server entry.

Server Name: select the server name from the drop-down menu.

Custom Service: It is a kind of service to let users customize the service they want. Enter the user-defined service name here. It is a parameter only available when users select **Custom Service** in the above parameter. Leave it blank if using the current external WAN IP address or only one WAN IP is available.

Server IP Address: Enter server (in the network) IP Address. Click the drop-down box of **Type or select from list box** for a list of available network device IP addresses for quick setup.

Time Schedule: Select or set exactly when the Virtual Server works. When set to “Always On”, the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to “Disable”, the rule is disabled and there will be an icon in the list table indicating the rule is disabled. See Time Schedule.

Exceptional Rule Group: Select an exceptional group from the list. It is to grant or block NAT access to a group of IPs. Example, if we had Group_1, in the **Exceptional Rule Group** section, configured to block an IP range, 172.16.1.102-172.16.1.106, from accessing to the Virtual Server.

External Port

- **Start:** Enter a port number as the external starting number for the range you want to give access to internal network.
- **End:** Enter a port number as the external ending number for the range you want to give access to internal network.

Internal Port

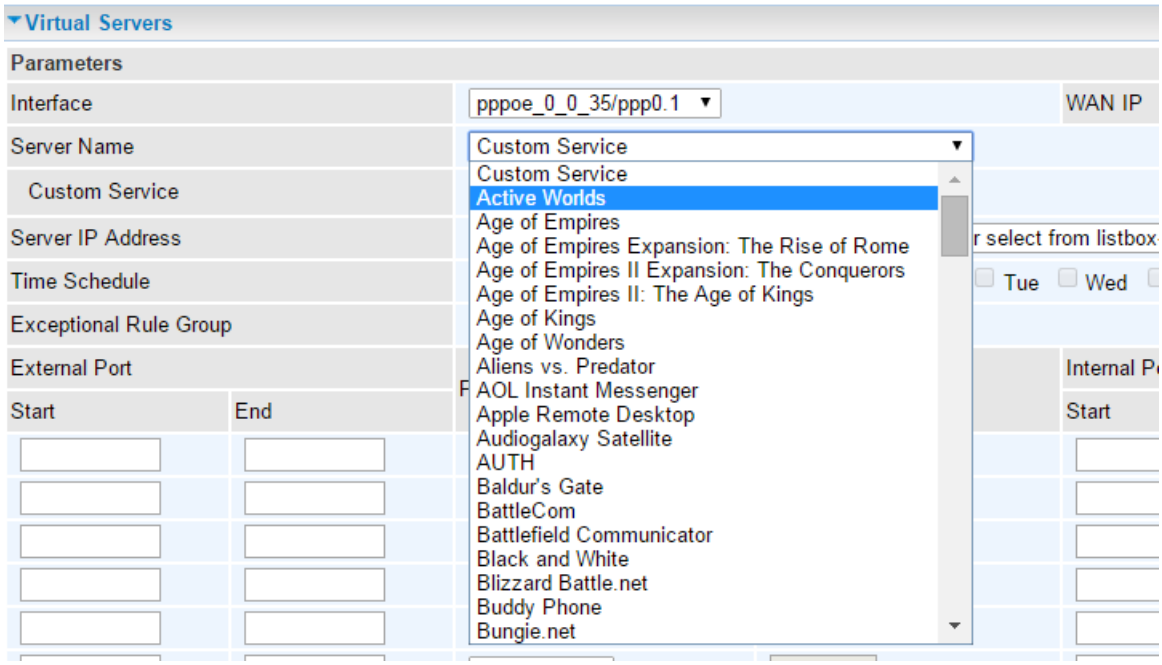
- **Start:** Enter a port number as the internal staring number.
- **End:** Here it will generate automatically according to the End port number of External port and can't be modified.

Protocol: select the protocol this service used: TCP/UDP, TCP, and UDP.

Time Schedule: Select or set exactly when the Virtual Server works. When set to "Always On", the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 of Sun to 19:00 of Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to "Disable", the rule is disabled and there will be an icon ✓ in the list table indicating the rule is disabled. See Time Schedule.

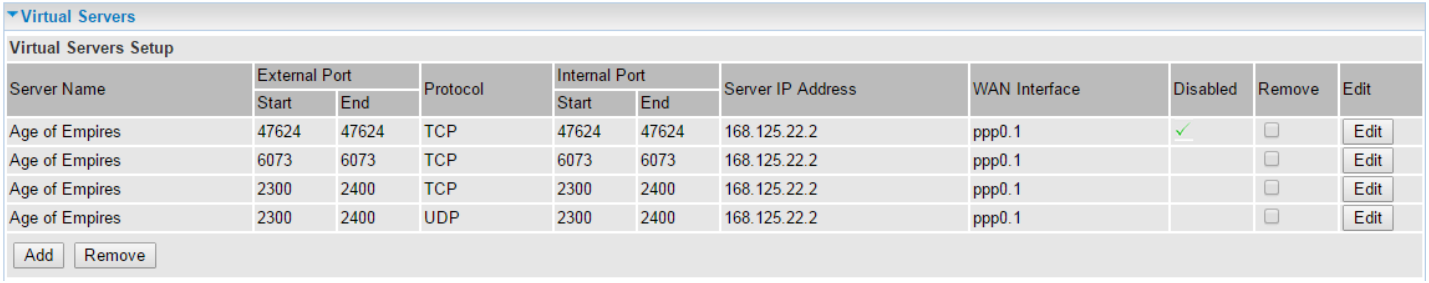
Example: How to create and delete a Virtual Server rule

1. Select a **Server Name** from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.



If **Server Name** does not contain the application you are looking for. You may manually create a rule of your own by specifying the **Server IP Address, External Port**, and **Internal Port**.

Click **Apply** to save the settings.

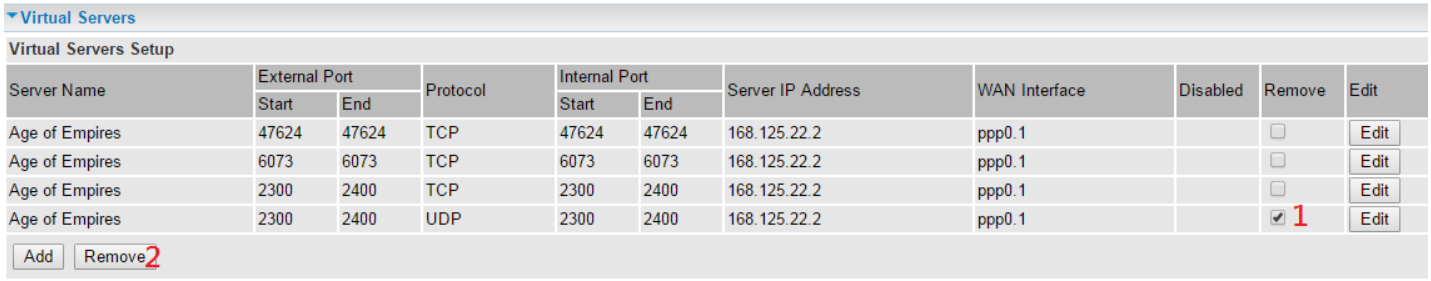


Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	168.125.22.2	ppp0.1	✓		Edit
Age of Empires	6073	6073	TCP	6073	6073	168.125.22.2	ppp0.1			Edit
Age of Empires	2300	2400	TCP	2300	2400	168.125.22.2	ppp0.1			Edit
Age of Empires	2300	2400	UDP	2300	2400	168.125.22.2	ppp0.1			Edit

This new rule will be listed in the **Virtual Servers Setup** table.

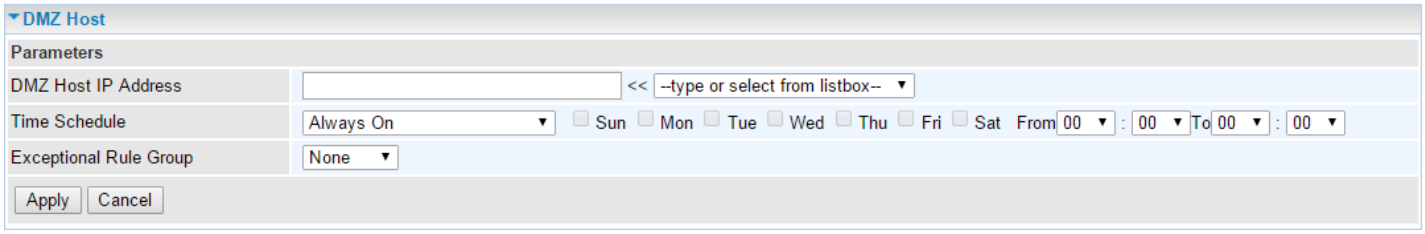
(✓ Means the rule is currently inactive)

To remove a rule, simply click the check-box of the unwanted rule then click **Remove** to delete it.



DMZ Host

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by Firewall and NAT algorithms before being passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.



DMZ Host IP Address: Enter the IP Address of a host you want it to be a DMZ host. Select from the list box to quick set the DMZ.

Time Schedule: Select or set exactly when the DMZ works. When set to “Always On”, the DMZ will work all time; and also you can set the precise time when DMZ works, like 01:00 of Sun to 19:00 of Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to “Disable”, the rule is disabled. See Time Schedule.

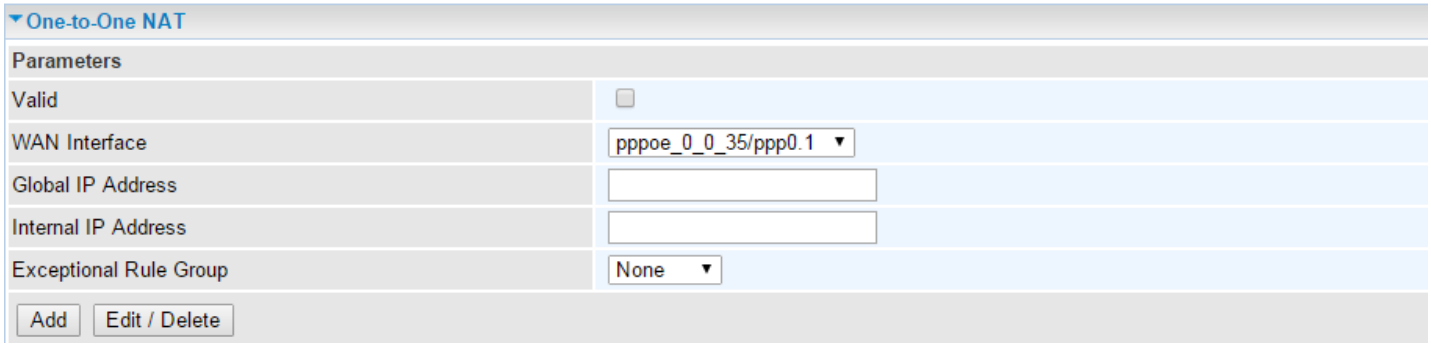
Exceptional Rule Group: Select an exceptional group from the list. It is to grant or block NAT access to a group of IPs. Example, if we had Group_1, in the **Exceptional Rule Group** section, configured to block an IP range, 172.16.1.102-172.16.1.106, from accessing to the DMZ.

NOTE!	Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

Attention	If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid. If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address. If user has multiple global/public IP addresses from your ISP, you are free to use one-to-one NAT to assign some specific public IP for an internal IP like a public web server mapped with a global/public IP for outside access.



Valid: Check whether to valid the one-to-one NAT mapping rule.

WAN Interface: Select one based WAN interface to configure the one-to-one NAT.

Global IP address: The Global IP mapped to an internal device. It can be left empty, and under this circumstance, it can be reached through the WAN IP of interface set in the field above.

Internal Address: The IP address of an internal device in the LAN.

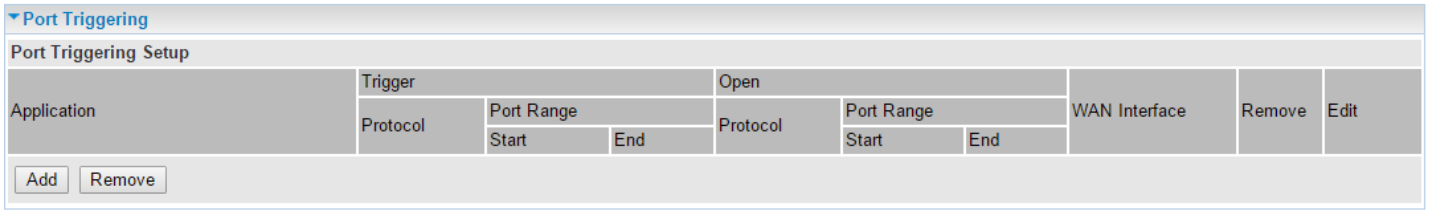
Exceptional Rule Group: Select an exceptional group from the list. It is to grant or block NAT access to a group of IPs. Example, if we had Group_1, in the **Exceptional Rule Group** section, configured to block an IP range, 172.16.1.102-172.16.1.106, from accessing to the One-to-One NAT.

Example: you have an ADSL connection of pppoe_0_8_35/ppp0.1 interface with three fixed global IP, and you then can assign the other two global IPs to two internal devices respectively.

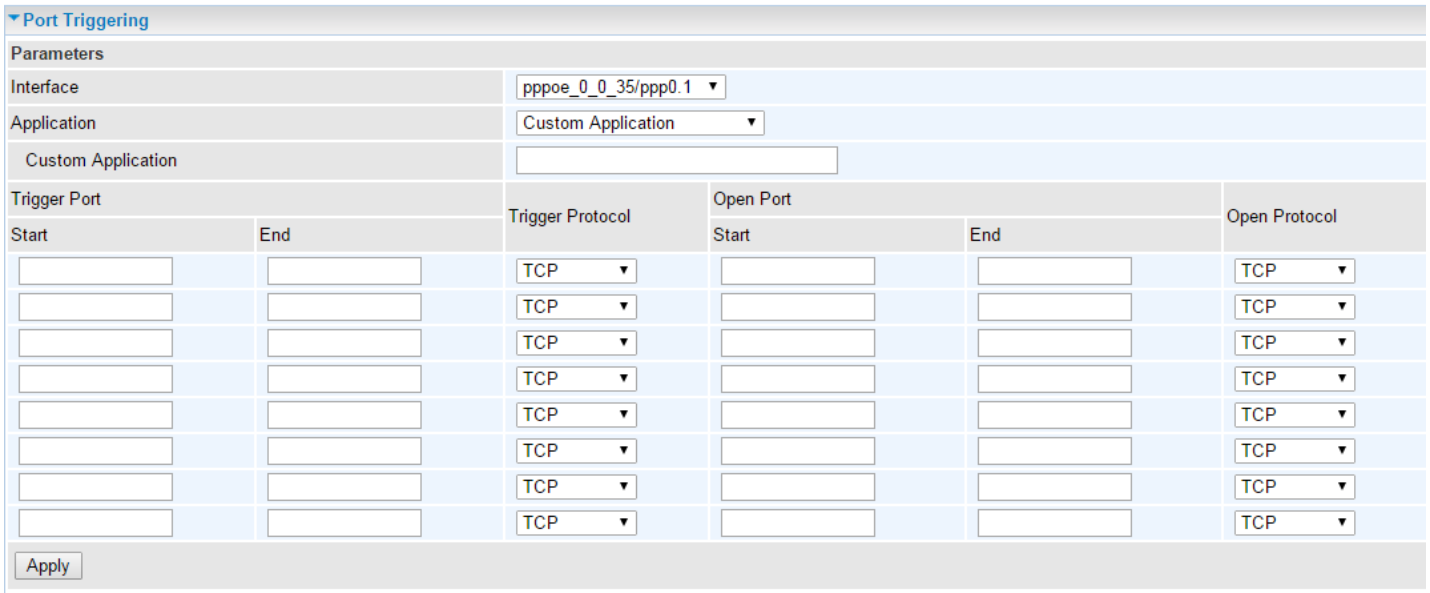
If you have a WEB server (IP address: 192.168.1.3) and a FTP server (IP address: 192.168.1.4) in local network, owning a public IP address range of 123.1.1.2 to 123.1.1.4 assigned by ISP. 123.1.1.2 is used as WAN IP address of the router, 123.1.1.3 is used for WEB server and 123.1.1.4 is used for FTP server. With One-to-One NAT, the servers with private IP addresses can be accessed at the corresponding valid public IP addresses.

Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.



Click **Add** to add a port triggering rule.



Interface: Select from the drop-down menu the interface you want the port triggering rules apply to.

Application: Contains a list of pre-configured applications with trigger port for quick access and setup

Custom Application: If **Application** does not contain the application you are looking for. Given a name to this rule and specify Trigger Ports, Protocol, Open Port and Open Protocol.

Trigger Port

- **Start:** Enter a port number as the triggering port starting number.
- **End:** Enter a port number as the triggering port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

Open port

- **Start:** Enter a port number as the open port staring number.
- **End:** Enter a port number as the open port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the preset forwarding port or open port.

Protocol: select the protocol this service used: TCP/UDP, TCP, and UDP.

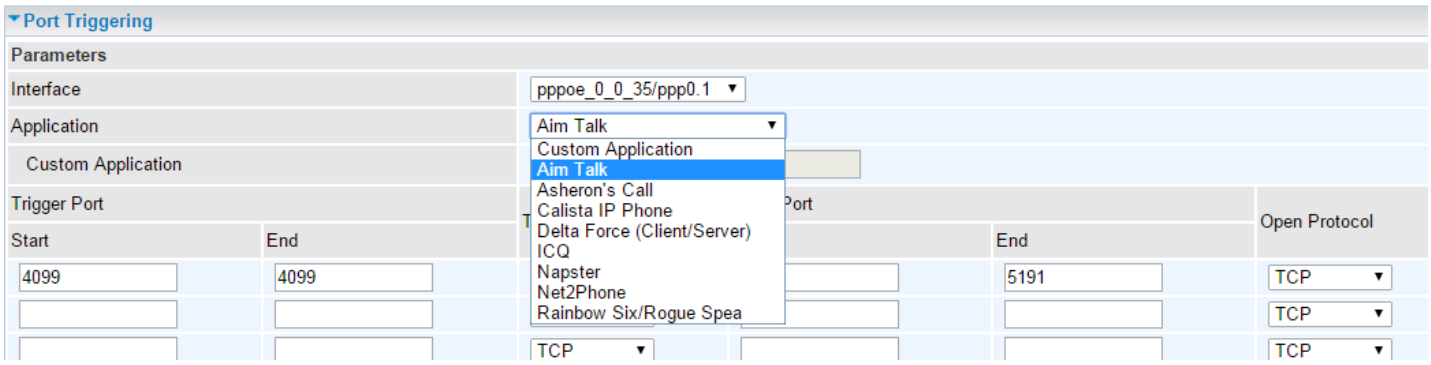
Example: How to create and delete a Virtual Server rule

An example of how port triggering works, when a client behind a NAT router connecting to Aim Talk, it is a TCP connection with the default port 4099.

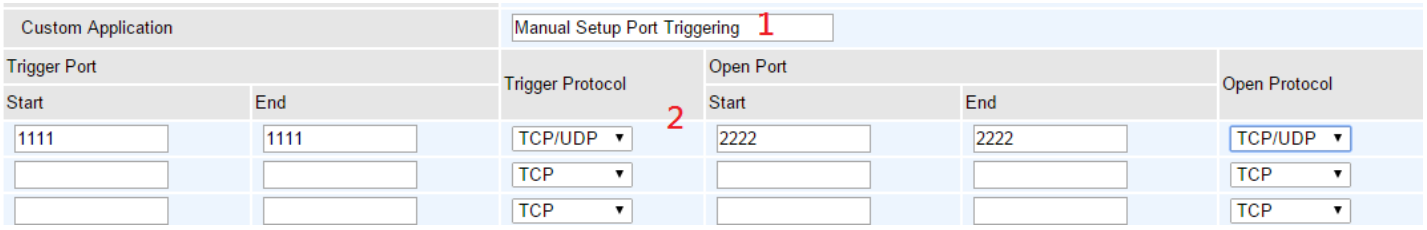
When connecting to Aim Talk, the client typically makes an outgoing connection on port 4099 to the Aim Talk server, but when the computer is behind the NAT, the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

So, in this case, port triggering in the router is working, when an outbound connection is attempted on port 4099 (or any port in the range set), it should allow inbound connections to that particular computer.

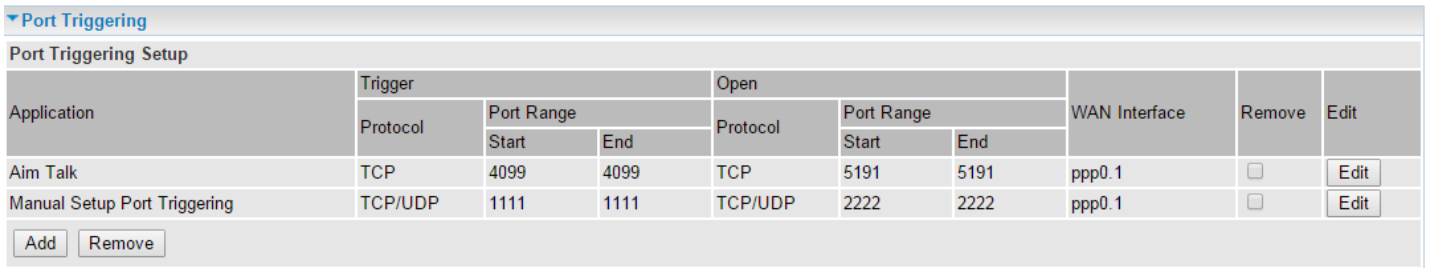
1. Select a **Server Name** from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.



Manually create a rule of your own If Application does not contain the application you are looking for.

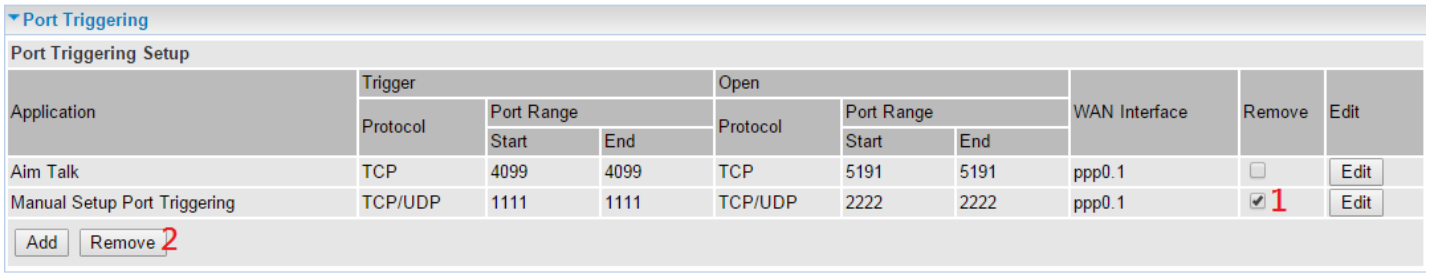


Click **Apply** to save the settings.



New rules will be listed in the **Port Triggering** table.

To remove a rule, simply click the check-box of the unwanted rule then click **Remove** to delete it.



Port Triggering

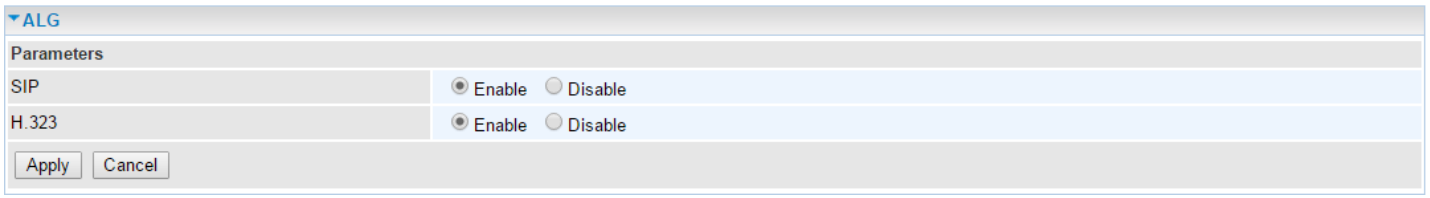
Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove	Edit
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	☐	Edit
Manual Setup Port Triggering	TCP/UDP	1111	1111	TCP/UDP	2222	2222	ppp0.1	☑ 1	Edit

Add Remove 2

ALG

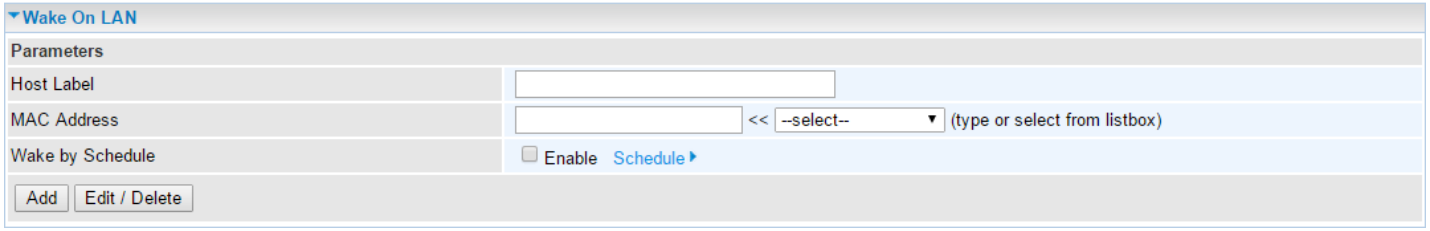
Application Layer Gateway (ALG) to help resolve NAT related problems for VoIP services.



Enable SIP and /or H.323 to allow system to make decision to either block or allow VoIP traffic to passthrough the NAT.

Wake on LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



Host Label: Given a name to this service.

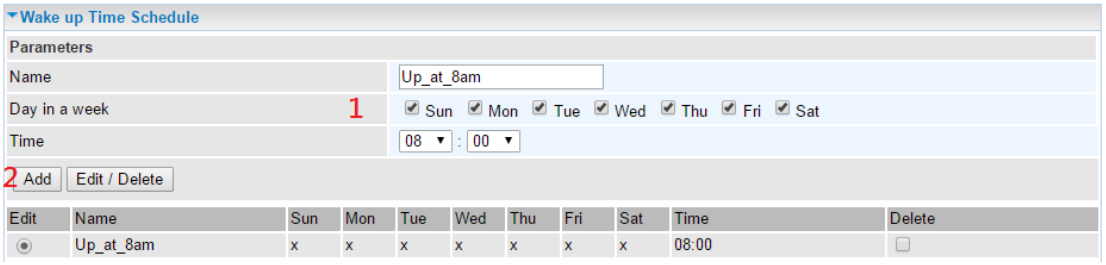
Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Wake by Schedule: Enable to wake up your set device at some specific time. For instance, user can set to get some device woken up at 8:00 every weekday. Click **Schedule** to enter time schedule configuring page to set the exact timeline.

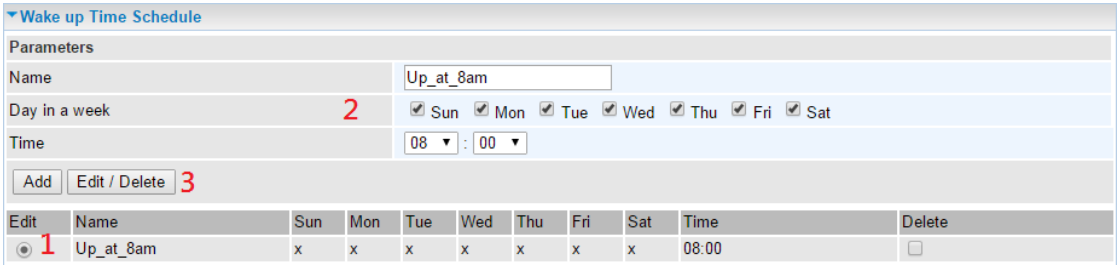
Setup a Schedule

To add new entries, Set the device to wake up at 8:00am everyday from Sunday thru Saturday.

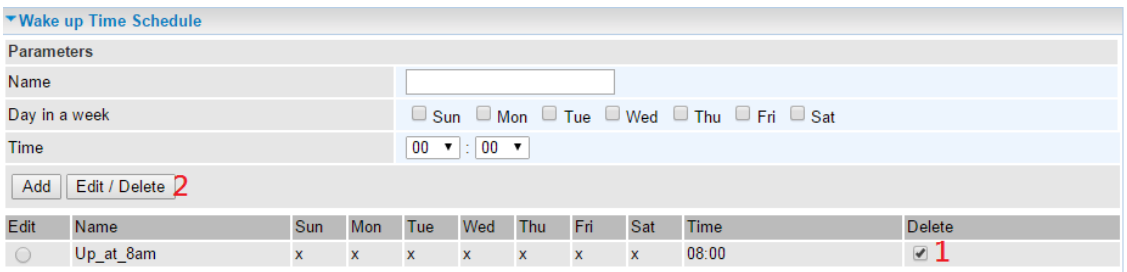
Click **Add** to add a time schedule.



To make changes, click **Edit** button of a WAN entry to re-configure the settings.



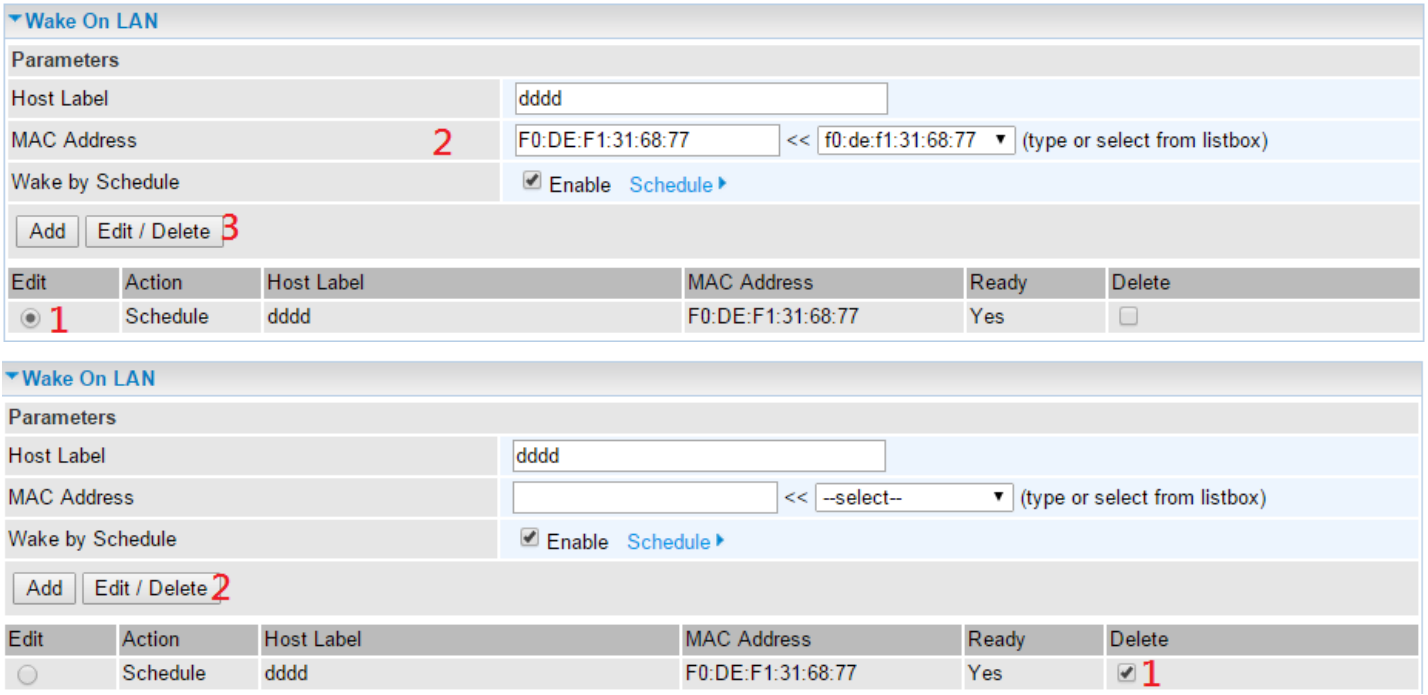
To delete entries, simply click **checkboxes** of the unwanted schedules then click **Delete** to remove entries.



Click **Add** to add a rule.

Ready:

- **Yes:** Indicates the remote computer is ready for your waking up.
- **No:** Indicates the remote computer is not ready, e.g. it is being powered off.

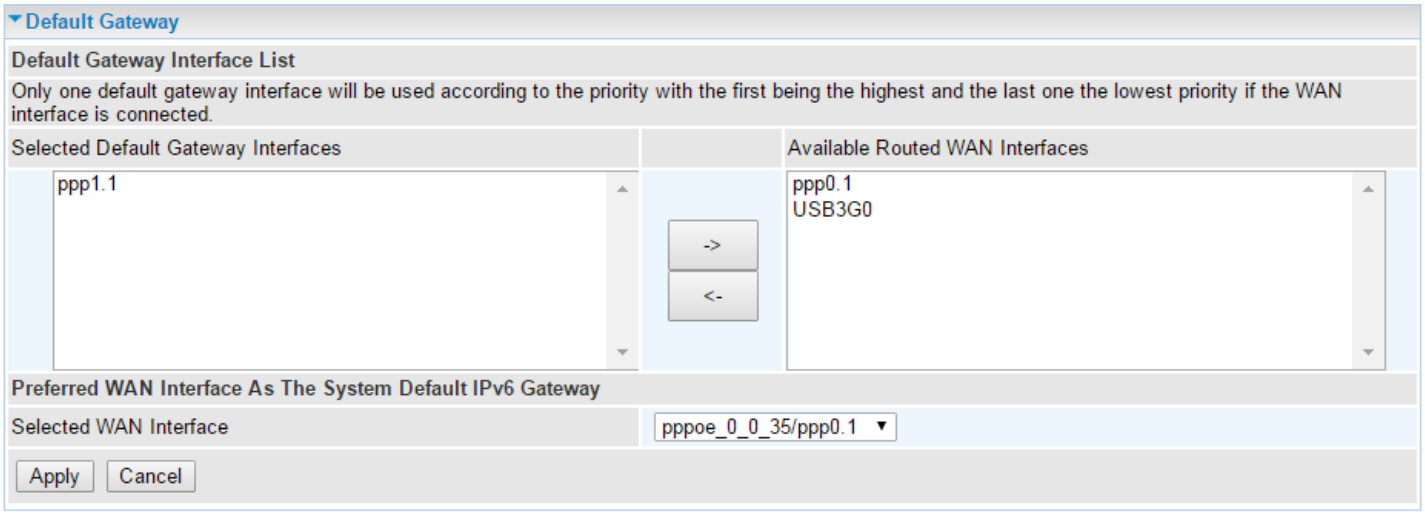


Advanced Setup

Routing

Default Gateway

Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.



Select an appreciated WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected Default Gateway Interface** box

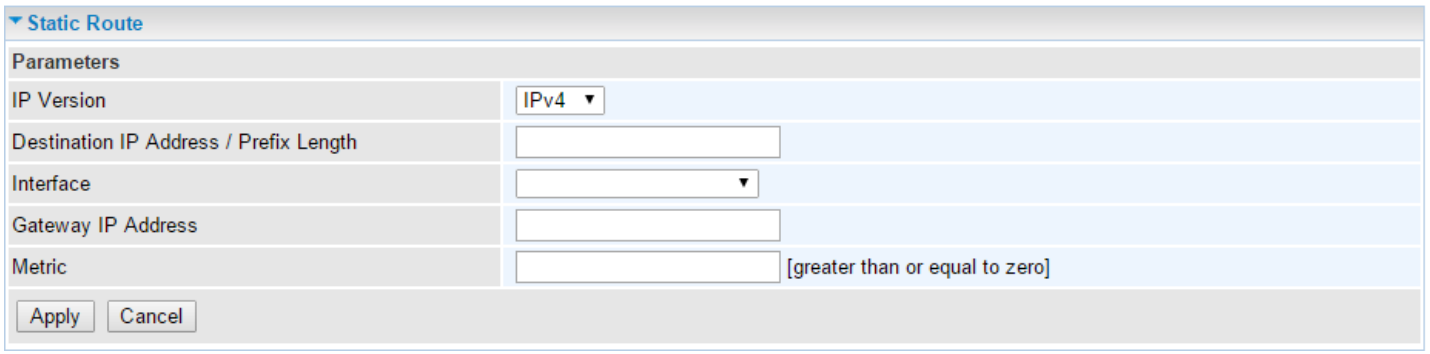
To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

For IPv6, please select a Default IPv6 Gateway from the drop-down menu.

Static Route

With static route feature, you can control the routing of all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed.

Above is the static route listing table, click **Add** to create static routing.



IP Version: Select the IP version, IPv4 or IPv6.

Destination IP Address / Prefix Length: Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask; it is another mode of presenting submask. One IPv4 address,192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

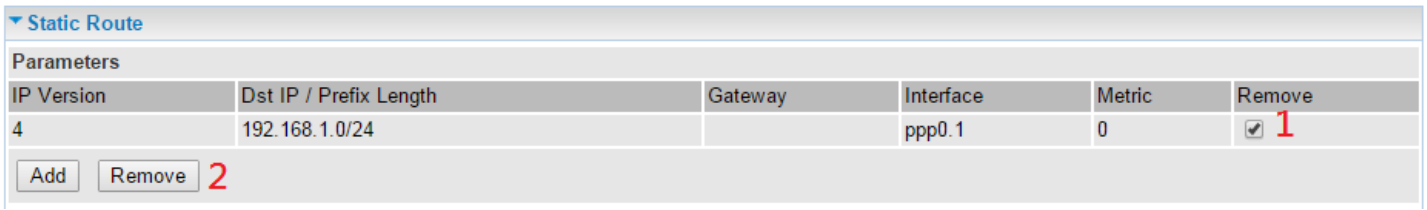
Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

To remove an entry, click the check-box of the unwanted entry then click **Remove** to delete it.

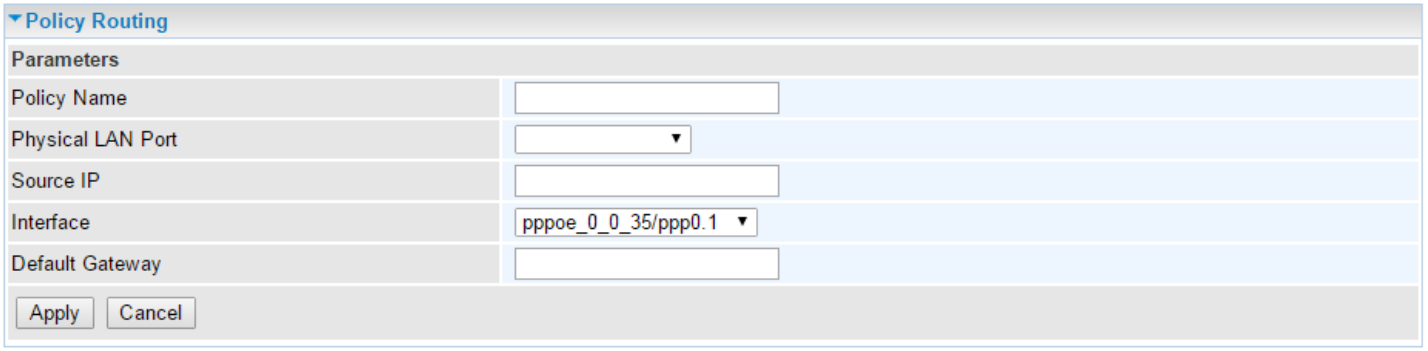


Policy Routing

Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

The following is the policy Routing listing table.

Click **Add** to create a policy route.



Policy Name: Given a name to this new policy rule.

Physical LAN Port: Select the LAN port.

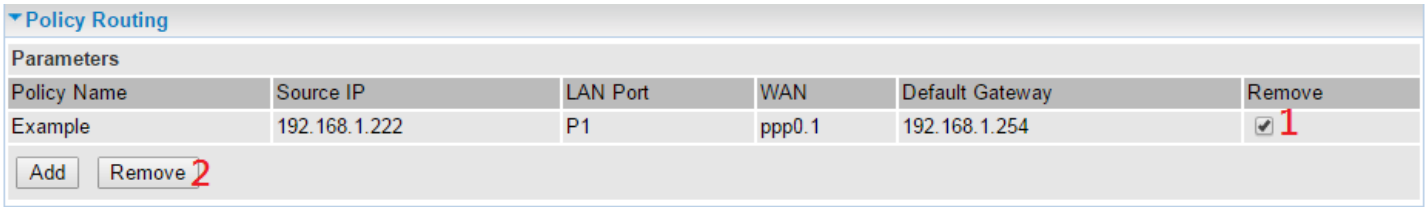
Source IP: Enter the Host Source IP.

Interface: Select the WAN interface which you want the Source IP to access outside through.

Default Gateway: Enter the default gateway which you want the Source IP to access outside through.

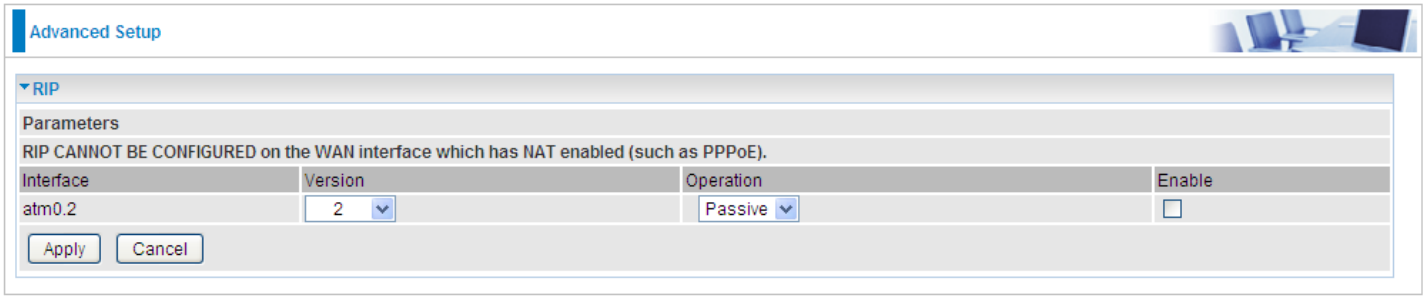
Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table.

To remove an entry, click the check-box of the unwanted entry then click **Remove** to delete it.



RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.



Interface: the interface the rule applies to.

Version: select the RIP version, there are two versions, RIP-1 and RIP-2.

Operation: RIP has two operation modes.

- **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- **Active:** working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

Enable: check the checkbox to enable RIP rule for the interface.

Note: RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE).

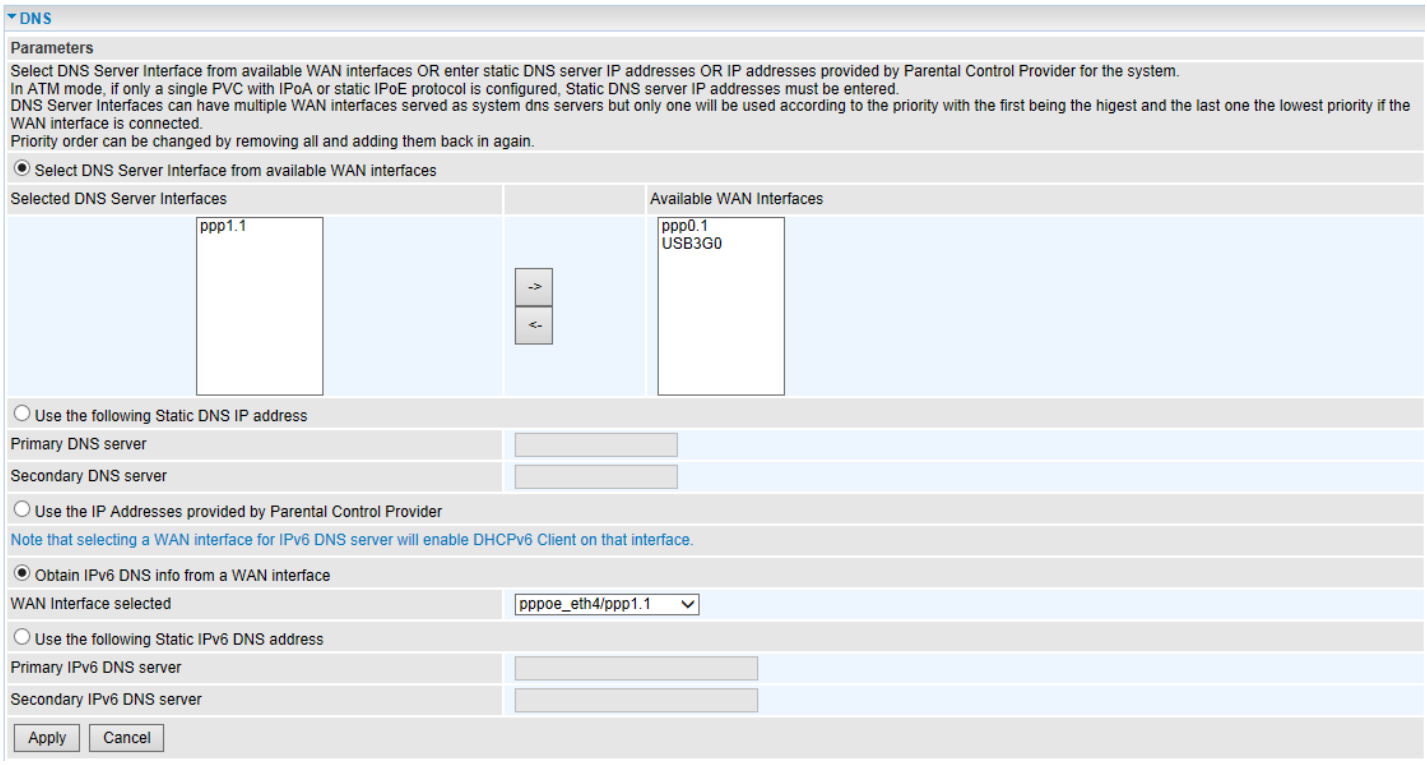
Click **Apply** to apply the settings.

DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation of Domain name to IP.

DNS

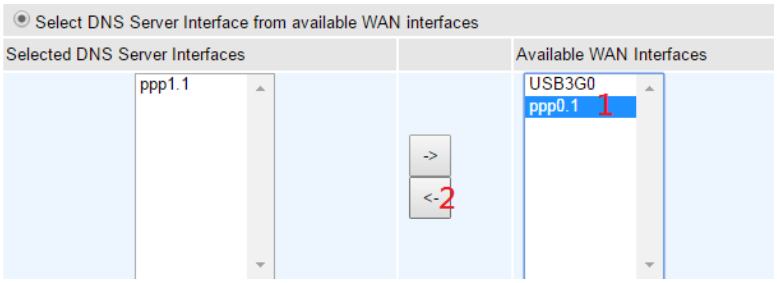
IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.



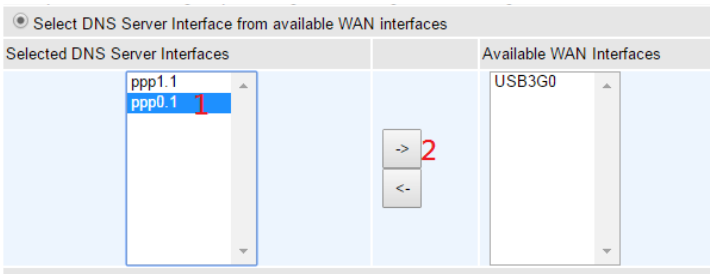
DNS for IPv4

DNS Server Interfaces

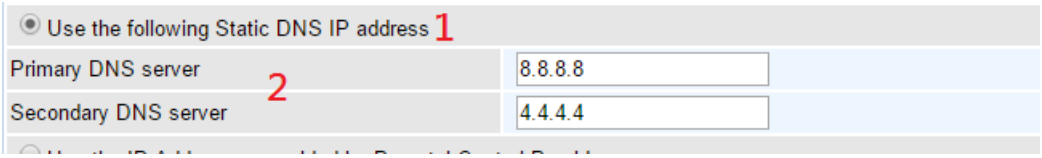
1. **Select DNS Server Interface:** Select a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected DNS Server Interface** box



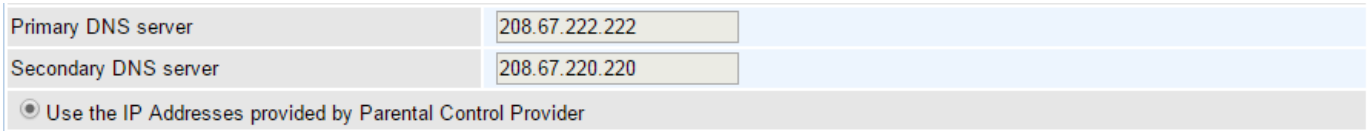
To remove interface(s) from **Selected DNS Server Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.



2. **Static DNS IP Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.



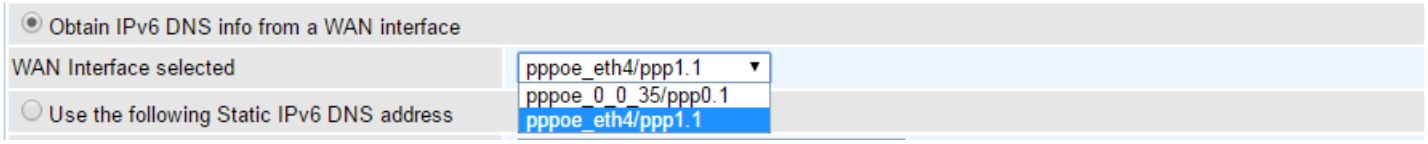
3. **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).



DNS for IPv6

DNS Server Interfaces

1. **Obtain IPv6 DNS from a WAN interface:** If your Internet Service Provider assigns DNS server address along with the WAN connection, please select an appropriated IPv6 WAN interface from **DNS Server Interface.**



2. **Use Static DNS IPv6 Address:** If your Internet Service Provide does not provide or you wish to use other DNS servers for your network, simply manually enter other DNS server IP address here:

   Primary / Secondary IPv6 DNS Server: Enter the specific primary and secondary IPv6 DNS Server address.

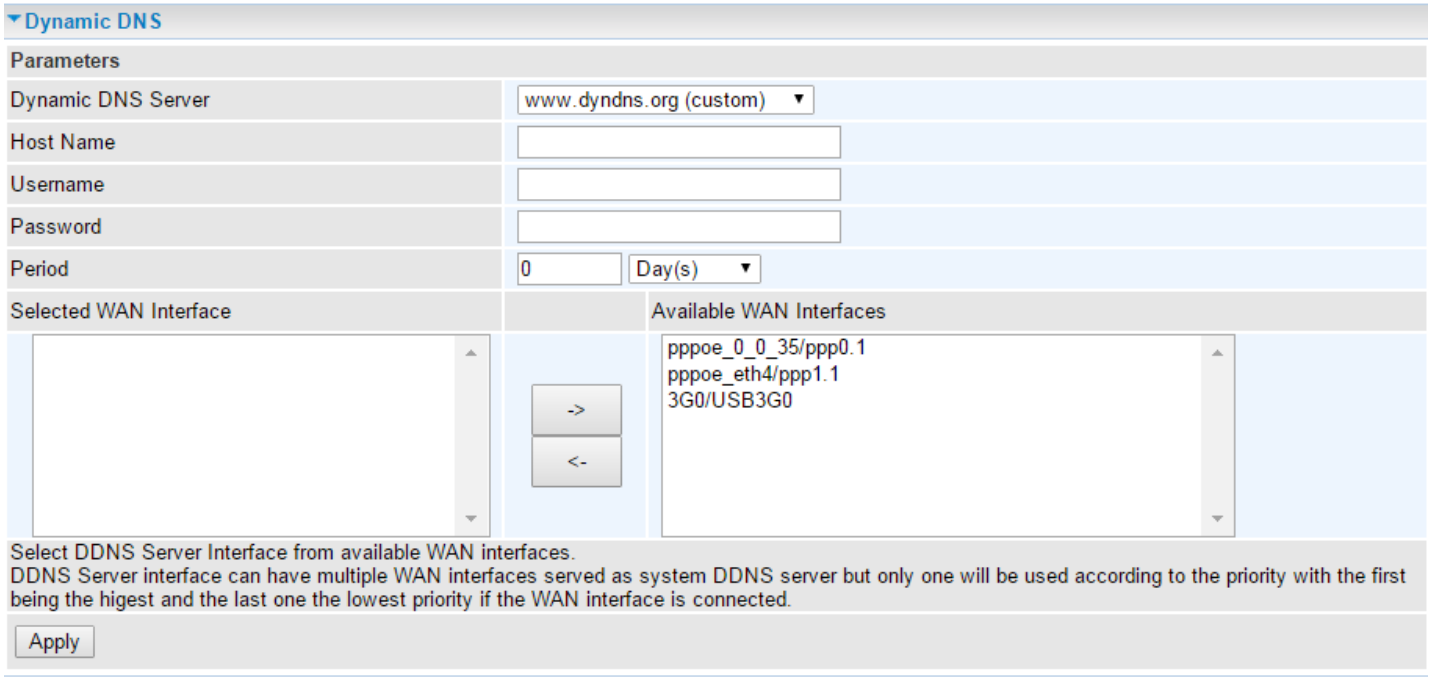
Click **Apply** to save the settings.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es).

Click **Add** to register a WAN interface with a DDNS Provider.



You will first need to register and establish an account with the Dynamic DNS provider using their website, for example **http://www.dyndns.org/**

Dynamic DNS Server: Select the DDNS service you have established an account with.

Host Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period on how often the MX-1000 will update the DDNS server with your current external IP address.

WAN Interface: Select the Interface that is bound to the registered Domain name. Pick a desirable WAN interface from **Available WAN Interface** box then using the left-arrow sign (←) to move it to the **Selected WAN Interface** box

To remove WAN interface(s) from **Selected WAN Interface** box, simply click the unwanted interface then use the right-arrow sign (→) to re move it.

Example: How to setup DDNS with different WAN interfaces

If you do not have an account with Dynamic DNS, please go to www.dyndns.org to register an account first.

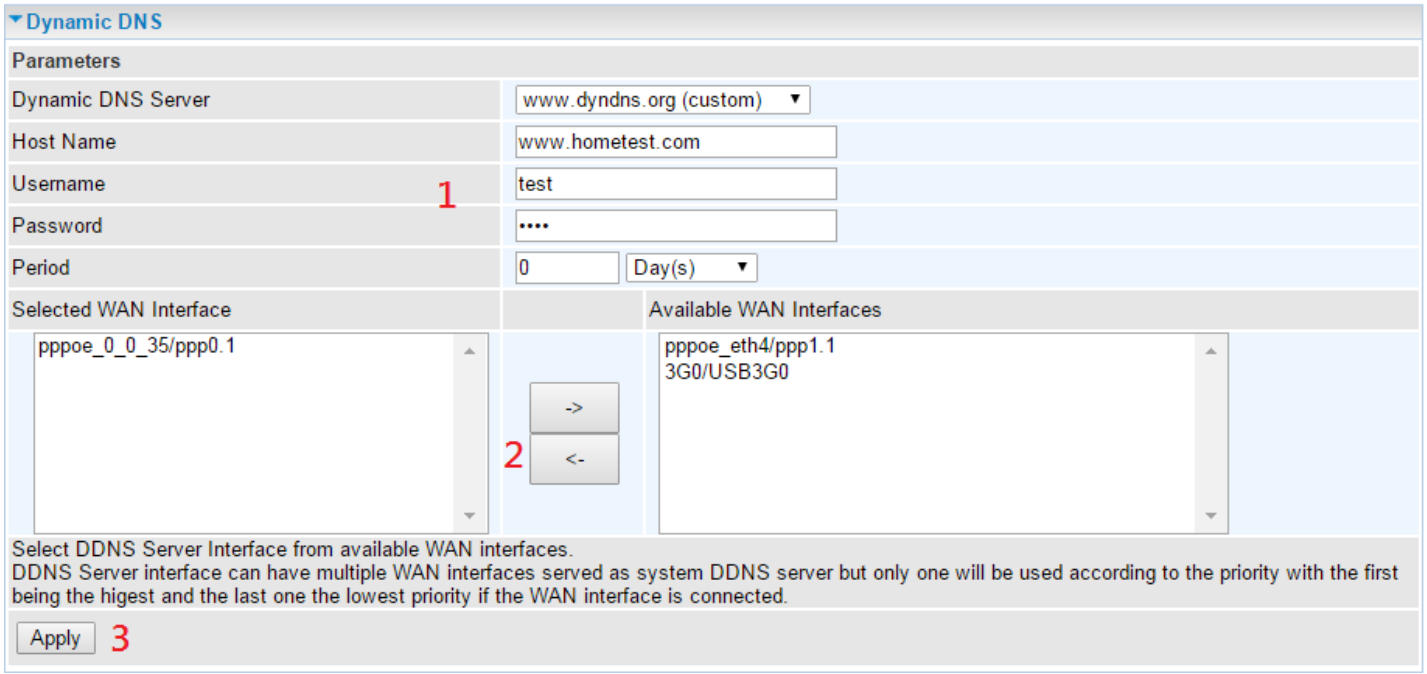
Use same account, ***test,*** to register two (2) DDNS hostname. .

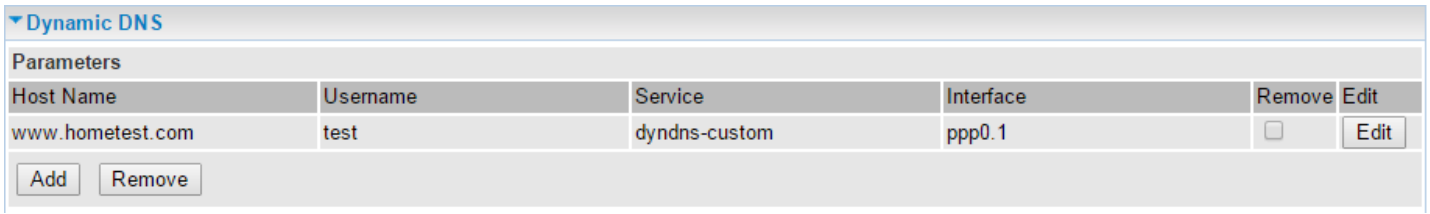
Account 1: DDNS Hostname as www.hometest.com

Using pppoe_0_0_35 WAN interface and username /password as test/test

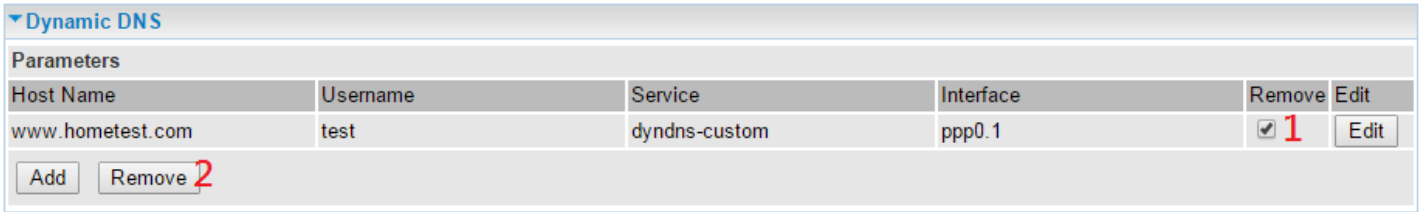
Click **Apply** to save the settings.

A new entry will appear on the **Dynamic DNS** page





To remove a rule, simply click the check-box of the unwanted rule then click **Remove** to delete it.

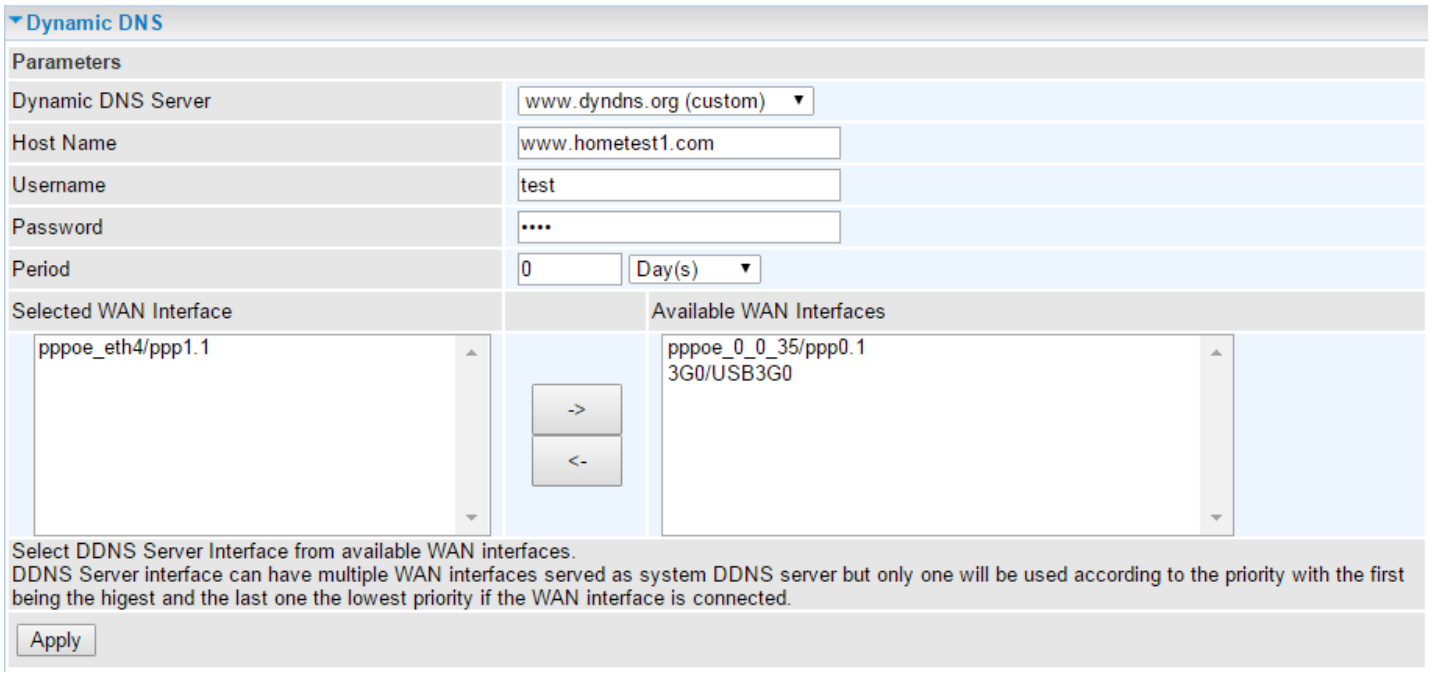


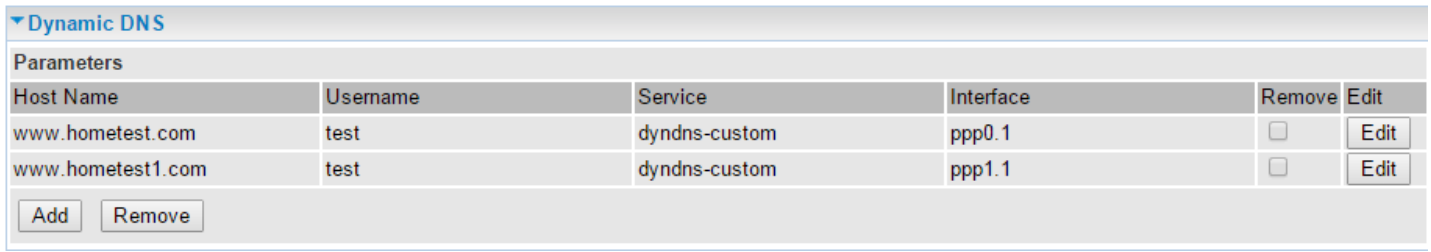
Account 2: DDNS Hostname as www.hometest1.com

Using pppoe_eth4 WAN interface and username /password as test/test

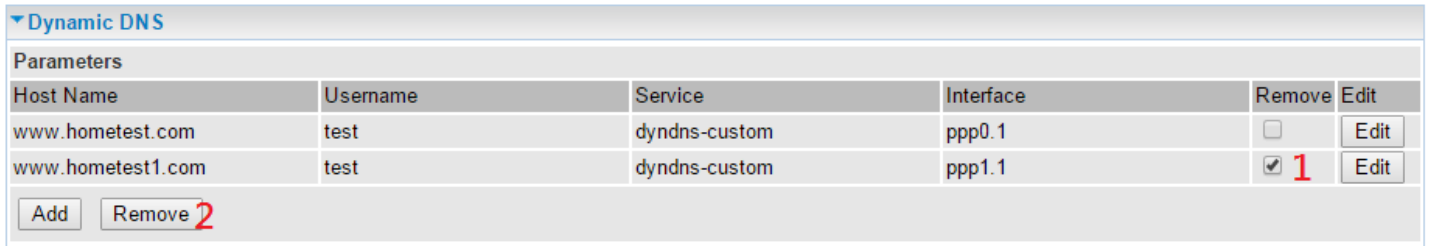
Click **Apply** to save the settings.

Another new entry will appear on the **Dynamic DNS** page





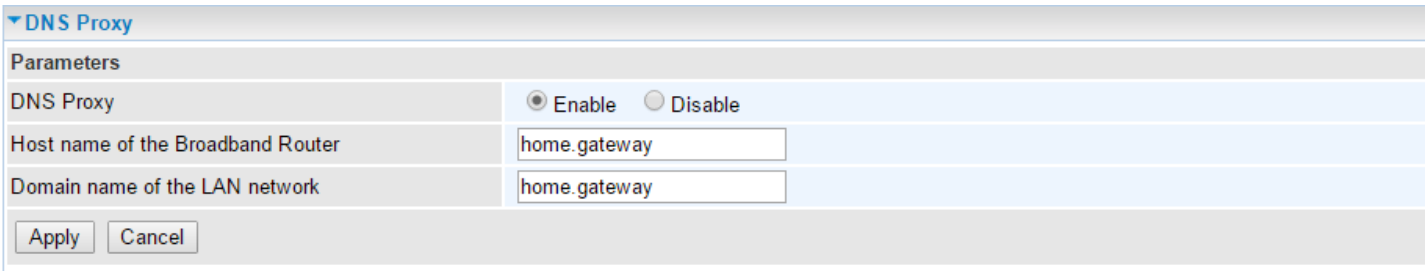
To remove a rule, simply click the check-box of the unwanted rule then click **Remove** to delete it.



DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server.

Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.



DNS Proxy: Select whether to enable or disable DNS Proxy function, default is enabled.

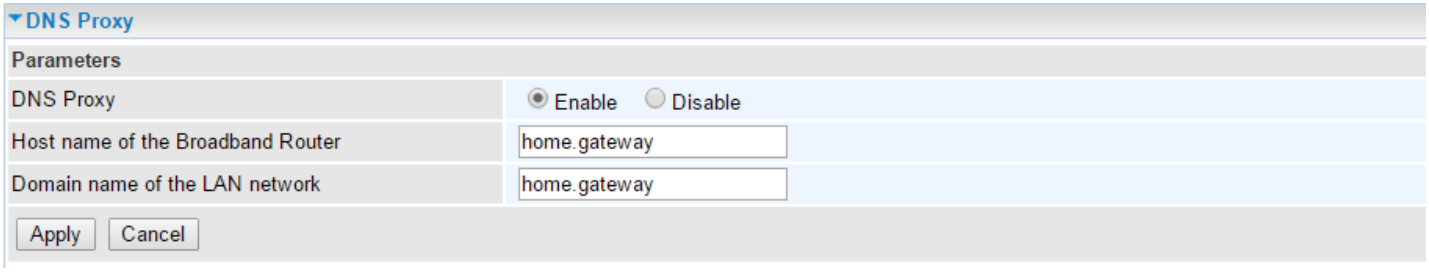
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.

Domain name of the LAN network: Enter the domain name of the LAN network. home.gateway.

Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.



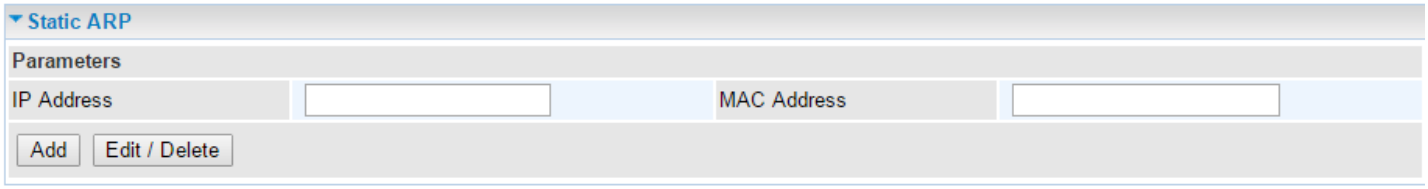
Host Name: Type the domain name (host name) for the specific IP .

IP Address: Type the IP address bound to the set host name above.

Click **Add** to save your settings.

Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.



IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

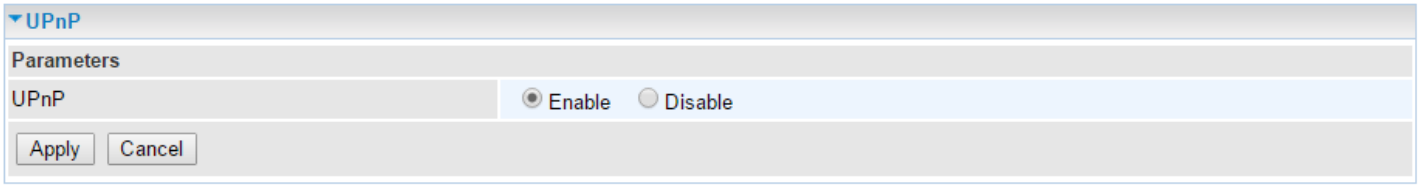
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click **Add** to confirm the settings.

UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user’s Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



UPnP:

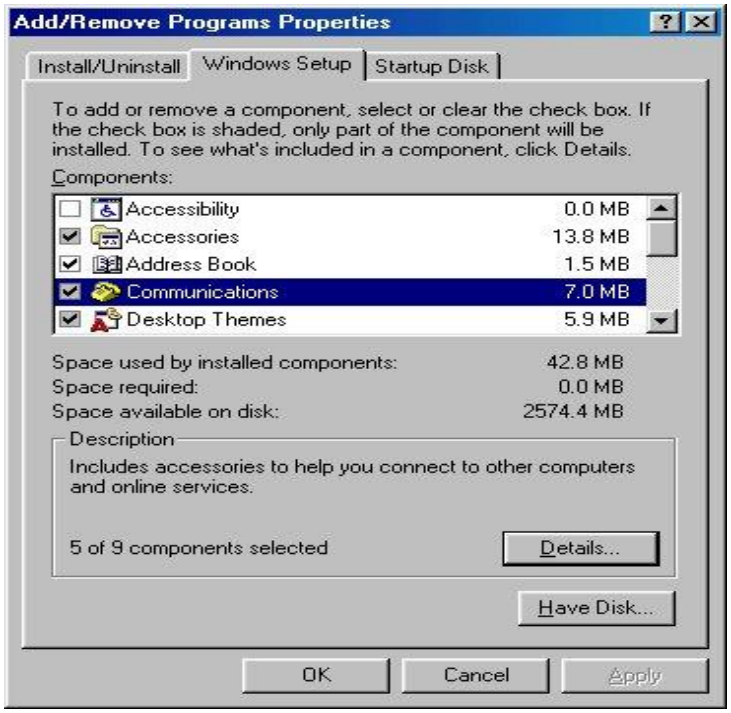
- **Enable:** Check to enable the router’s UPnP functionality.
- **Disable:** Check to disable the router’s UPnP functionality.

Example: Installing UPnP in Windows

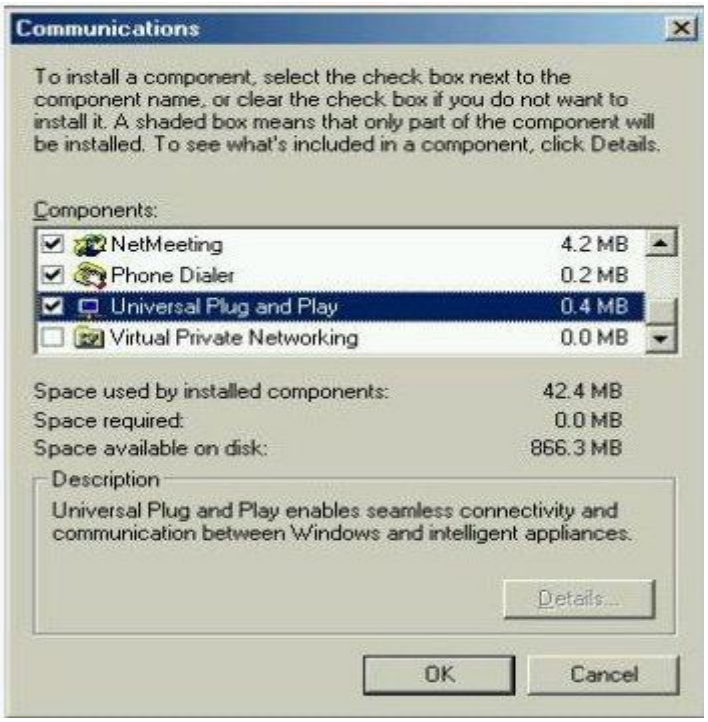
In Window ME.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

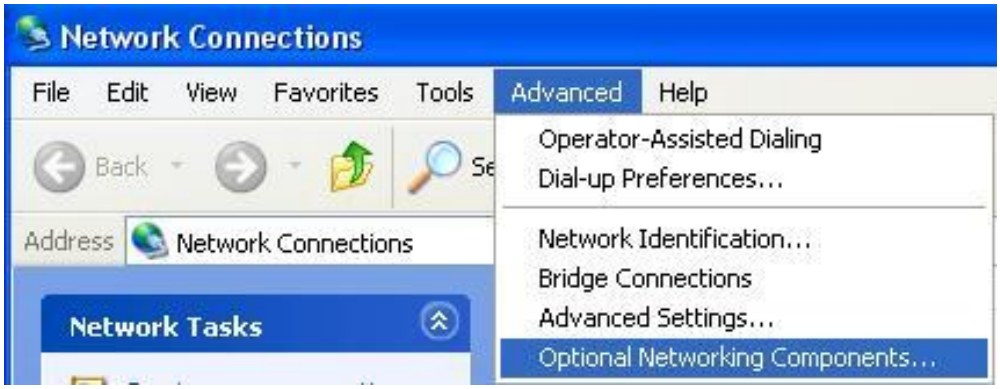
Step 5: Restart the computer when prompted.

In Window XP.

Step 1: Click Start and Control Panel.

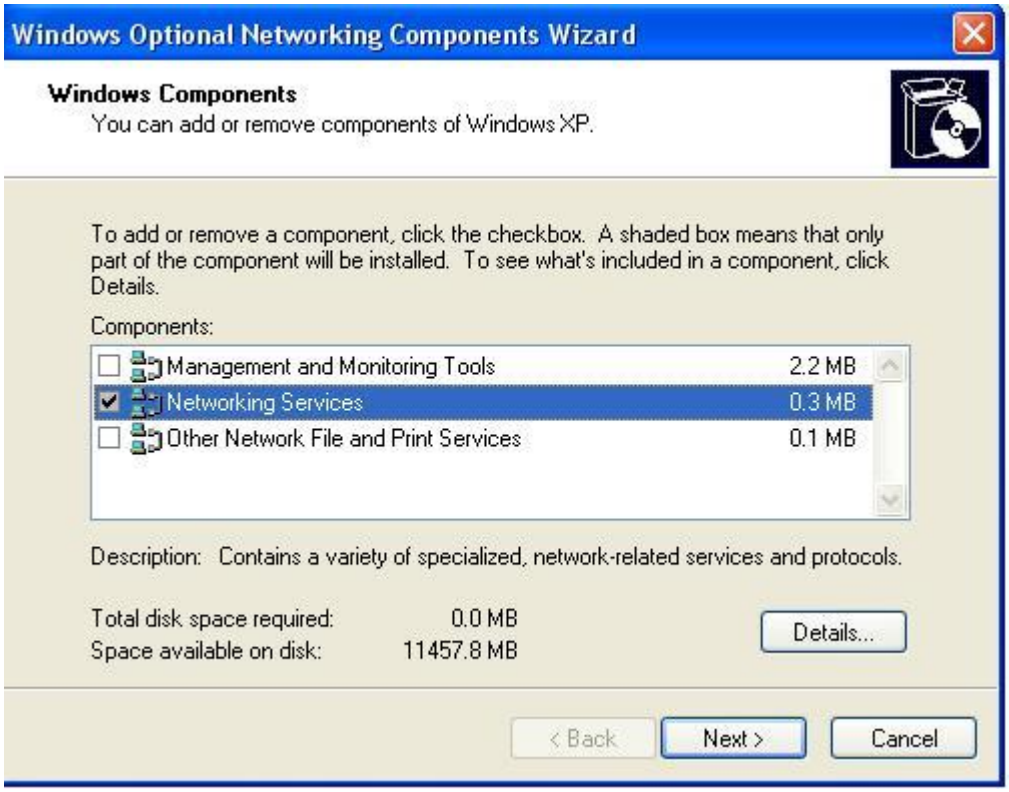
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….



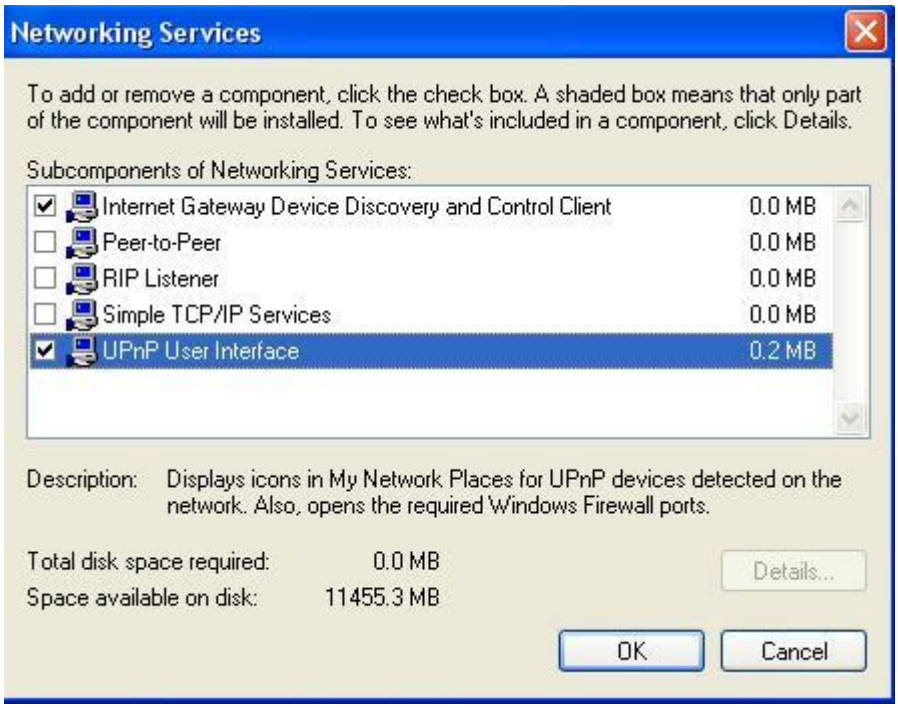
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



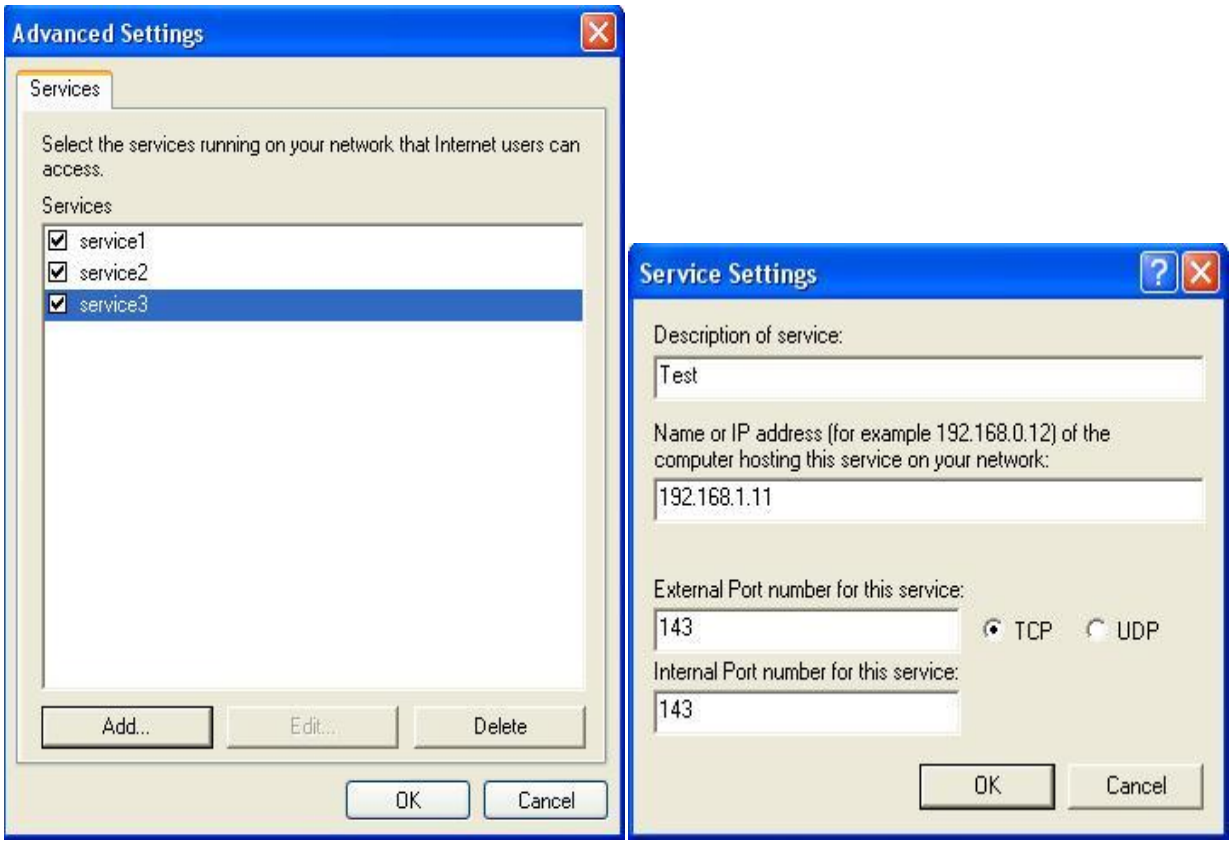
Auto-discover your UPnP-enabled network device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

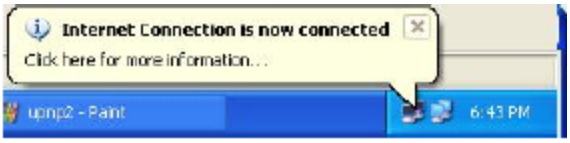
Step 2: Right-click the icon and select Properties.

Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

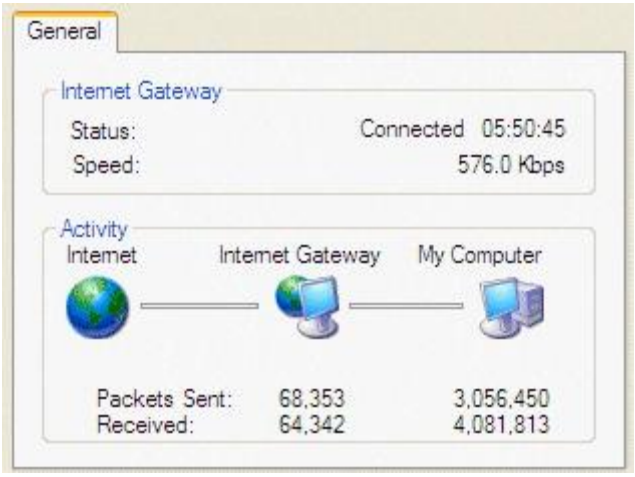
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



Web Configurator Easy Access

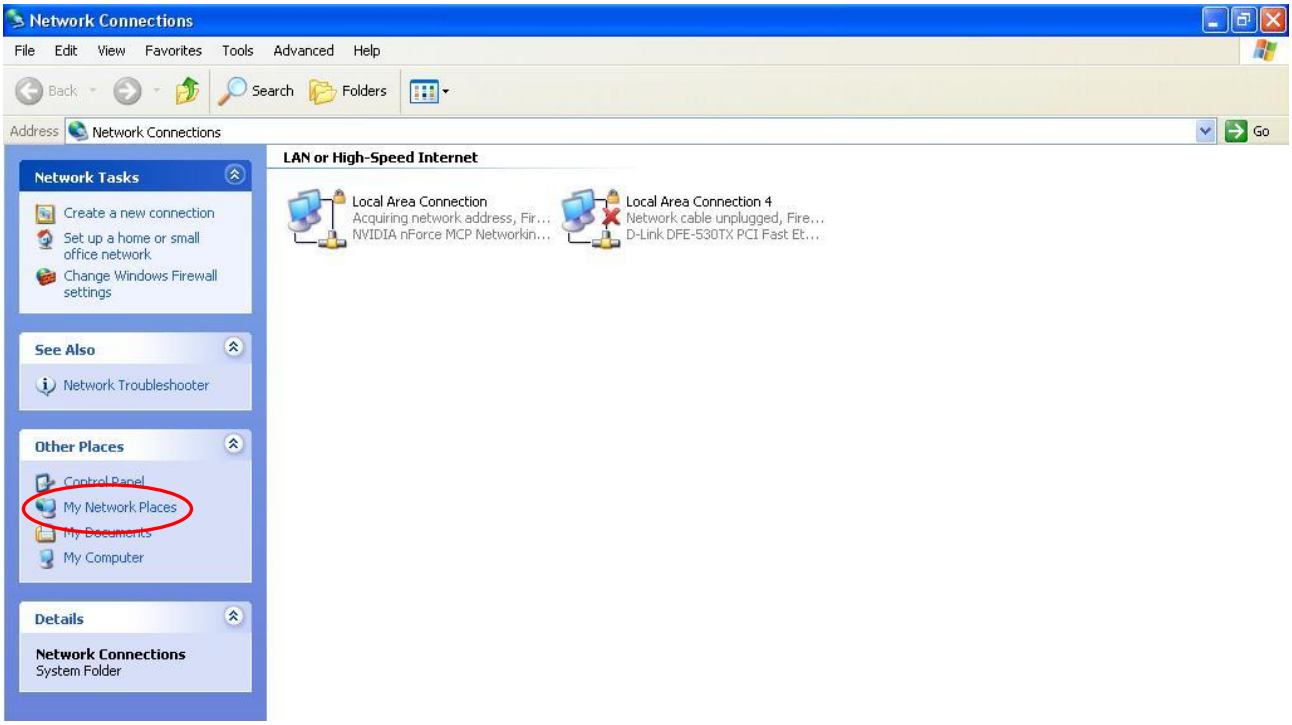
With UPnP, you can access web-based configuration for the BEC 8920AC without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BEC 8920AC and select Invoke. The web configuration login

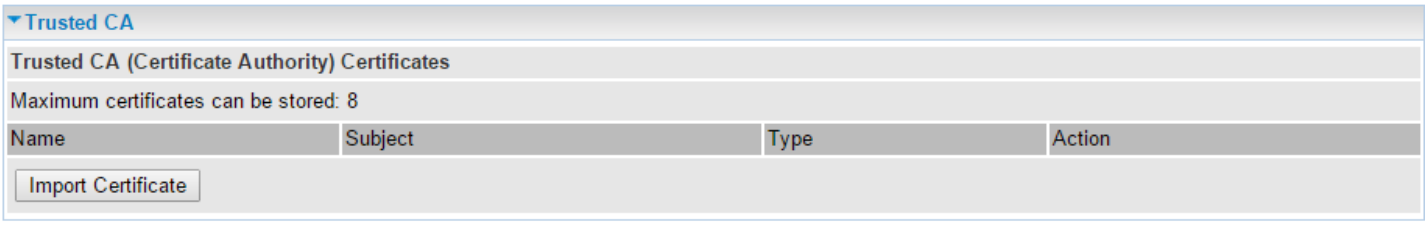
screen displays.

Step 6: Right-click on the icon of your BEC 8920AC and select Properties. A properties window displays basic information about the 8920AC.

Certificate

This feature is used for TR069 ACS Server authentication of the device using certificate, if necessary. If the imported certificate doesn't match the authorized certificate of the ACS Server, the device will have no access to the server.

Trusted CA



Name: The given name to identify this specific certificate.

Subject: The certificate subject.

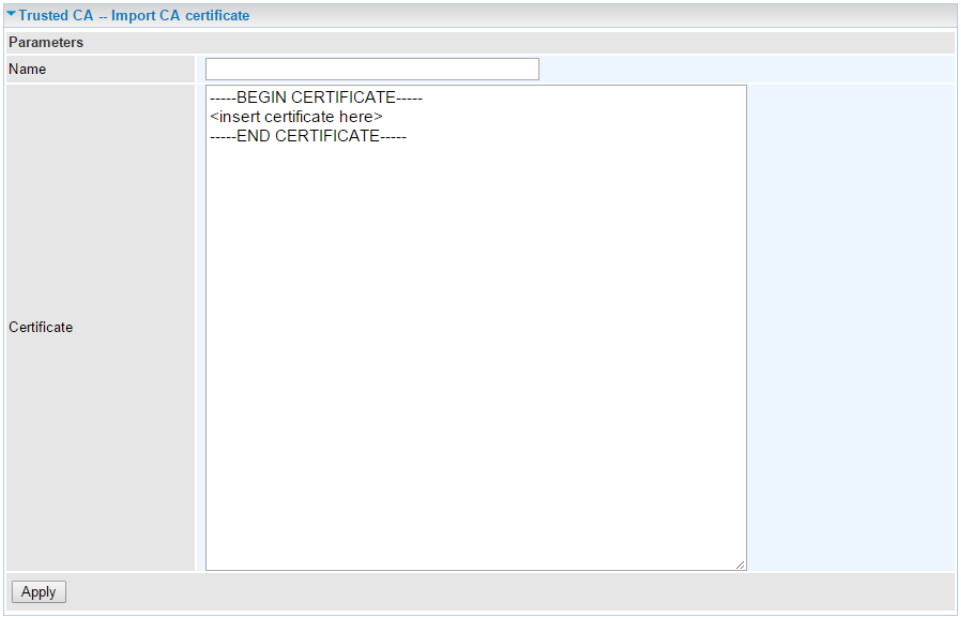
Type: The certificate type information.

- **ca**: Indicates that the certificate is a CA-signed certificate.
- **self**: Indicates that the certificate is a certificate owner signed one.
- **x.509:** Indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

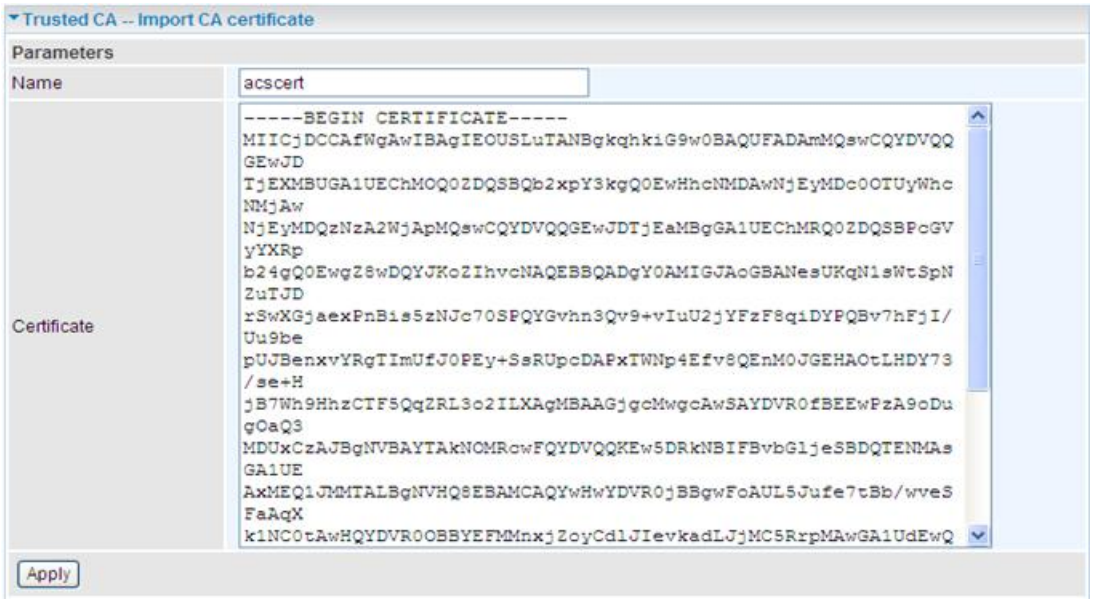
Action:

- View: view the certificate.
- Remove: remove the certificate.

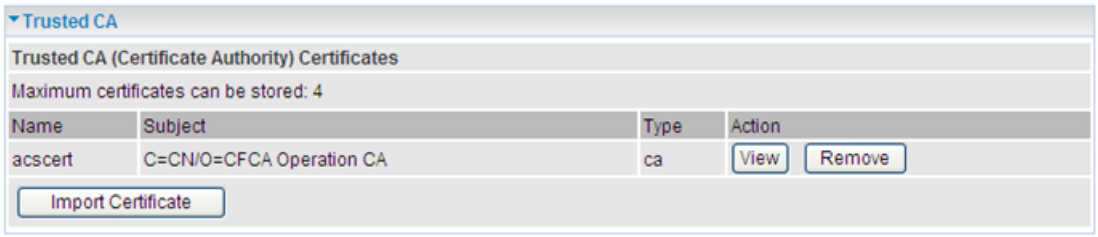
Click **Import Certificate** to import your certificate.



Enter the certificate name and insert the certificate.



Click **Apply** to confirm the settings.

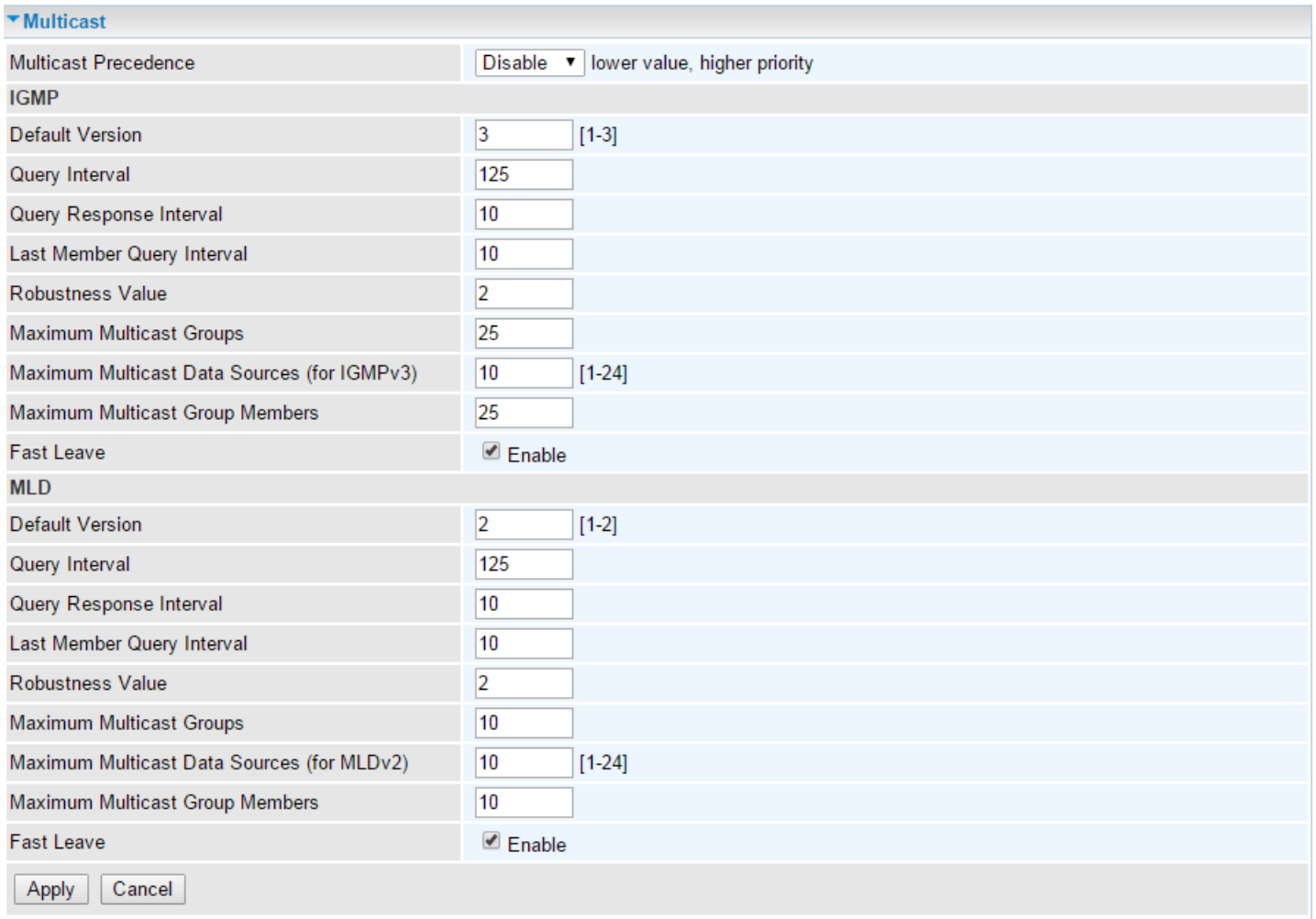


Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, and Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol,** it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, they are IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.



Multicast Precedence: It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

IGMP (for IPv4)

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v3.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, 2-7. Higher the value, the more robust the querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for IGMP v3): Enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

MLD (for IPv6)

Default Version: Enter the supported MLD version, 1-2, default is MLDv2.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for MLDv2): Enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

Management

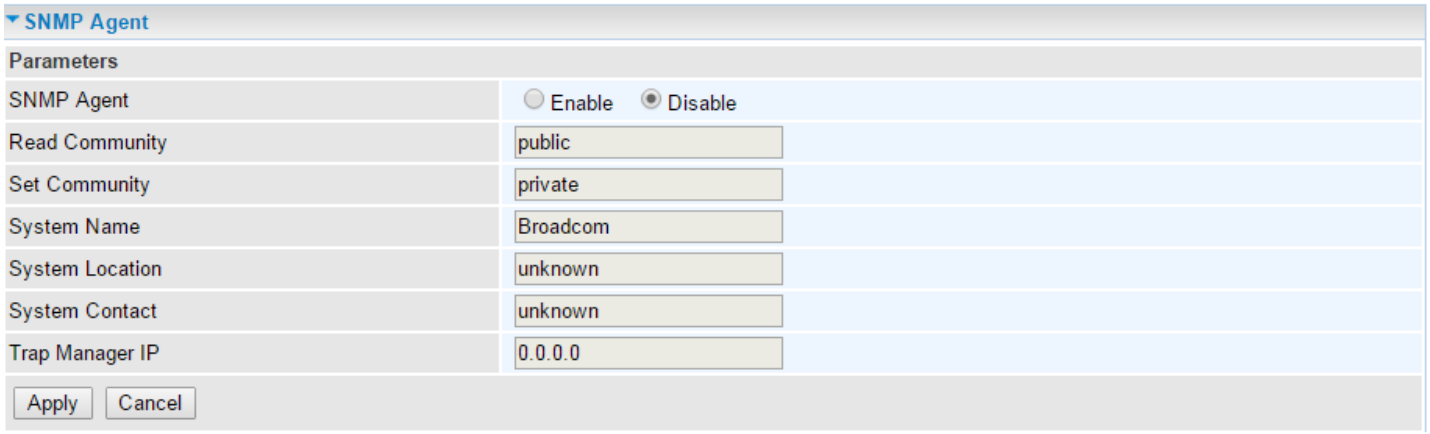
SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager，SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest、GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.



SNMP Agent: Enable to activate the SNMP Agent.

Read Community: Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

Set Community: Type the Set Community, which is the authentication for incoming Set requests from the management station.

System Name: here it refers to your router.

System Location: user-defined location.

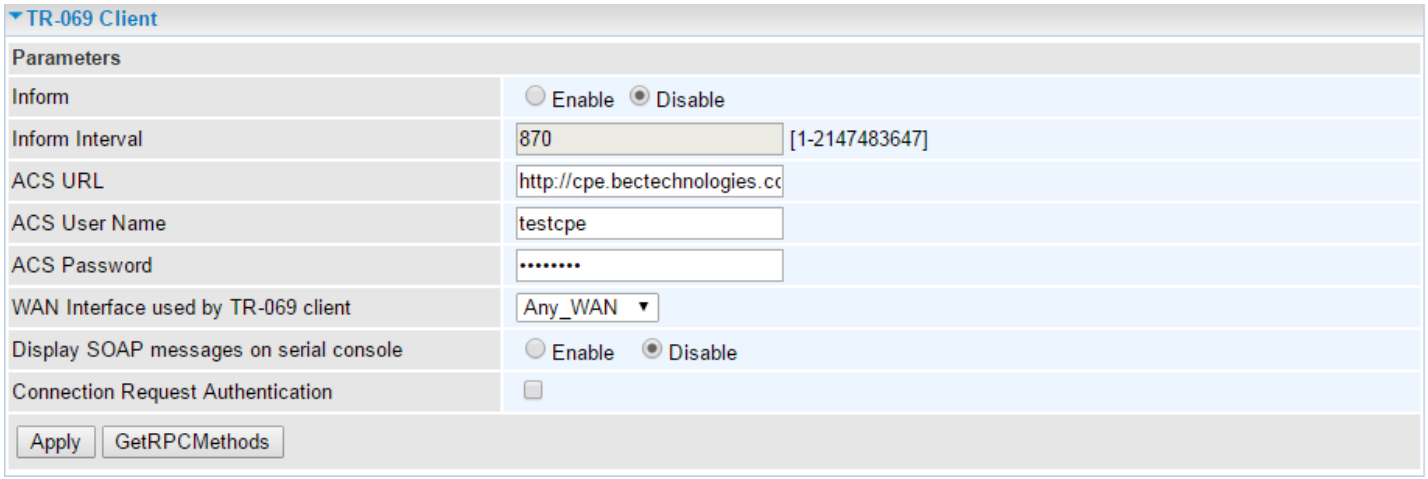
System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

TR- 069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Inform: Enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Inform Interval: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

ACS URL: Enter the ACS server login name.

ACS User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

ACS password: Enter the ACS server login password.

WAN interface used by TR-069: select the interface used by TR-069.

Display SOAP message on serial console: select whether to display SOAP message on serial console.

Connection Request Authentication: Check to enable connection request authentication feature.

Connection Request User Name: Enter the username for ACS server to make connection request.

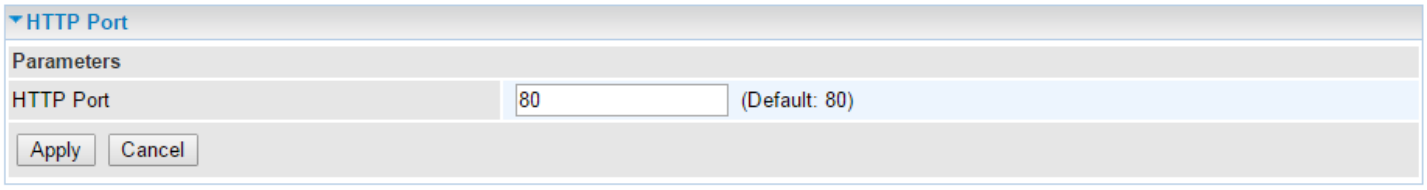
Connection Request User Password: Enter the password for ACS server to make connection request.

Connection Request URL: Automatically match the URL for ACS server to make connection request.

Click **Apply** to apply the settings.

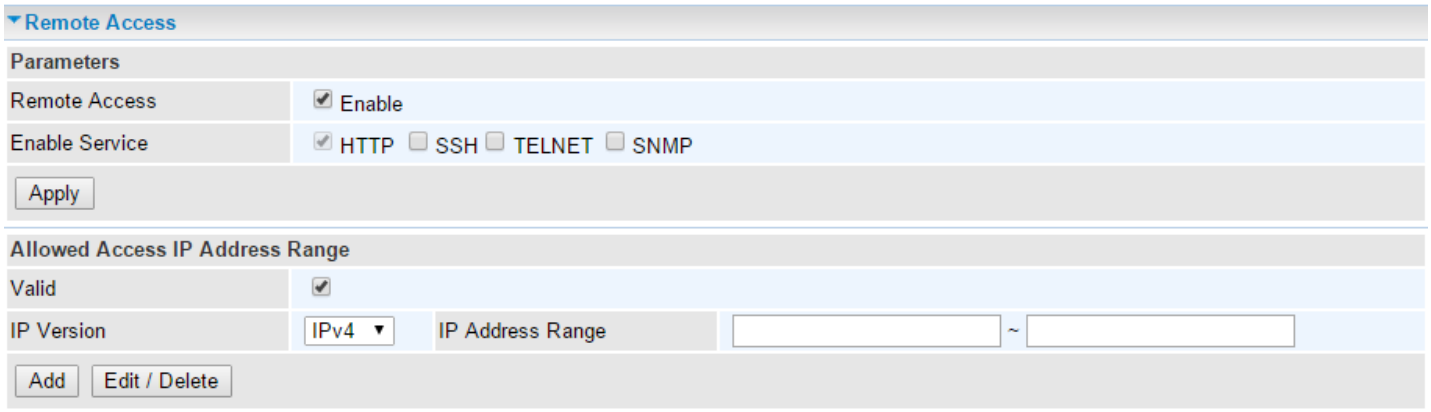
HTTP Port

Device management offers users a way to change the embedded web server accessing port, default 80. User can change the http port to 8080 or something else here.



Remote Access

It is to allow remote access to the router to view or configure.



Parameters

Remote Access: Select “Enable” to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

Enable Service: Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit the settings.

Allowed Access IP Address Range

Used to restrict IP address(es) to access to the system web GUI.

Valid: Enable/Disable Allowed Access IP Address Range

IP Version & IP Address Range: Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

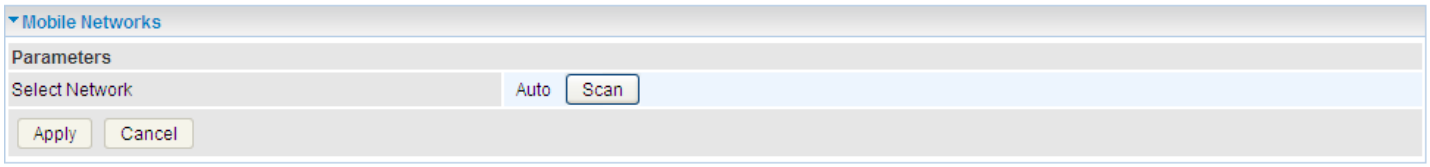
Click **Add** to add an IP Range to allow remote access.

Example: How to Enable the Remote Access

1. If user wants to grant remote access to IPs, first enable **Remote Access**.
2. **Remote Access enabled:**
   - Enable ***Valid*** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.
   - Disable ***Valid*** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.
   - No listing to prohibit remote access to the device.

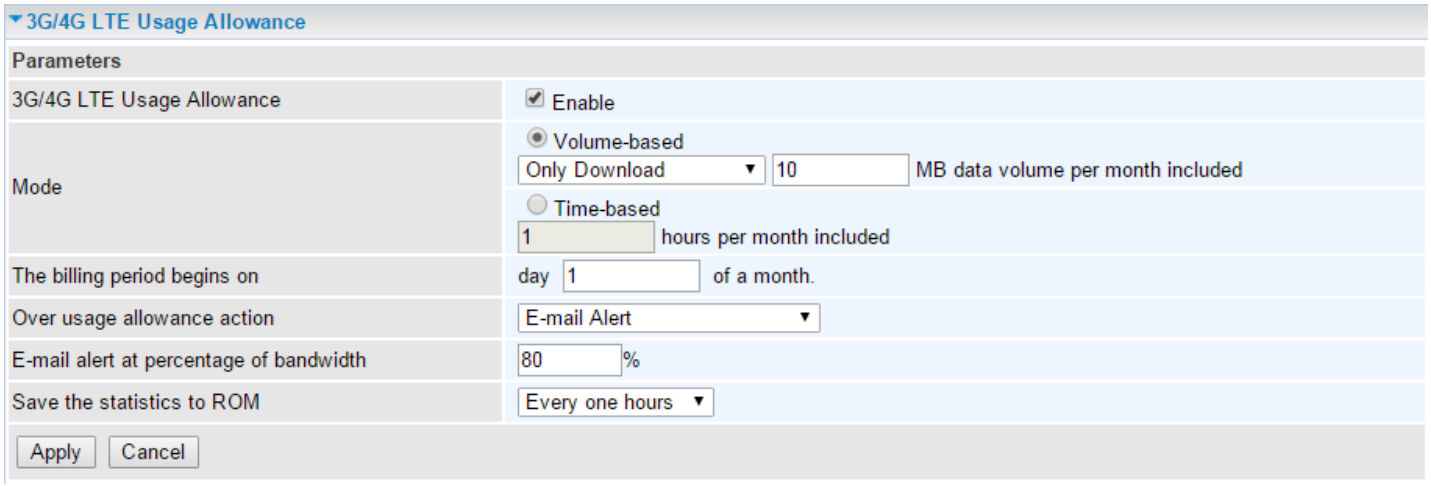
Mobile Network

Click **Scan** to discover available 3G/4G_LTE mobile network.



3G/4G LTE Usage Allowance

3G/4G LTE usage allowance is designated for users to monitor and control your 3G or 4G flow usage.



3G/4G LTE Usage Allowance: Enable to monitor 3G/4G LTE usage.

Mode: include Volume-based and Time-based control.

- **Volume-based** include “only Download”, ”only Upload” and “Download and Upload” to limit the flow.
- **Time-based** control the flow by providing specific hours per month.

The billing period begins on: The beginning day of billing each month.

Over usage allowance action: What to do when the flow is over usage allowance, the available methods are “E-mail Alert”, ”Email Alert and Disconnect” and “Disconnect”.

E-mail alert at percentage of bandwidth: When the used bandwidth exceeds the set proportion, the system will send email to alert.

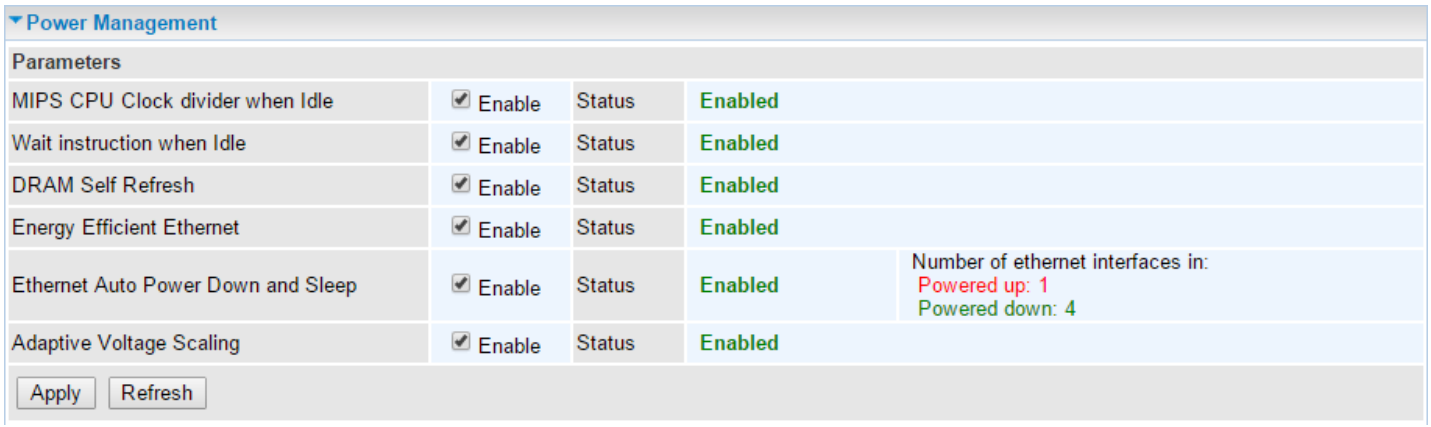
Save the statistics to ROM: To save the statistics to ROM system.

Click **Apply** to save the settings.

Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

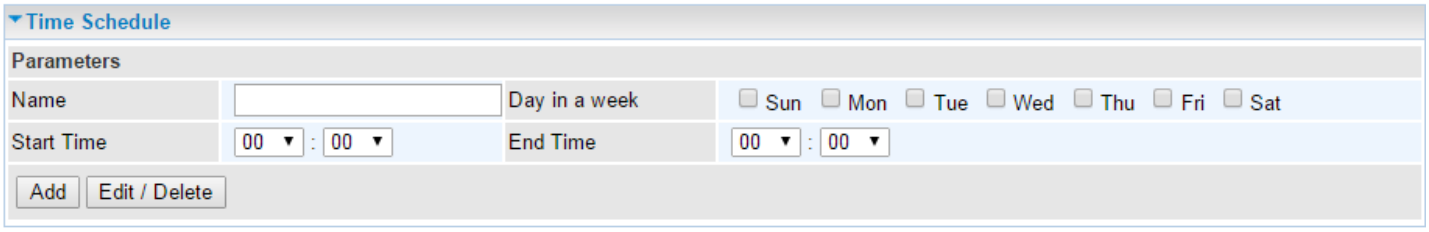
Five main parameters are listed for users to check to manage the performance of the router.



Time Schedule

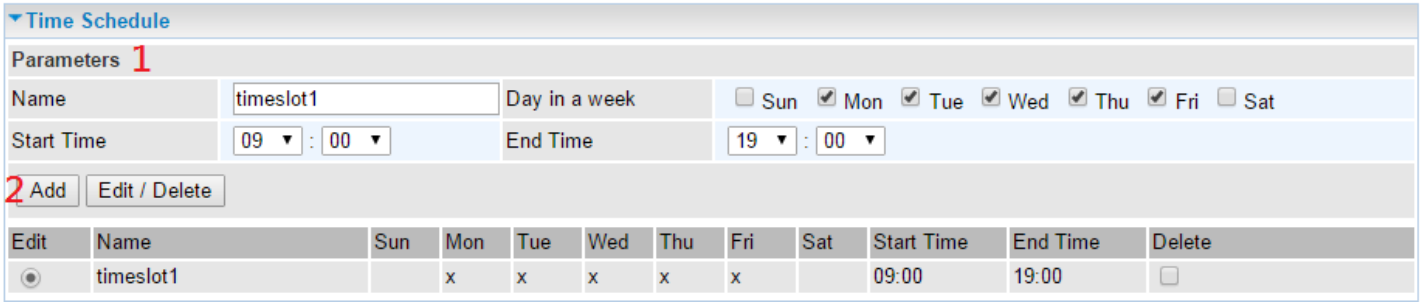
The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to Internet Time for details. You router time should synchronize with NTP server.

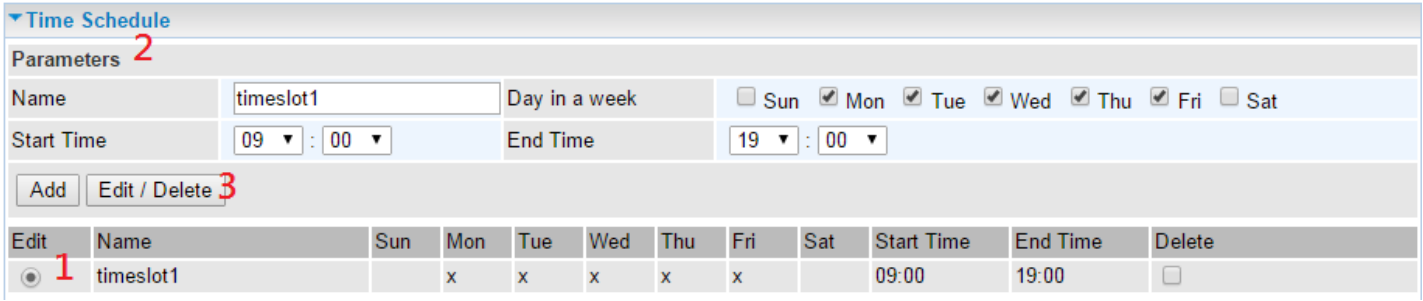


To add new entries: Add a timeslot named "timeslot1" features a period of 9:00-19:00 on every weekday (Monday thru Friday).

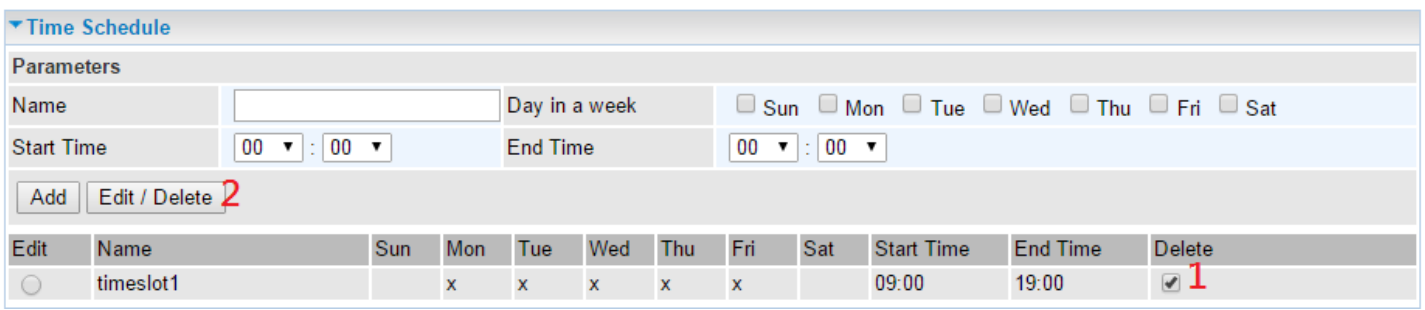
Click **Add** to add a rule



To make changes, click **Edit** button of a WAN entry to re-configure the settings.



To delete entries simply click **checkboxes** of the unwanted schedules then click **Delete** to remove entries.

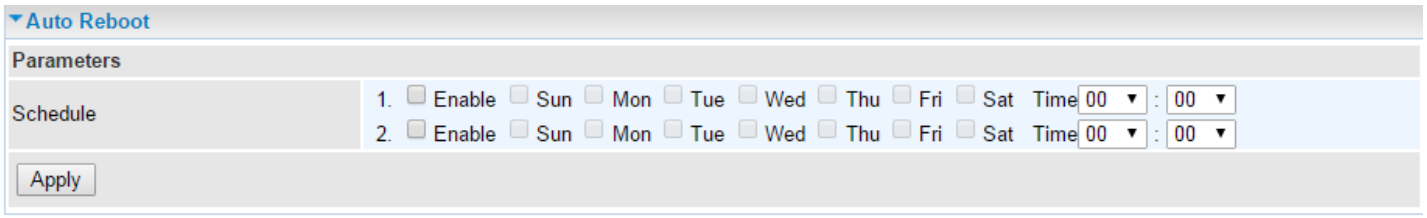


Auto Reboot

Schedule an automatic reboot for your 8920AC router to ensure proper operation and best performance.

This reboot will only reboot with current configuration settings and not overwrite any existing settings.

Click **Apply** to save the settings

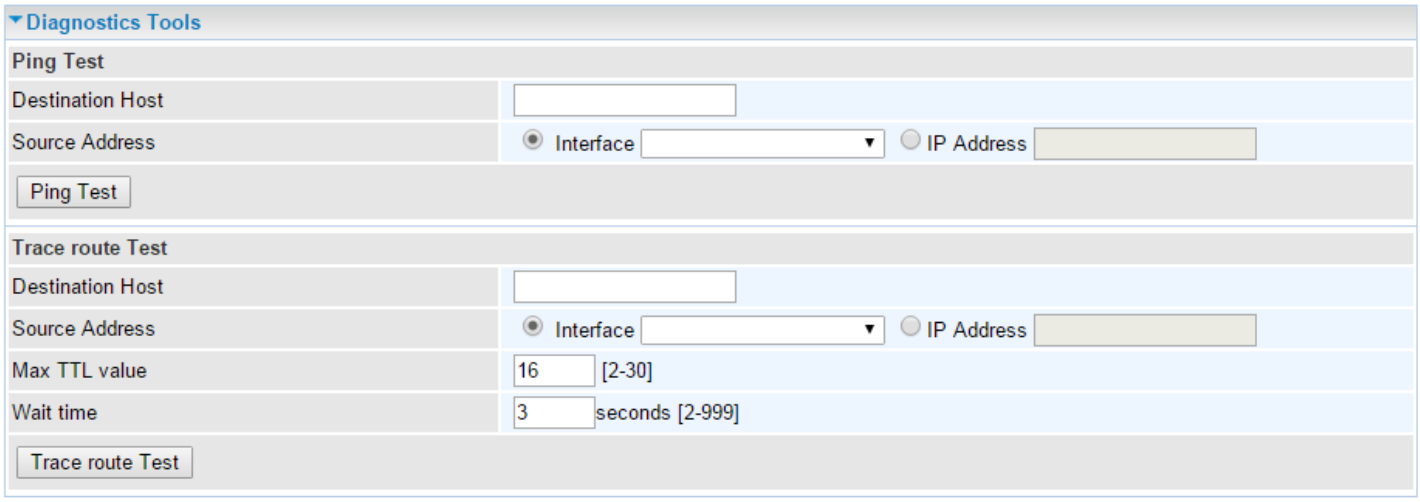


Example: Schedule 8920AC to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.

Diagnostics

Diagnostic Tools

BEC 8920AC offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.



Ping Test

Use to verify the connectivity between source and destination.

Destination Host: Enter the destination host (IP, domain name) to be checked for connectivity.

Source Address: Select a WAN interface or specify a source IP address to test the connectivity from the source to the destination.

Ping Test: Press this button to start the ping test.

Trace Route Test

Use to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

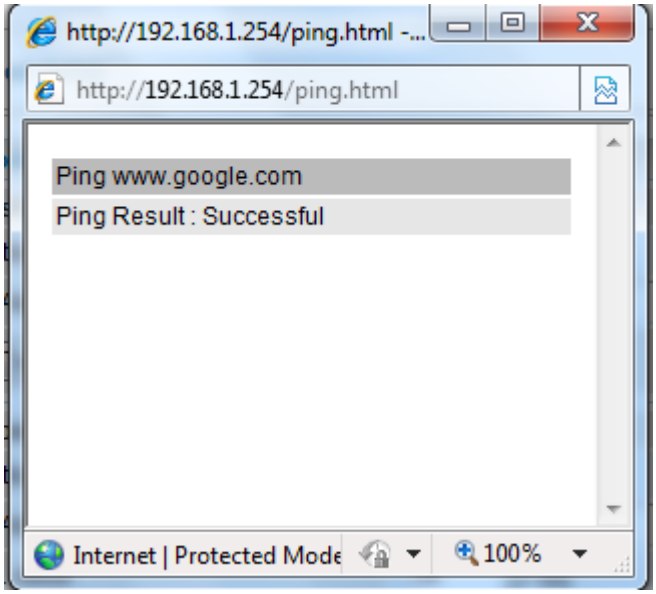
Destination Host: Set the destination host (IP, domain name) to be traced.

Source Address: Select a WAN interface or specify a source IP address to trace the route from the source to the destination.

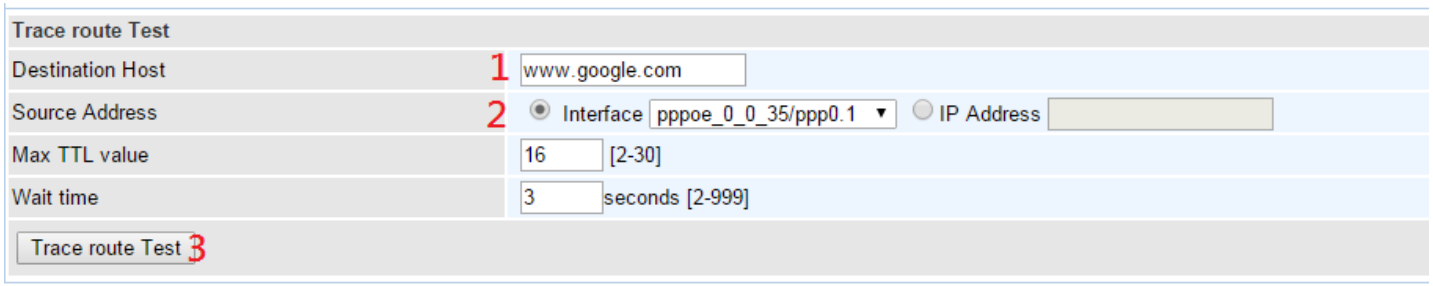
Max TTL value: Set the max Time to live (TTL) value.

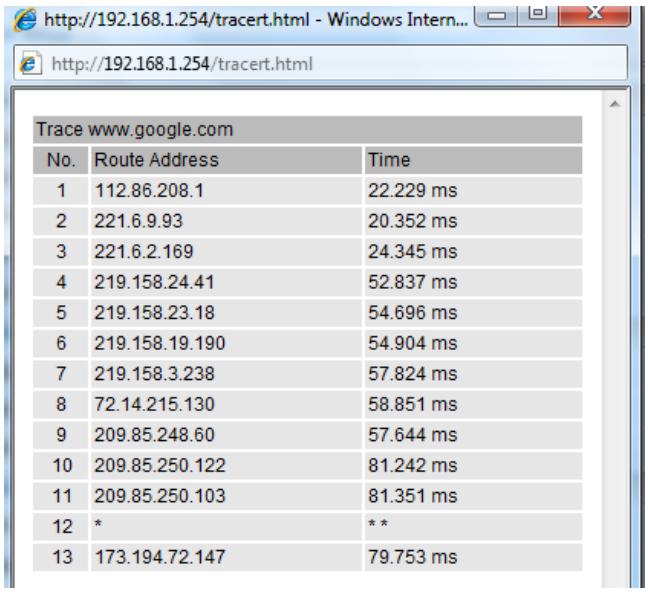
Wait time: Set waiting time for each response in seconds.

Example: Ping Test to www.google.com



Example: Trace route to www.google.com

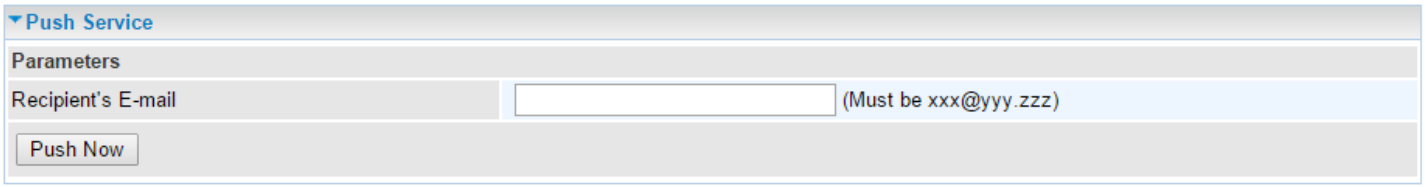




No.	Route Address	Time
1	112.86.208.1	22.229 ms
2	221.6.9.93	20.352 ms
3	221.6.2.169	24.345 ms
4	219.158.24.41	52.837 ms
5	219.158.23.18	54.696 ms
6	219.158.19.190	54.904 ms
7	219.158.3.238	57.824 ms
8	72.14.215.130	58.851 ms
9	209.85.248.60	57.644 ms
10	209.85.250.122	81.242 ms
11	209.85.250.103	81.351 ms
12	*	* *
13	173.194.72.147	79.753 ms

Push Service

With push service, the system can send email messages with consumption data and system information.



Recipient's E-mail: Enter an e-mail address. Click **Push Now** to send **system log, system configuration**, and **security log** to this e-mail address.

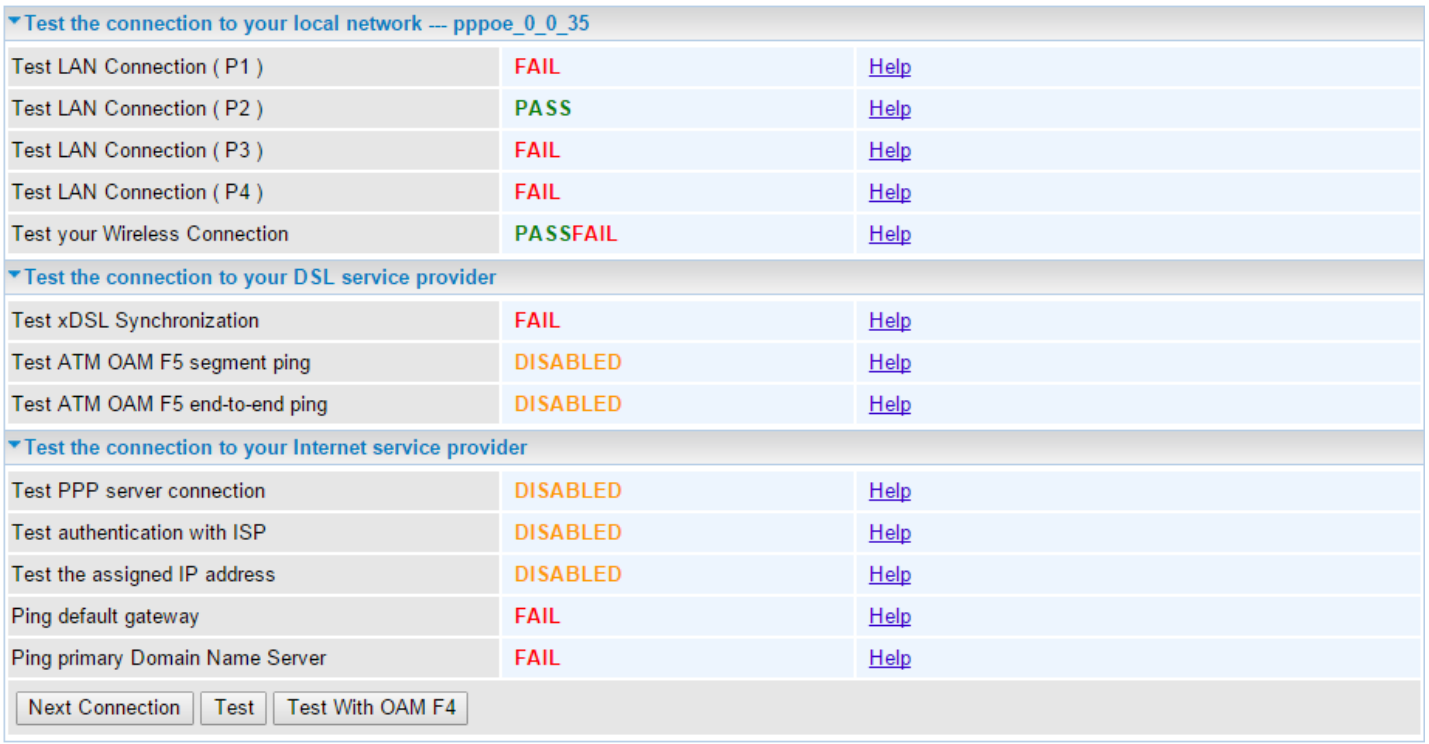
Note: This e-mail address is used for one-time only. To receive logs again, please reenter your e-mail address again.

Note: Make sure you have configured the SMTP server parameter correctly in Mail Alert section.

Diagnostics

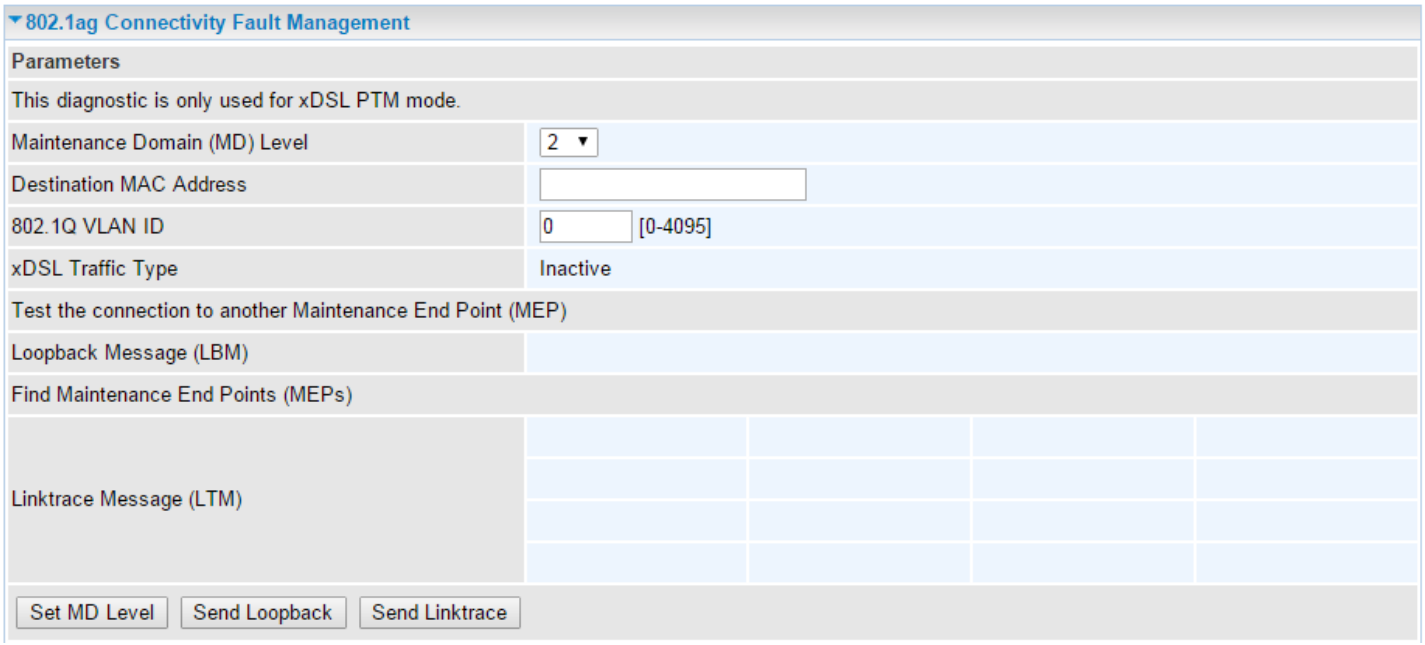
Check the connections, including Ethernet connection, Internet Connection and wireless connection.

Click **Help** link that can lead you to the interpretation of the results and the possible, simply troubleshooting.



Fault Management

IEEE 802.1ag Connectivity Fault Management (CFM) is a standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Fault Management is to uniquely test the VDSL PTM connection; Push service



Maintenance Domain (MD) Level: Maintenance Domains (MDs) are management spaces on a network, typically owned and operated by a single entity. MDs are configured with Names and Levels, where the eight levels range from 0 to 7. A hierarchal relationship exists between domains based on levels, larger the domain higher the level value.

Destination MAC Address: Specify a MAC of the target device for the system to perform a CFM loop test. Click **Send Loopback** or Send **Linktrace** to begin the test.

802.1Q VLAN ID: Specify a VLAN ID

xDSL Traffic Type: Display current activate xDSL (ADSL / VDSL) mode

Loopback Message (LBM): Display details on how many loopback messages are sent and if Loop Back Response (LBR) received from a remote Maintenance End Point (MEP)

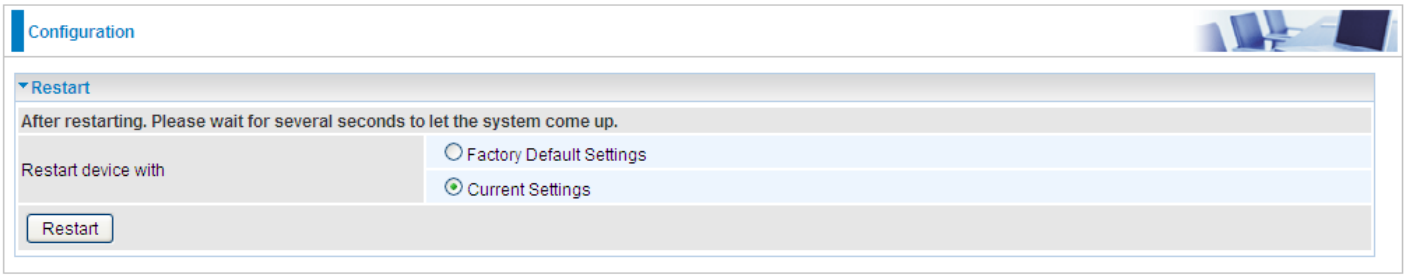
Find Maintenance End Point: Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

Send Loop-back: Loop-back messages otherwise known as MAC ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loopback to successive MIPs can determine the location of a fault. Sending a high volume of Loopback Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loopback to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

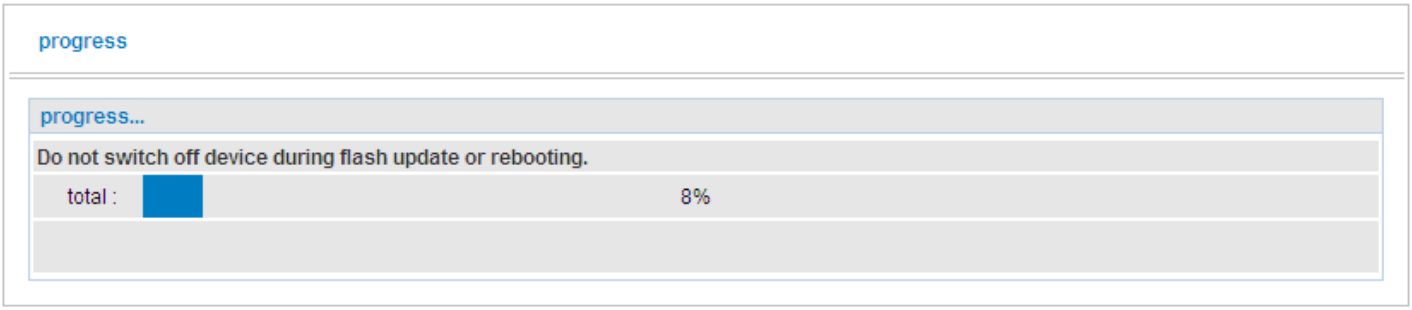
Send Link Trace: Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

Restart

This section lets you restart your router if necessary. Click Restart in the low right corner of each configuration page.



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.



CHAPTER 6: TROUBLESHOOTING

If your Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Problem with WAN Interface

Problem	Suggested Action
Frequent loss of ADSL/VDSL line sync (disconnections)	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your xDSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems please contact the dealer from where you purchased your product.

Contact BEC @ http://www.bectechnologies.net

Windows 7/98, Windows NT, Windows 2000, Windows ME, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

V250adl11