BiPAC 7800(N)

(802.11n) Dual WAN
ADSL2+ Firewall Router

User Manual

Version released: 1.06f

Last revised on Dec 27 2011

Table of Contents

Chapter 1: Introduction

Introduction to your Router

Thank you for purchasing BiPAC 7800(N) Router. Your new router is an all-in-one unit that combines an ADSL modem, ADSL2/2+ router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

BiPAC 7800(N) router complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

BiPAC 7800(N) supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with your ISP. Your new router also supports VC-based and LLC-based multiplexing.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, BiPAC 7800(N) allows multiple users to have high-speed Internet access simultaneously.

Your new router also serves as an Internet firewall, protecting your network from access by outside users. Not only does it provide a natural firewall function with Network Address Translation (NAT), it also provides rich firewall features to secure your network. All incoming data packets are monitored and filtered. You can also configure your new router to block internal users from accessing the Internet.

BiPAC 7800(N) provides two levels of security support. First, it masks LAN IP addresses making them invisible to outside users on the Internet, so it is much more difficult for a hacker to target a machine on your network. Second, it can block and redirect certain ports to limit the services that outside users can access. To ensure that games and other Internet applications run properly, you can open specific ports for outside users to access internal services on your network.

The Integrated DHCP (Dynamic Host Control Protocol) client and server services allow multiple users to get IP addresses automatically when the router boots up. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from the DHCP server and reboot. Each time a local machine is powered up; the router recognizes it and assigns an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service (port mapping) functions allow the product to provide limited visibility to local machines with specific services for outside users. For instance, a dedicated web server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

Virtual Server can also be used to re-task services to multiple servers. For instance, you can set the router to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

Features

Express Internet Access

The router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis. plus (ITU G.992.5)).

EWAN

BiPAC 7800(N) EWAN port provides user an alternative means to connect to Cable Modems, VDSL, fiber optic lines and PON besides using ADSL for internet connection. If one uses ADSL to connect to the internet, EWAN can act as the 5th Ethernet port of the LAN. This alternative provides users with more flexibility & a faster way to get online.

IPv6 Supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4.

IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2128 (about 3.4×1038) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).

Fast Ethernet Switch

A 4-port 1000Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X. An Ethernet straight or crossover cable can be used directly for auto detection.

Multi-Protocol to Establish a Connection

It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

PPP over Ethernet (PPPoE)

BiPAC 7800(N) provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer.

Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

Network Address Translation (NAT)

Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like **http://www.dyndns.org/**. More than 5 DDNS servers are supported.

Virtual Server

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from the Internet and vice versa, in addition to providing a higher level of security control.

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and

distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

802.11n Wireless AP with WPA Support

With an integrated 802.11n Wireless Access Point in the router, the device delivers up to 6 times faster speeds and 3 times farther range than an 802.11b/g wireless network. It supports a fast data transfer rate up to 300Mbps and is fully compatible with 802.11b/11g equipments. The supported features of Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) enhance the security level of data protection and access control via Wireless LAN. The router also supports Wi-Fi Protected Setup (WPS) that features the establishment of a secured wireless network. The built-in Wireless Distribution System (WDS) also facilitates the flexibility for wireless network expansion without the need for any external wires or cables.

Web based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Hardware Specifications

Physical Interface

- WLAN: 3 x 2 dbi detachable antennae (BiPAC 7800NA only)
- DSL: ADSL port
- EWAN: RJ-45 Ethernet port for connecting to ADSL / Cable / FTTH / VDSL device
- Ethernet: 4-port 10/100/1000M auto-crossover (MDI / MDI-X) Switch
- Factory default reset button
- WPS push button (BiPAC 7800NA only)
- Power jack
- Power switch

Chapter 2: Installing the Router

Package Contents

BiPAC 7800(N) (802.11n) Dual WAN ADSL2+ Firewall Router

CD containing the online manual

RJ-11 ADSL/Telephone cable

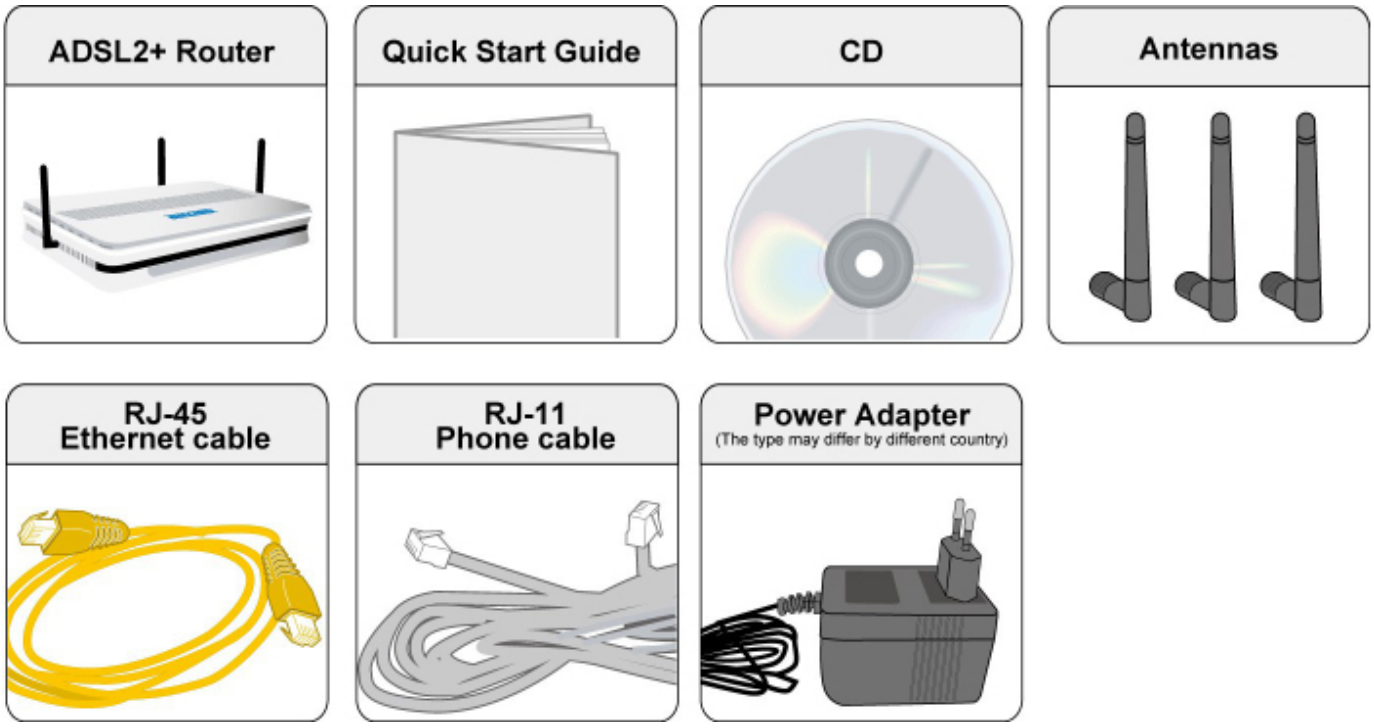
Ethernet (RJ-45) cable

Three 2dBi detachable antennas (Wireless model only)

Power adapter

Quick Start Guide

Splitter / Microfilter (Optional)



Important note for using this router

Warning

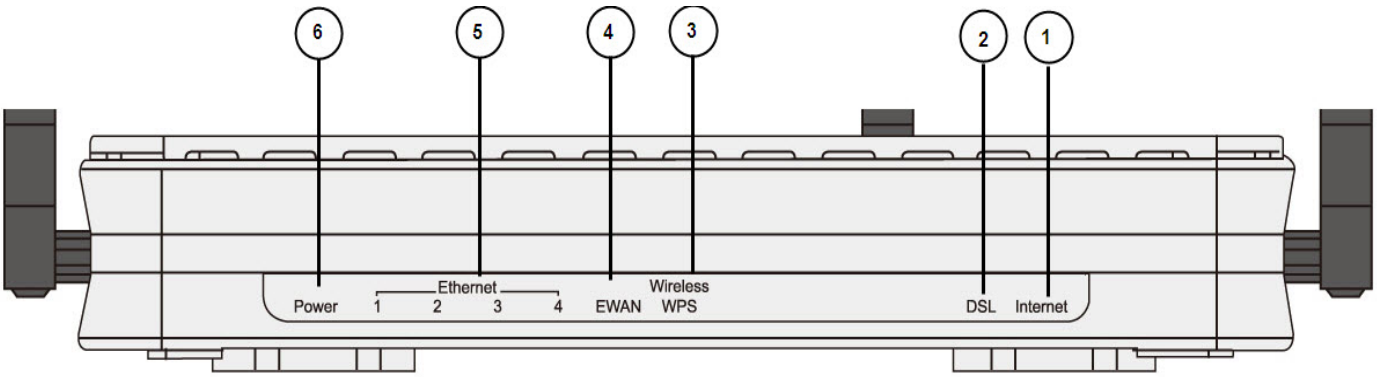
- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this 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.

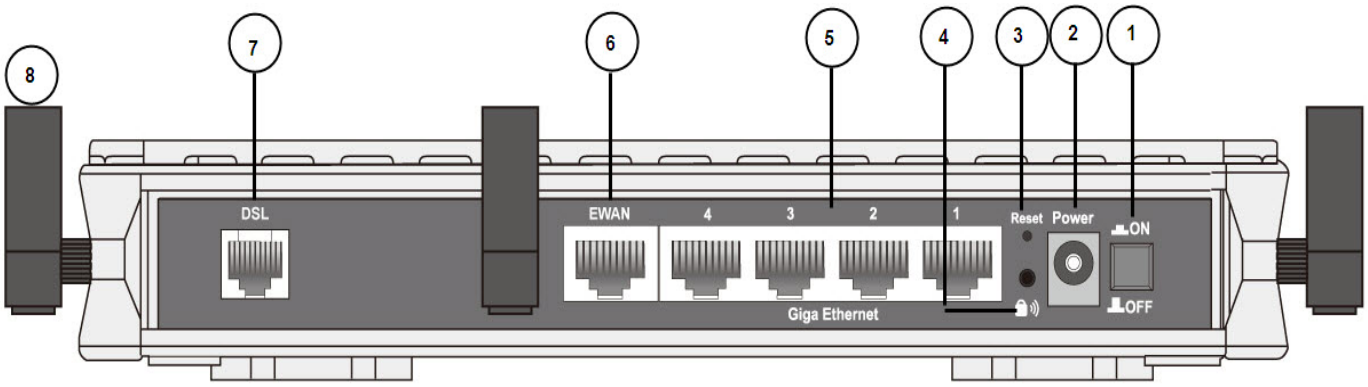
Device Description

The Front LEDs



LED		Meaning
1	**Internet**	Lit orange when WAN port fails to get IP address. Lit green when WAN port gets IP address. Lit off when device in bridged mode or ADSL connection not present.
2	**DSL**	Lit Green when the device is successfully connected to an ADSL DSLAM. (“line sync”).
3	**Wireless / WPS (only available for BiPAC 7800N)**	Lit green when a wireless connection is established. Flash orange when WPS configuration is in progress. However, if WPS fails the LED will only lit for 1 min before goes off. Flash green when data is sent / received.
4	**EWAN**	Lit orange when connected to a broadband connection device. Lit orange for 10/100Mbps. Blinking when data is Transmitted / Received.
5	**Ethernet port 1X - 4X (RJ-45 connector)**	Lit orange when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission hits 1000Mbps; Lit orange when the speed of transmission hits 10/100Mbps. Blink when data is being Transmitted / Received.
6	**Power**	When the device is booting, the green light will lit while the orange light will flash. When the system is ready, it will lit green. Lit orange when the device fails to boot or when the device is in emergency mode.

The Rear Ports



Port		Meaning
1	**Power Switch**	Power ON/OFF switch.
2	**Power**	Connect it with the supplied power adapter.
3	**RESET**	Press more than 5 seconds to restore the device to its default mode.
4	**WPS** **(only for BiPAC 7800N)**	By controlling the pressing time, users can achieve two different effects: (1)**WPS:** Press less than 5 seconds until WPS LED flashes orange to trigger WPS function. But if WPS service is disabled, this short time press does nothing. (2) **Wireless ON/OFF button:** Press over 5 seconds to switch on wireless function and the Wireless/WPS LED will lit green. Press over 5 seconds again to disable wireless function and the Wireless/WPS LED is off.
5	**Giga Ethernet**	Connect to a PC or an office/home network of 10Mbps, 100Mbps or 1000Mbps using the provided RJ-45 Ethernet cables.
6	**EWAN**	WAN 10/100Mbps Ethernet port (with auto crossover support). Connect to Cable Modem, VDSL, Fiber Modem or PON optic lines with your RJ-45 cable.
7	**DSL**	Connect this port to the ADSL/telephone network with the RJ-11 cable (telephone) provided.
8	**Antenna** **(BiPAC 7800N only)**	Connect the detachable antenna to this port.

The detail instruction in Reset Button

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):
Hold the Reset Button on the back of the modem in. Keep this button held in and turn on the modem. Once power LED lits orange, release the Reset Button. The modem's emergency-reflash web interface will then be accessible via http://192.168.1.254 where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

Before powering on the router to enter the recovery process, please configure the IP address of the PC as 192.168.1.100 and proceed with the following step by step guide.

1. Power the router off.
2. Hold the "Reset Button".
3. Power on the router. Then Router's IP will reset to Emergency IP address (Say 192.168.1.254)
4. Download the firmware.

Cabling

One of the most common causes of problems is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify if you are using the proper cables.

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your ADSL connection or may result in frequent disconnections.

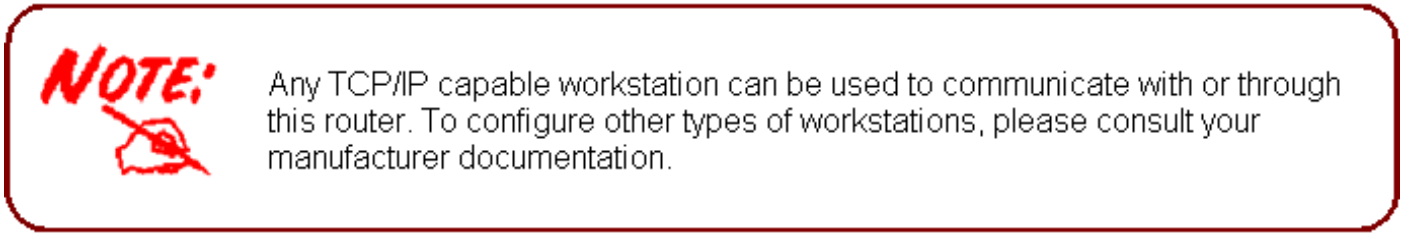
Chapter 3: Basic Installation

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

Please check your PC 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.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs 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 problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

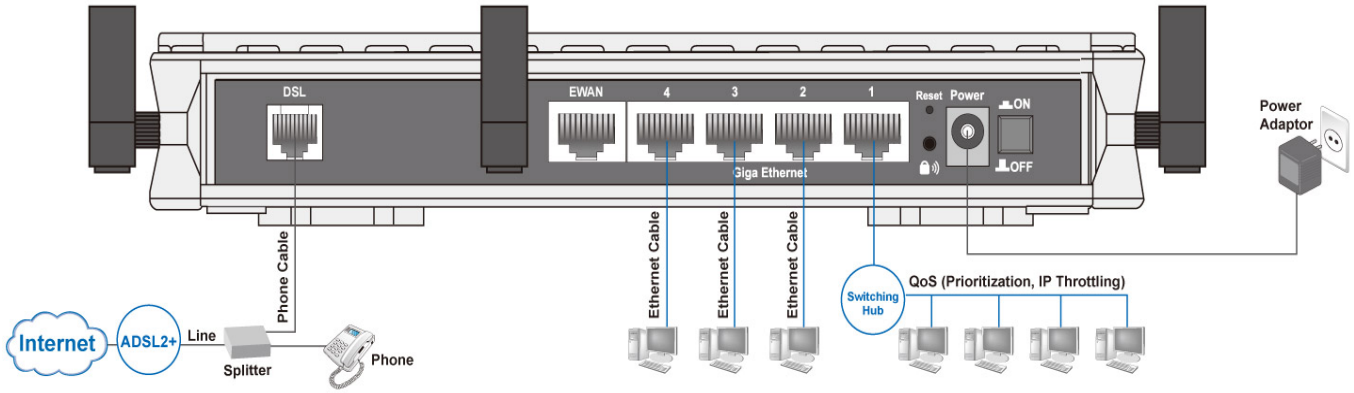
Please follow the following steps to configure your PC network environment.



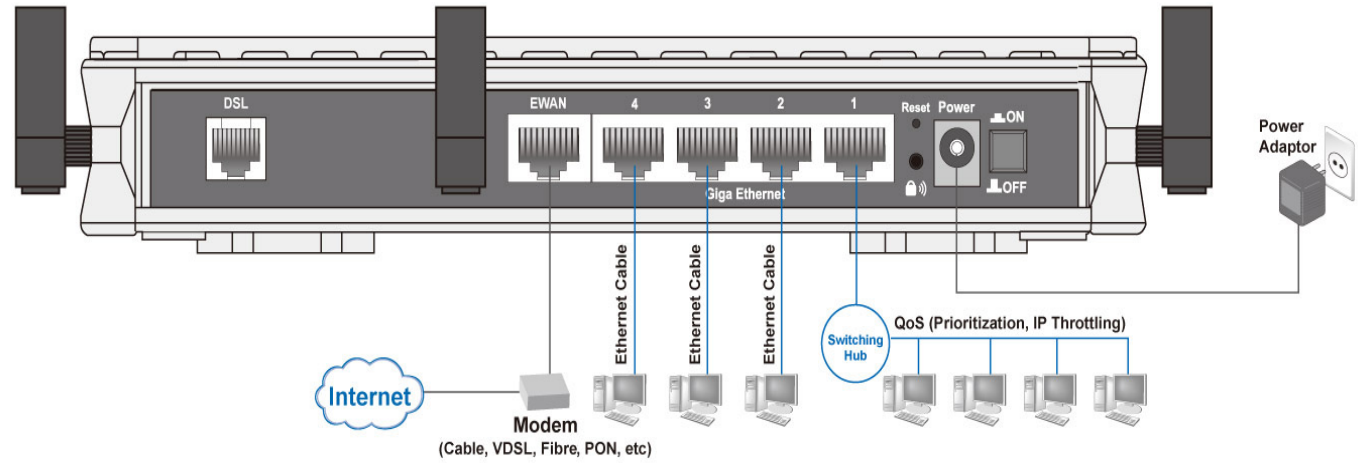
Connecting Your Router

Users will not be able to connect to the internet through EWAN if DSL is already connected to the internet. Only one connection type (EWAN or DSL) is allowed to connect to the internet at one time.

ADSL Router Mode



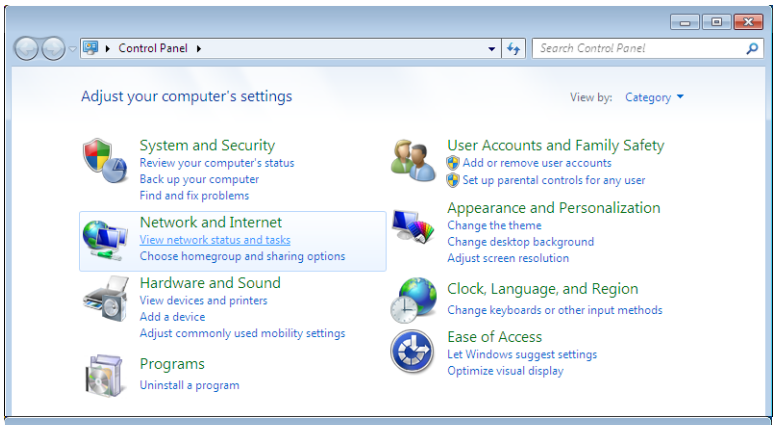
Broadband Router Mode



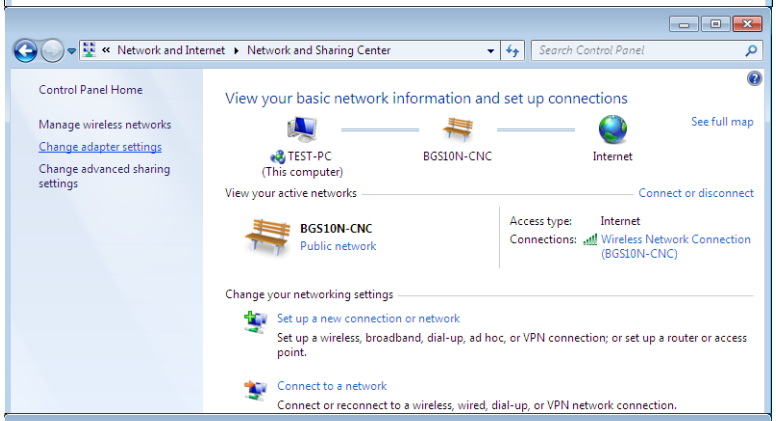
Network Configuration

Configuring PC in Windows 7

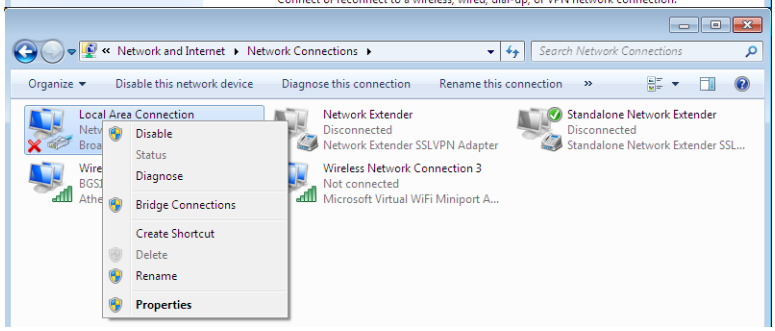
1. Go to Start. Click on Control Panel.
2. Then click on Network and Internet.



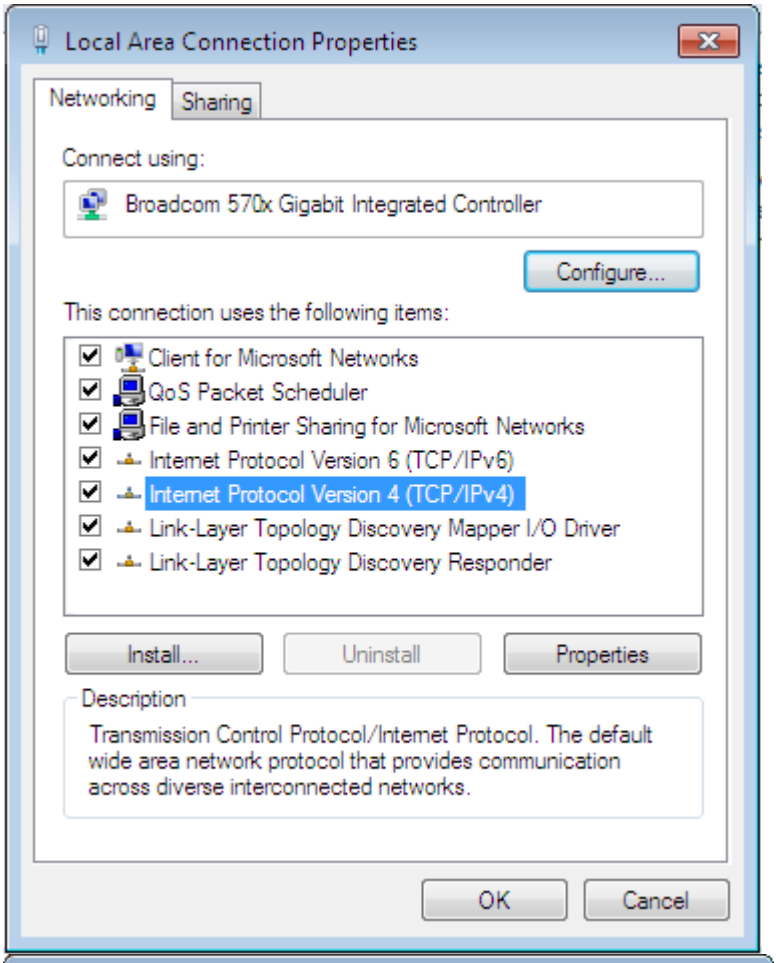
3. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.



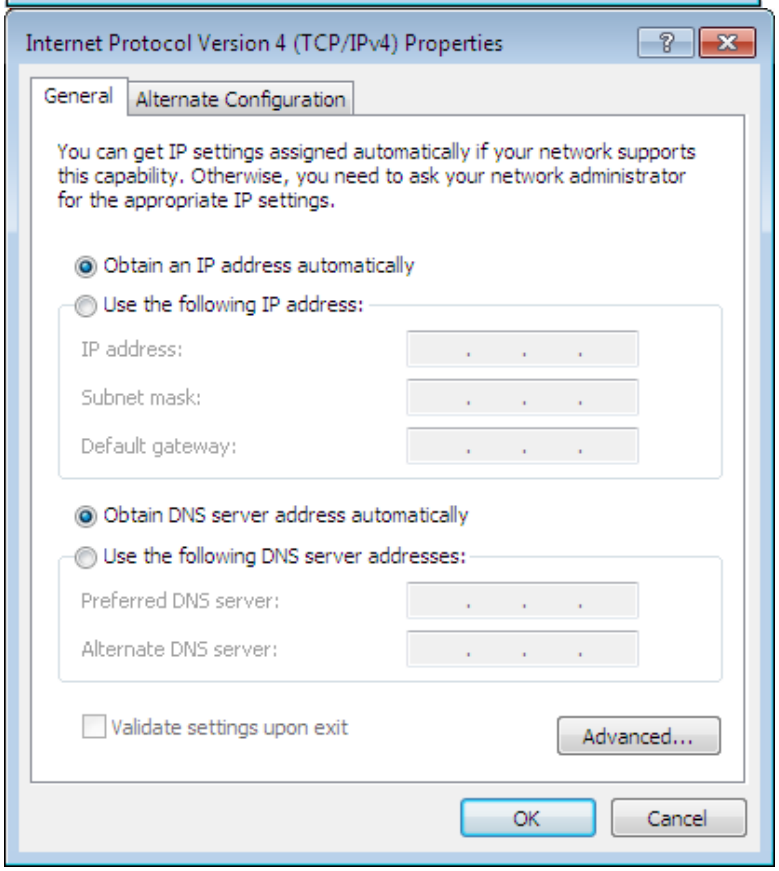
4. Select the Local Area Connection, and right click the icon to select Properties.



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

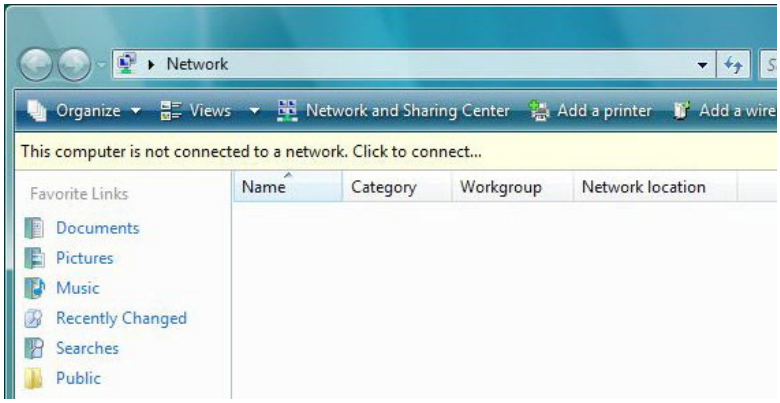


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

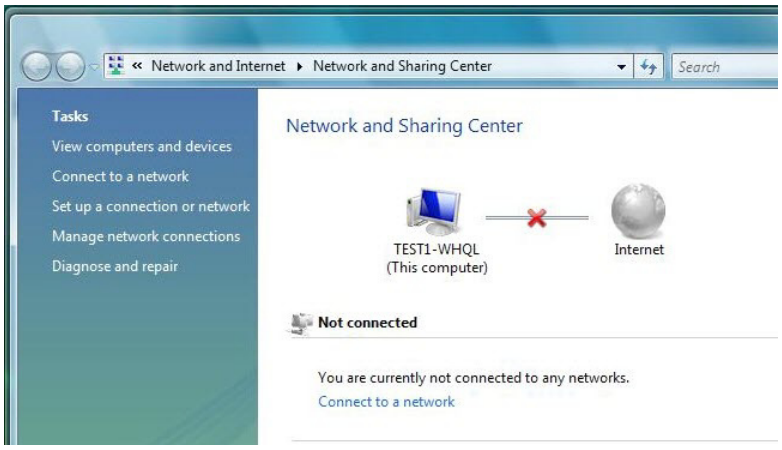


Configuring PC in Windows Vista

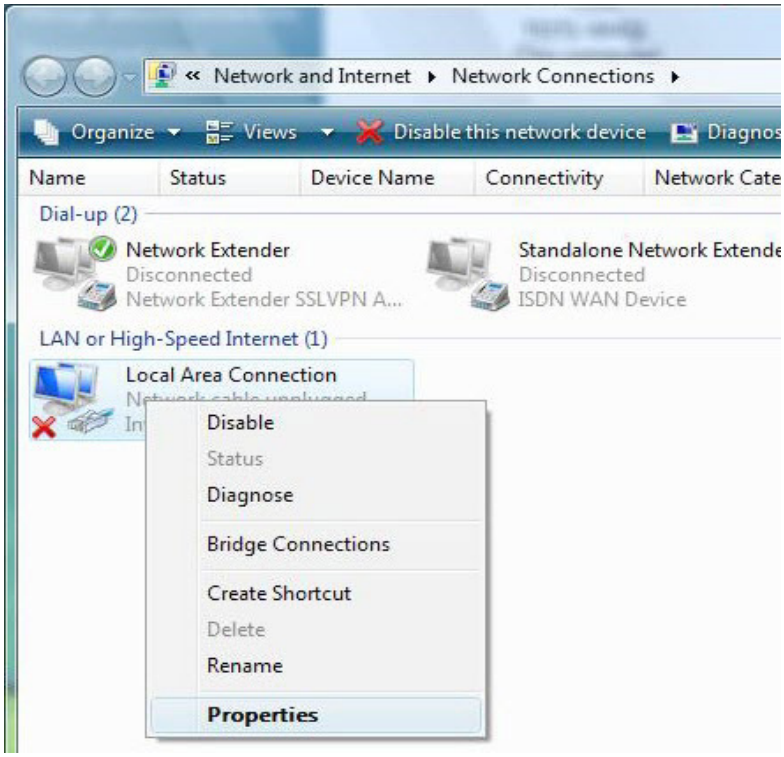
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



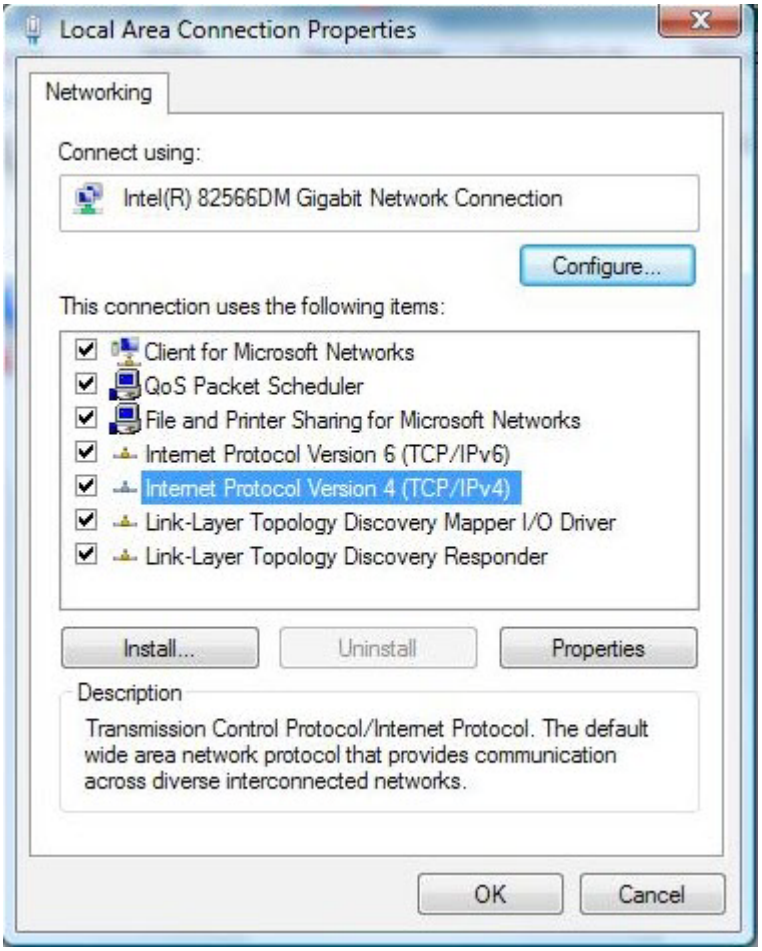
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



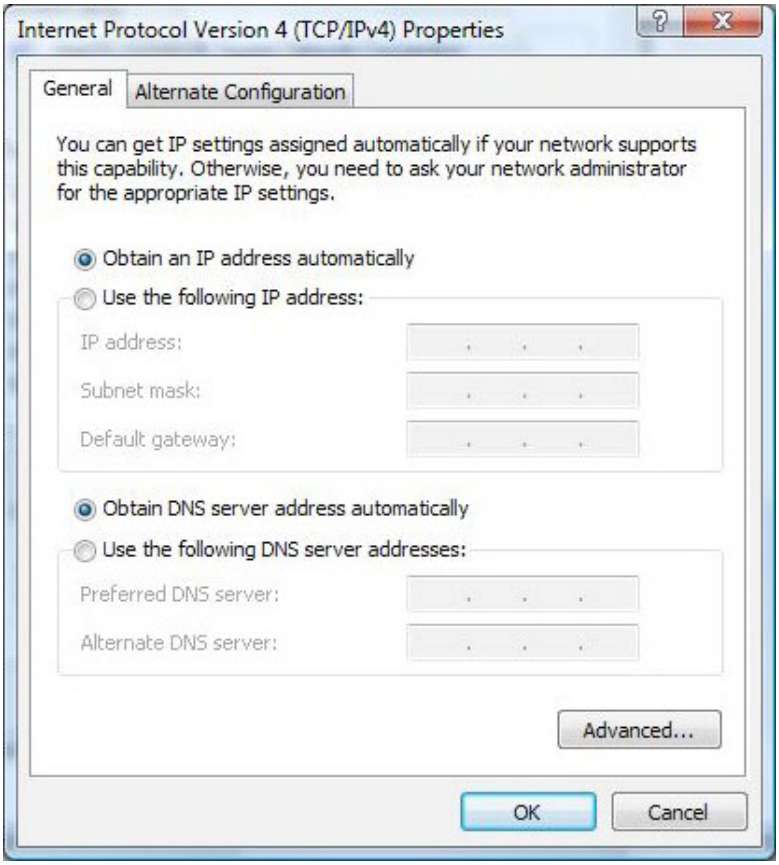
4. Select the Local Area Connection, and right click the icon to select Properties.



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

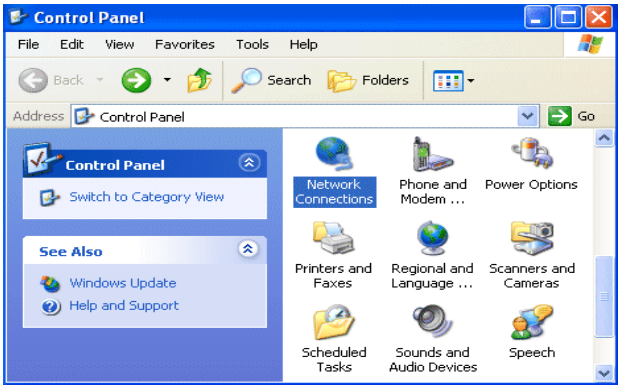


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

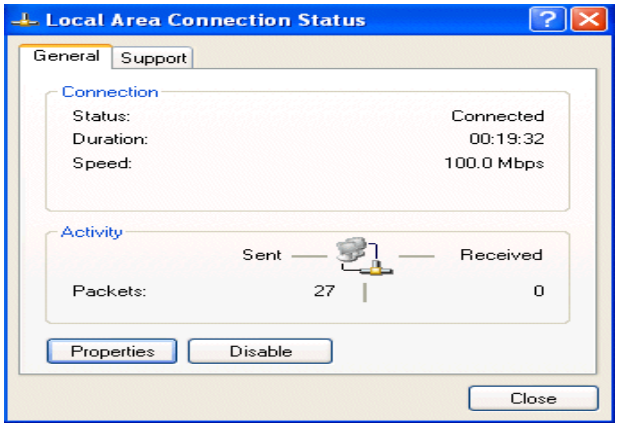


Configuring PC in Windows XP

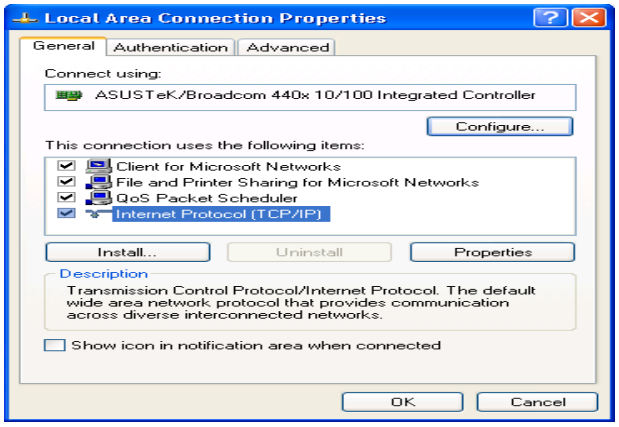
1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.



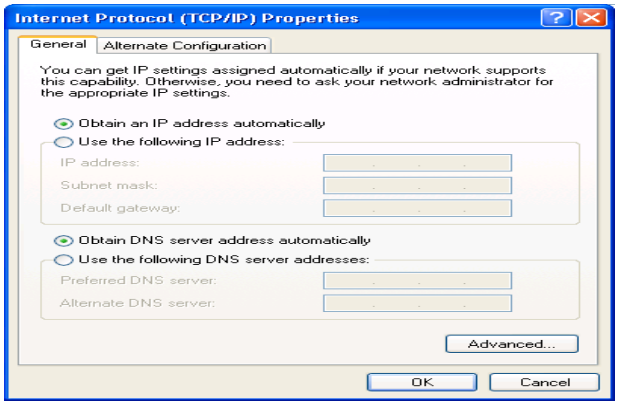
3. In the Local Area Connection Status window, click Properties.



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

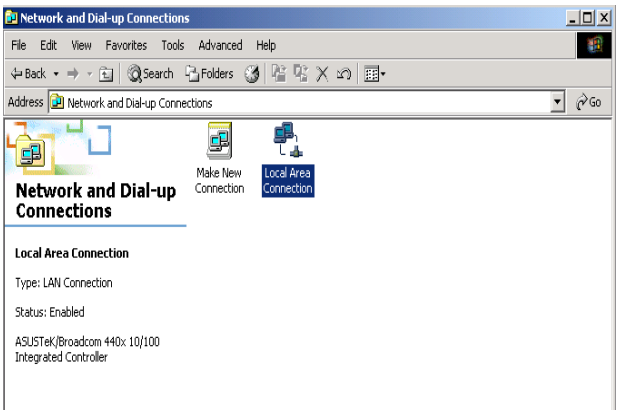


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

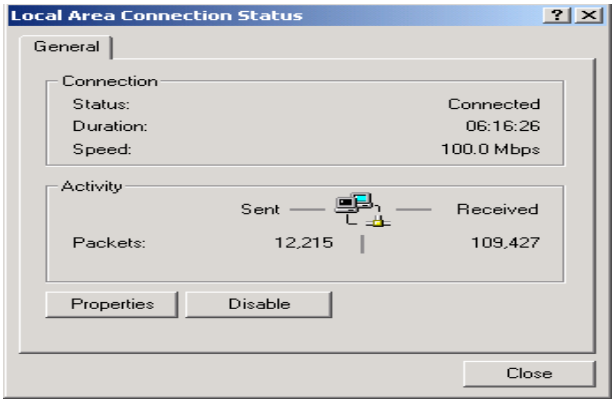


Configuring PC in Windows 2000

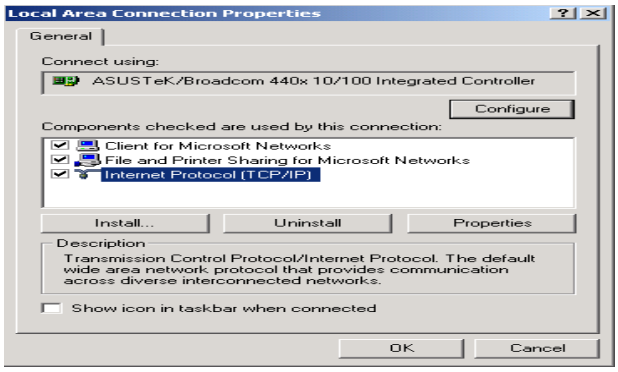
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



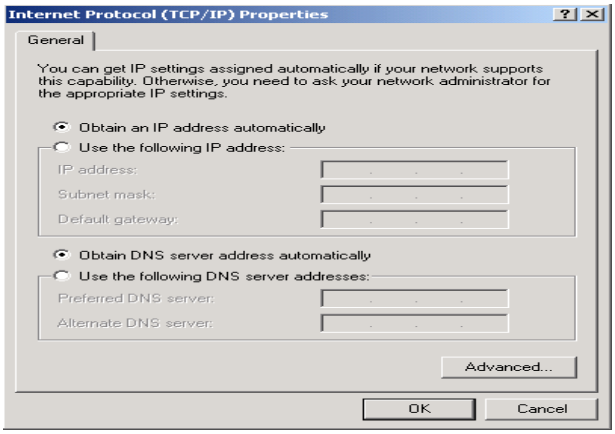
3. In the Local Area Connection Status window click Properties.



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

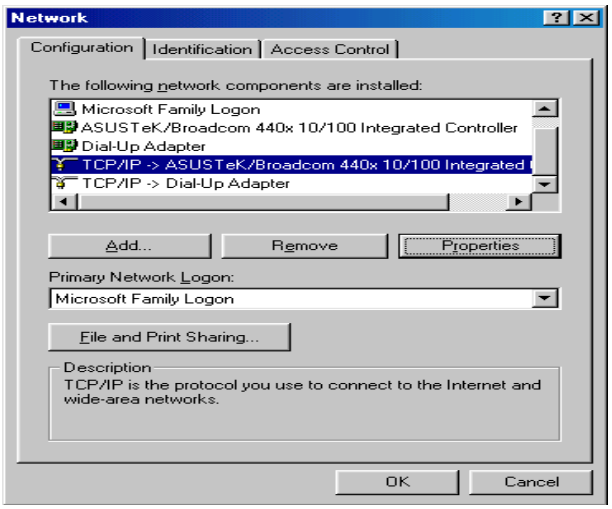


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

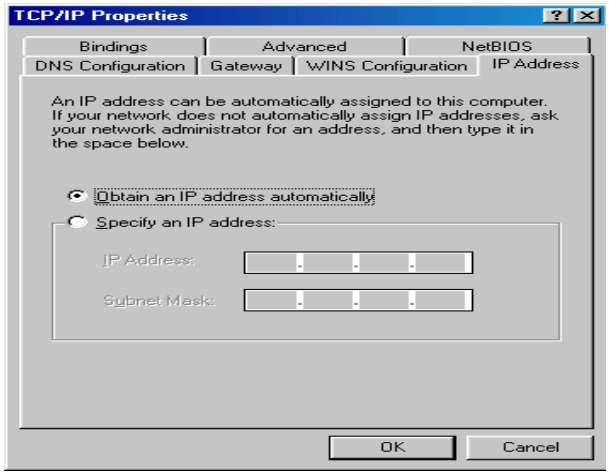


Configuring PC in Windows 95/98/Me

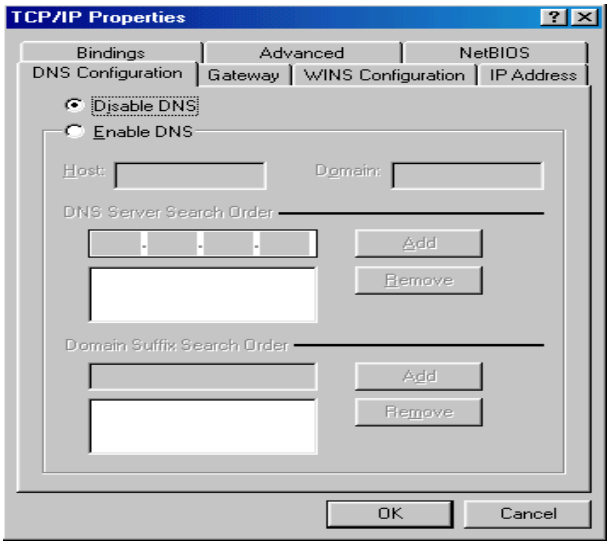
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



3. Select the Obtain an IP address automatically radio button.

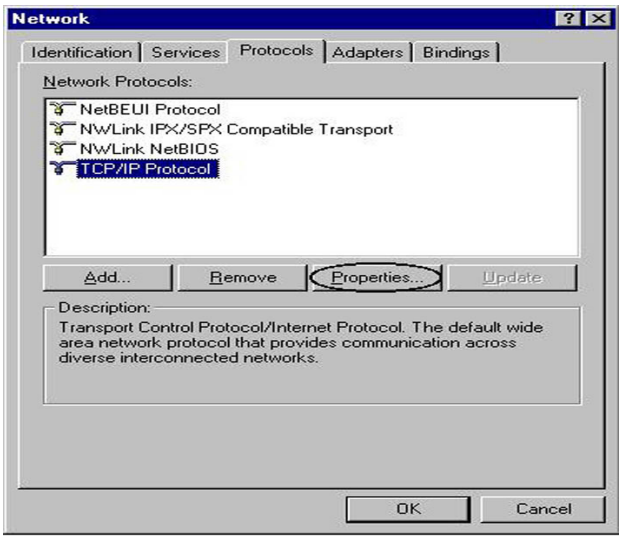


4. Then select the DNS Configurationtab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

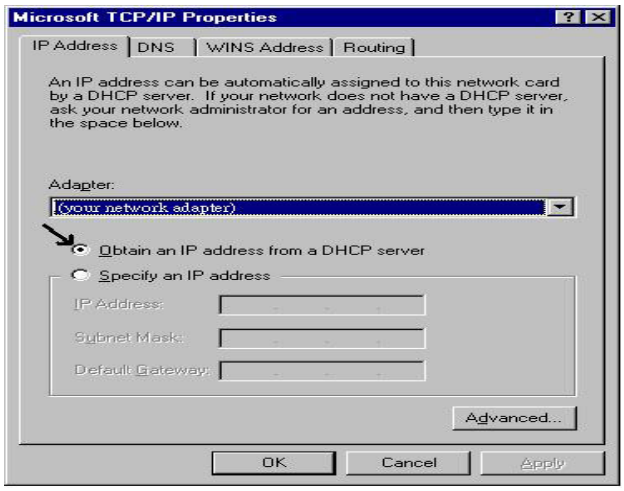


Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.



3. Select the Obtain an IP address from a DHCP server radio button and click OK.



Factory Default Settings

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

Web Interface (Username and Password)

Three user levels are provided by this router, thus Administrator, Basic and Advanced respectively. You can turn to User Management to change the corresponding passwords and get more.

- Administrator
  - Username: admin
  - Password: admin
- Basic(local)
  - Username: user
  - Password: user
- Advanced (for remote login)
  - Username: support
  - Password: support

Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 5 seconds.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

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

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the tale.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

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).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

Chapter 4: Configuration

To easily configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There are basically 2 ways to configure your router before you are able to connect to the internet: **Easy Sign-On** & **Web Interface**. Configuration of each method will be discussed in detail in the following sections.

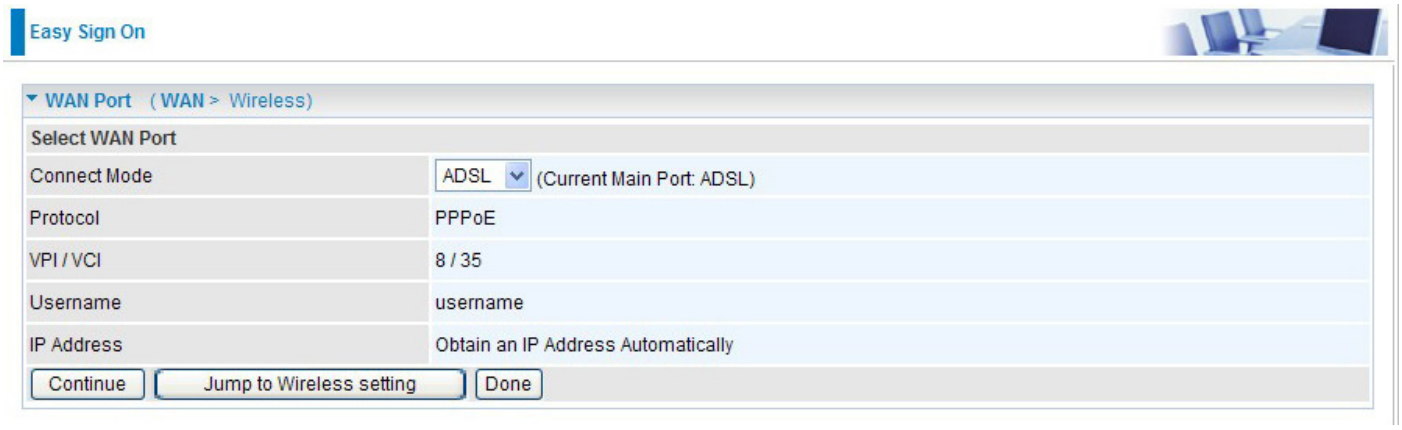
Easy Sign-On (EZSO)

This special feature makes it easier for you to configure your router so that you can connect to the internet in a matter of seconds without having to logon to the router GUI for any detail configuration. This configuration method is usually auto initiated if user is to connect to the internet via Billion's router for the first time.

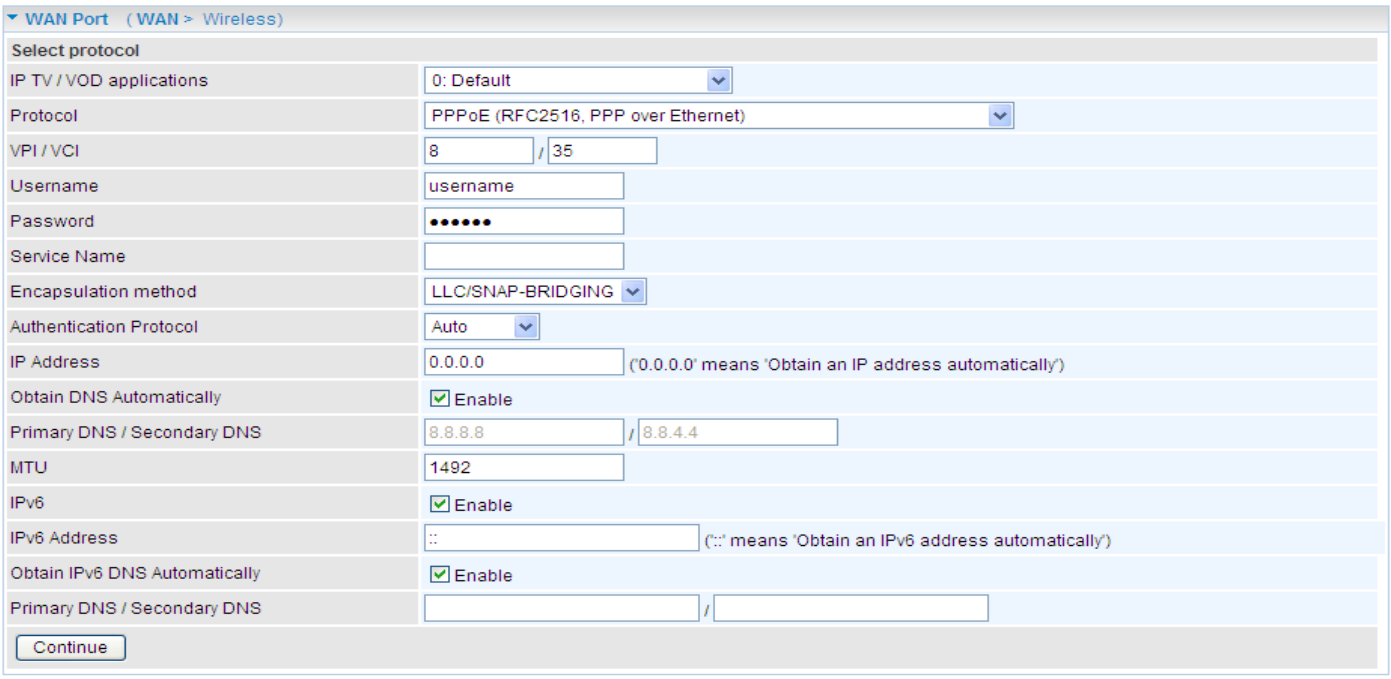
After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information that you have obtained from your ISP. By following the instructions given carefully and through the information you provide, the router will be configured in no time and you will find yourself surfing the internet sooner than you realize.

Follow the Easy Sign-On configuration wizard to complete the basic network configuration.

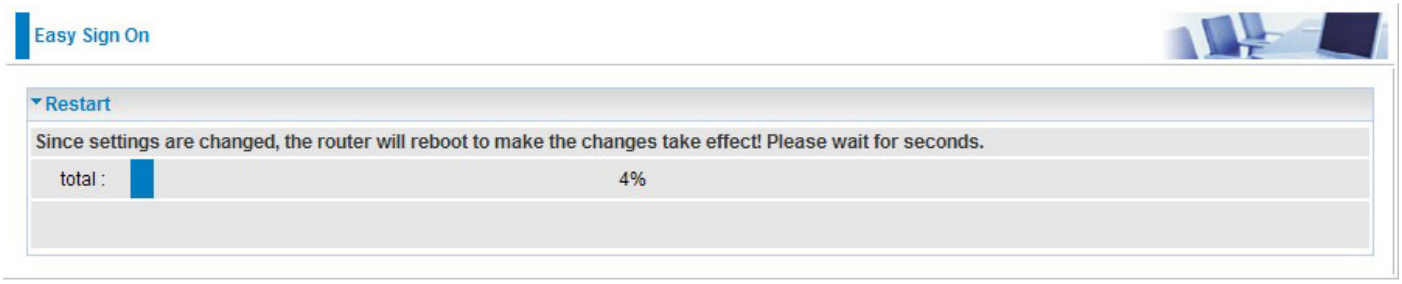
1. Connect your router with all the appropriate cables. Then, load your IE / netscape browser.
2. When the EZSO configuration wizard pops up, select the connect mode which you want to set up and then click continue.



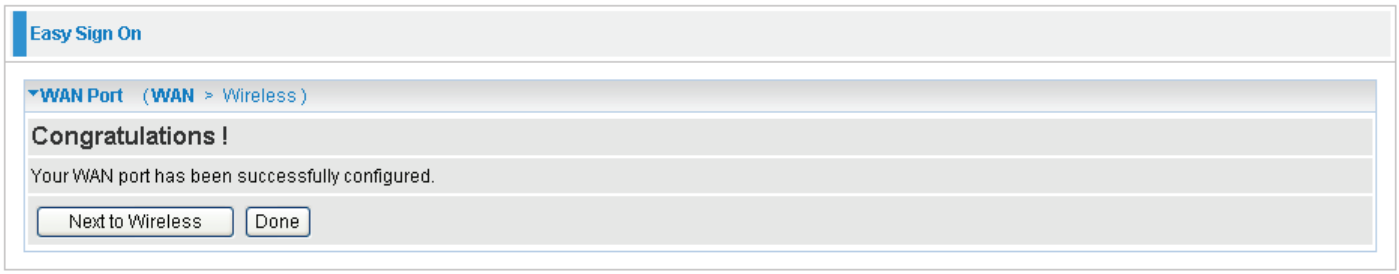
3. Please enter all the information in the blanks provided and then click continue.



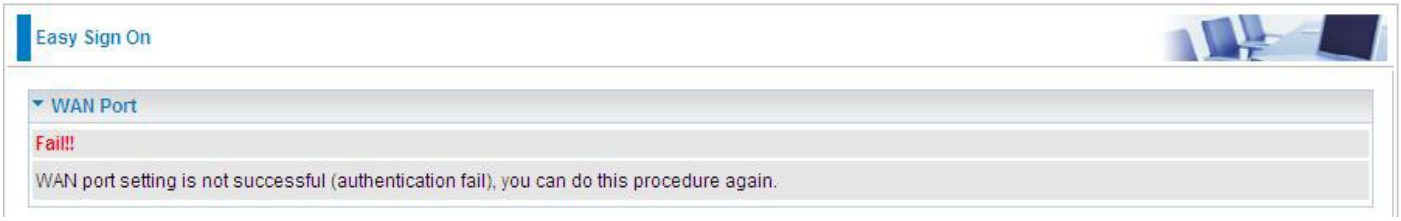
4. The device will reboot and then load the new configuration.



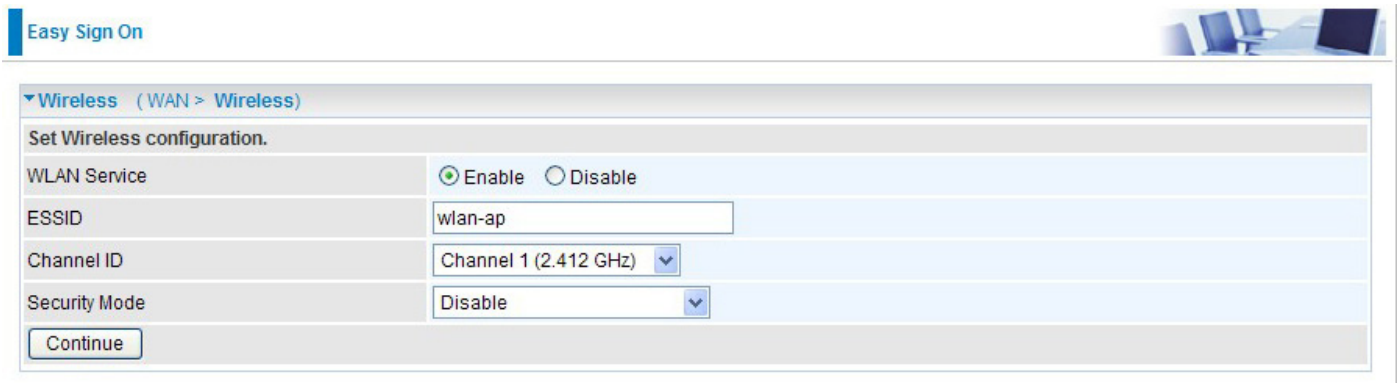
5. If all information provided is valid and the device successfully connects to WAN, a dialog box will appear to signify the completion of the WAN port setup. At this point you can either click Done to finish the EZSO configuration or you can click Next to wireless to proceed to the wireless configuration if you have.



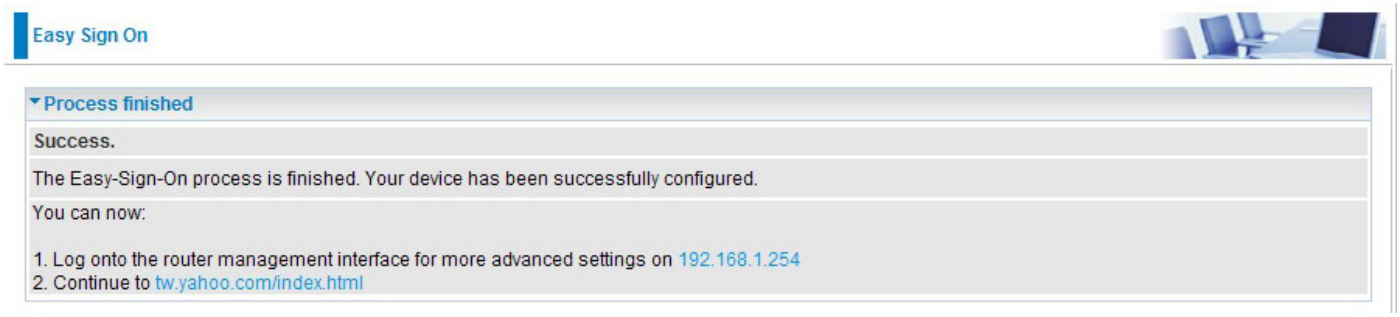
6. However, if any error occurs during device configuration that results in WAN connection failure, the system will prompt that the setup has failed.



7. Select Enable and enter the necessary information in the blanks provided for the Wireless LAN setting (wireless setting is only available for BiPAC 7800N) if you would like to use this feature and then click Continue.

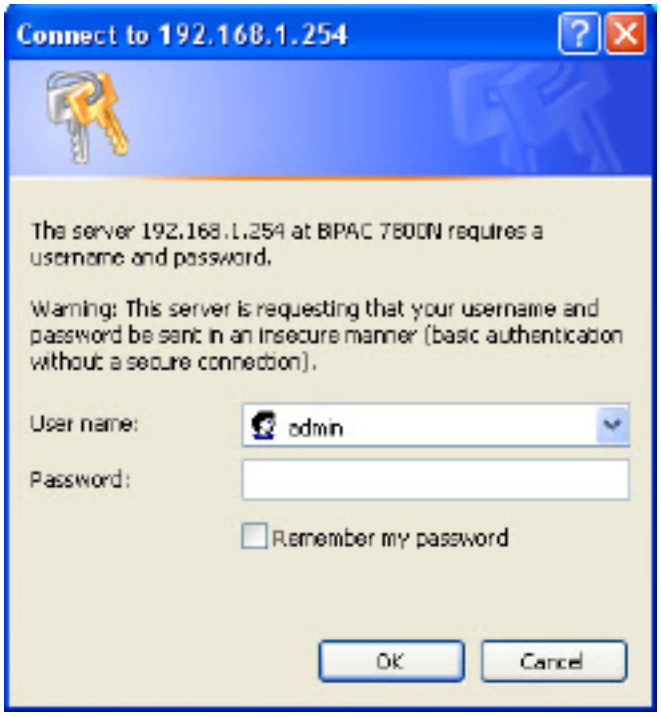


8. The system will save your new configuration and complete the setup. You can test the connection by clicking on the URL link provided. If the setup is successful you will be redirected to website.



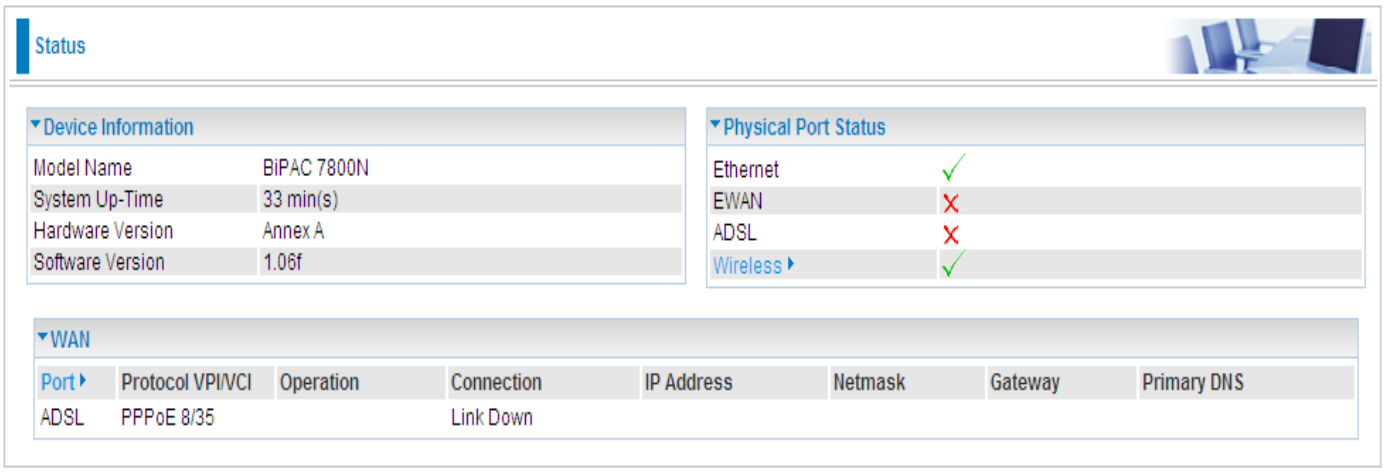
Configuration via Web Interface

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click  or press 'Enter' key on the keyboard, a login prompt window will appear. The default username and password are "admin" and "admin" respectively.



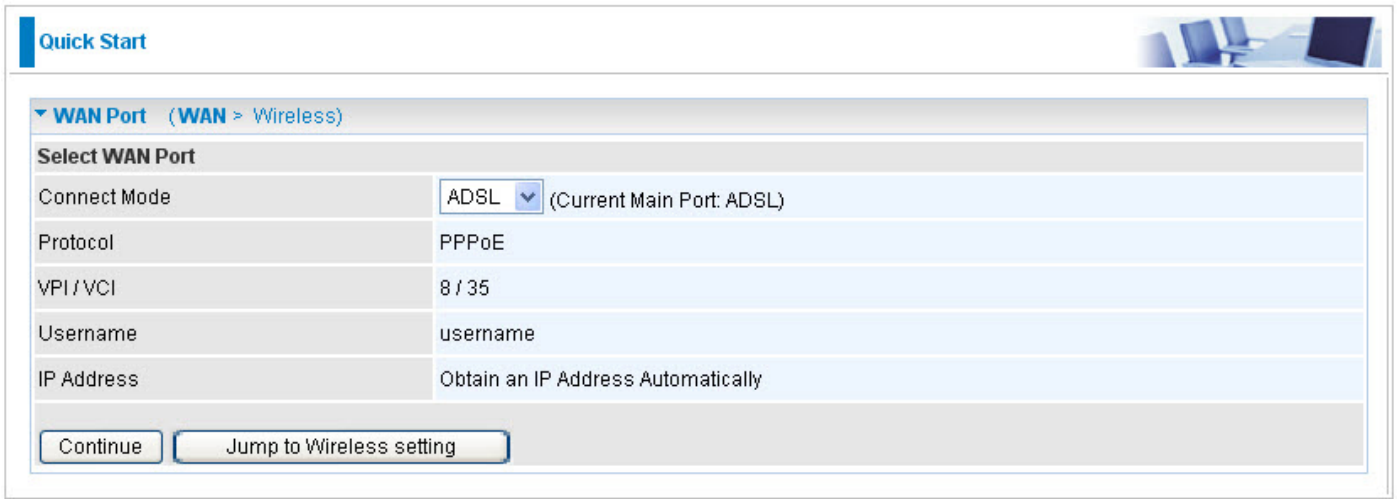
Congratulations! You are now successfully logged in to the Firewall Router!

If the authentication succeeds, the homepage Status will appear on the screen.



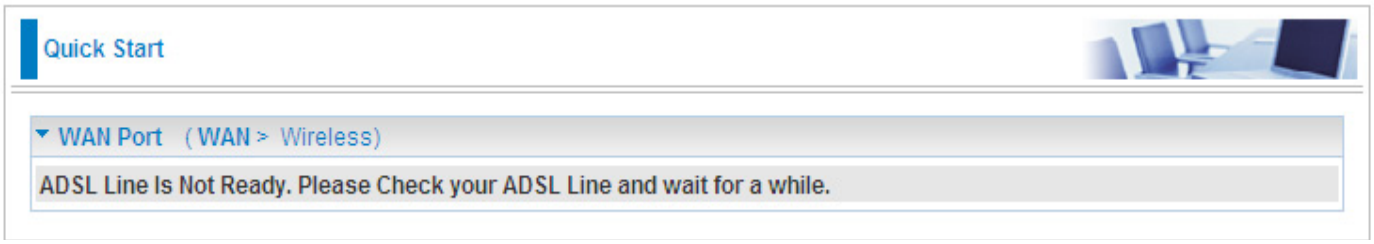
Quick Start

ADSL Mode

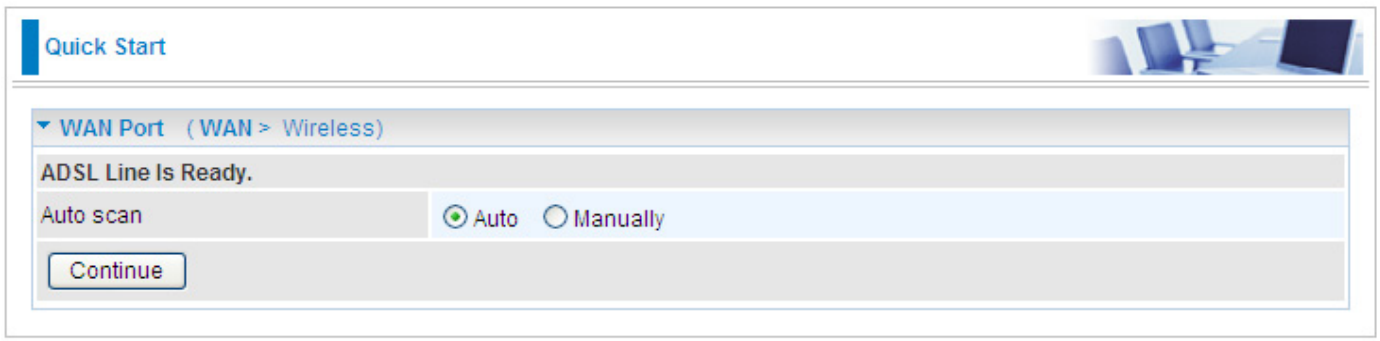


Step 1: Select WAN port connect mode from the connect mode drop down menu. There are two types of connect mode to choose from: ADSL or EWAN. Here select **ADSL** and click **Continue**. If you only want to configure Wireless, press **Jump to Wireless setting**.

Step 2: When ADSL line is not ready, the screen1 below will appear to remind you. Then you should connect the ADSL line. While ADSL line is ready, the screen 2 below will appear to let you go on.Here you can select Auto or Manually. Select **Auto** will go to step 3, and select **Manually** will go to step 4.

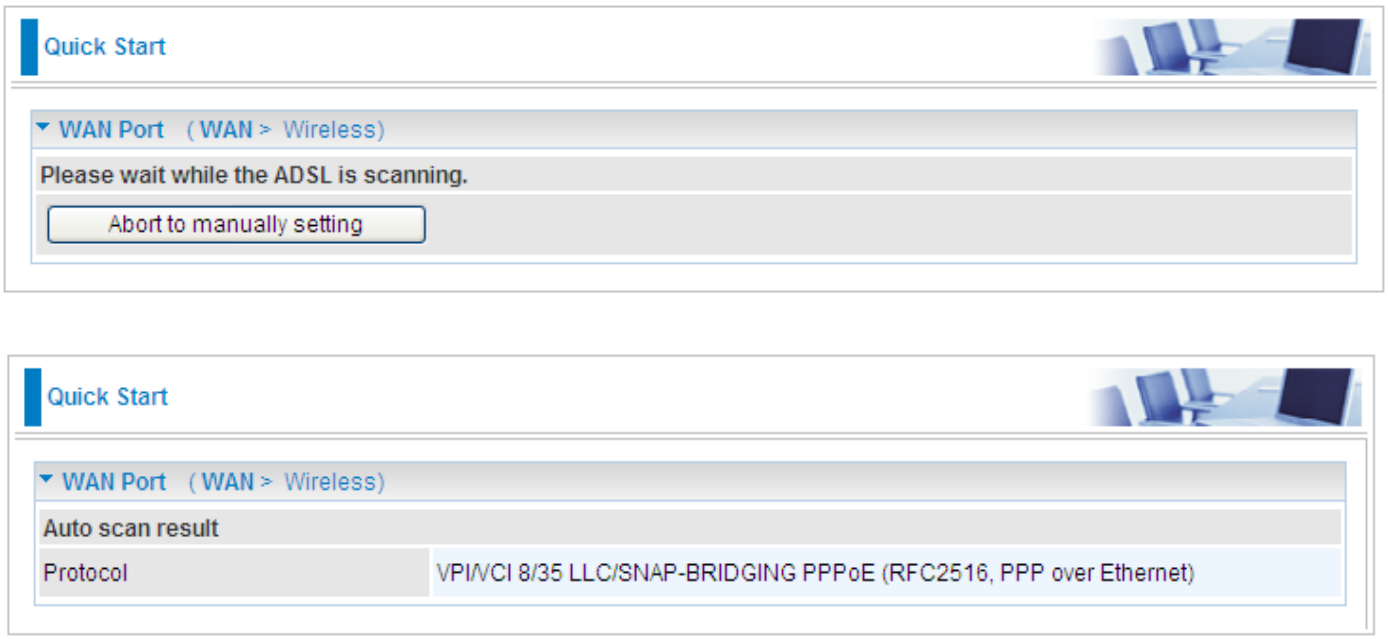


Screen1



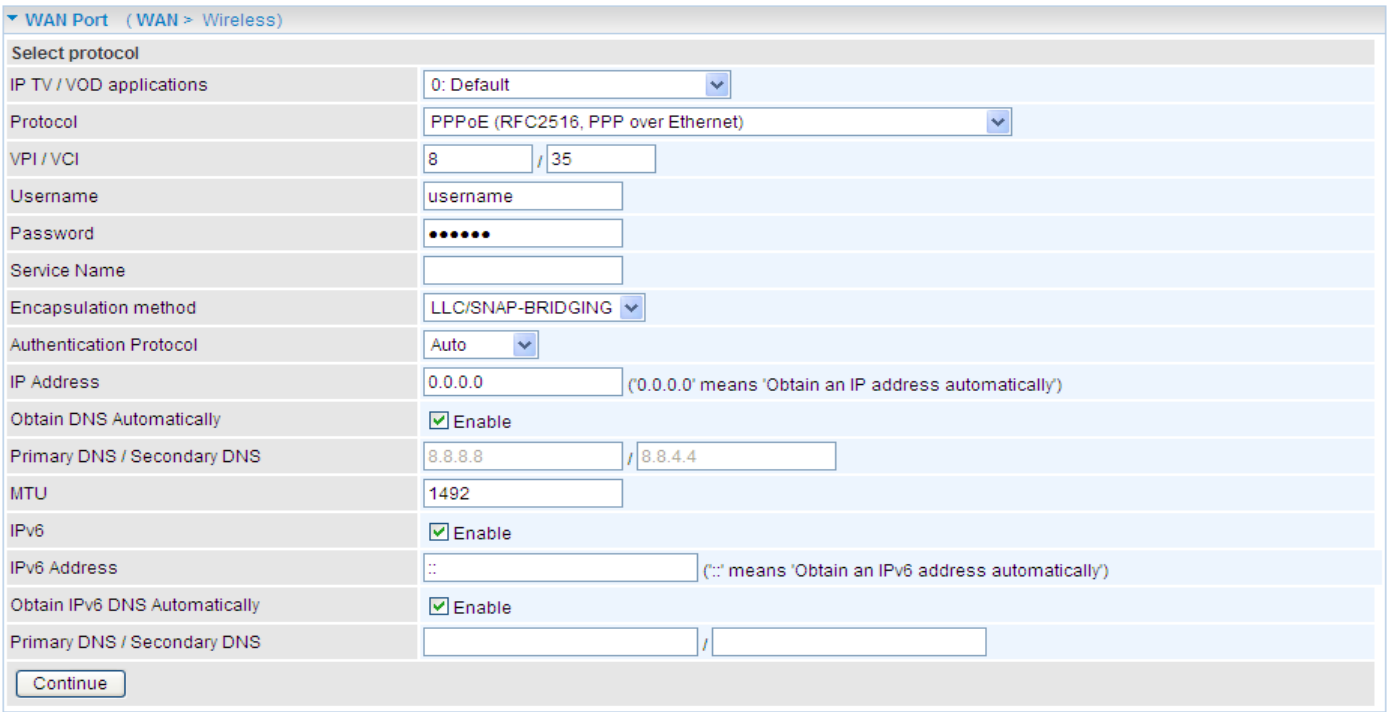
Screen 2

Step3: Wait while the DSL is scanning, when the scanning is OK, the scanning result will appear, see screen 3, and then it will quickly goes to step 4. Or you can **Abort to manually setting** to step 4.

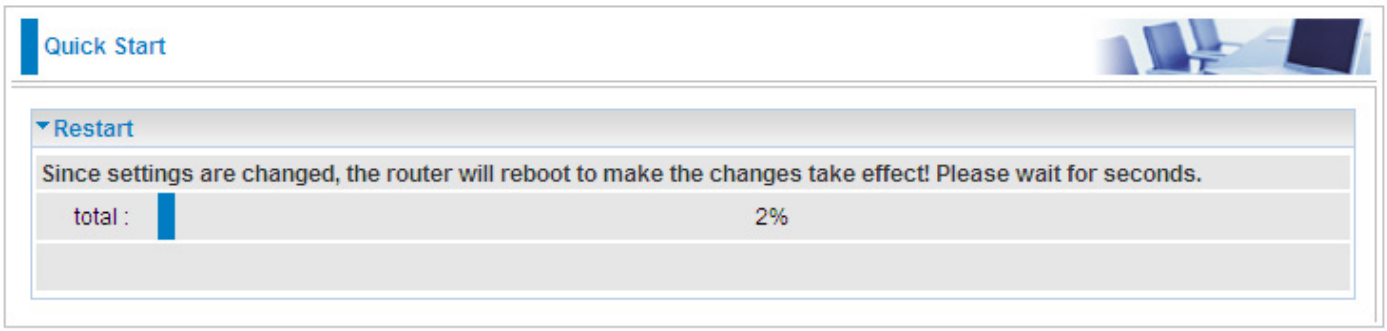


Screen 3

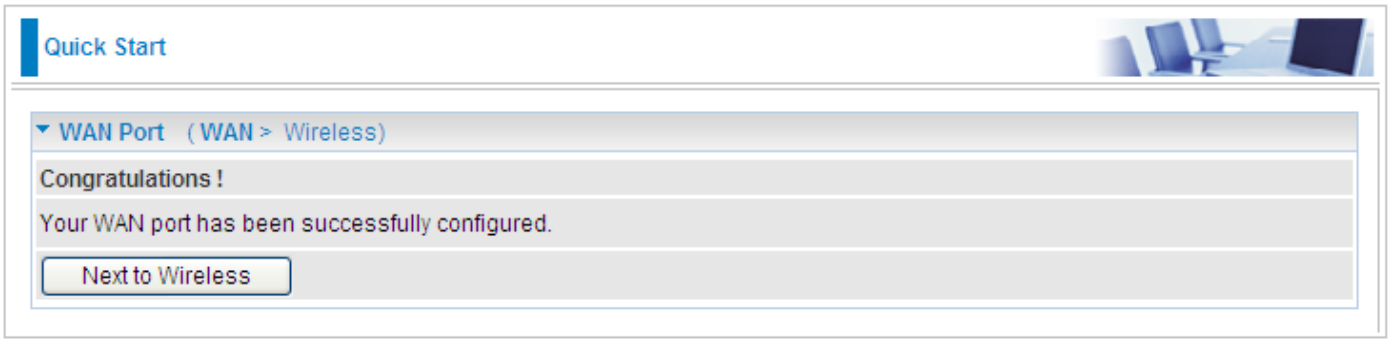
Step 4: There are 5 types of connection protocols available under ADSL connect mode .***Each type of connection mode is described in the following sections of ADSL Connect mode.*** Select the needed protocol and enter the needed information from your ISP.



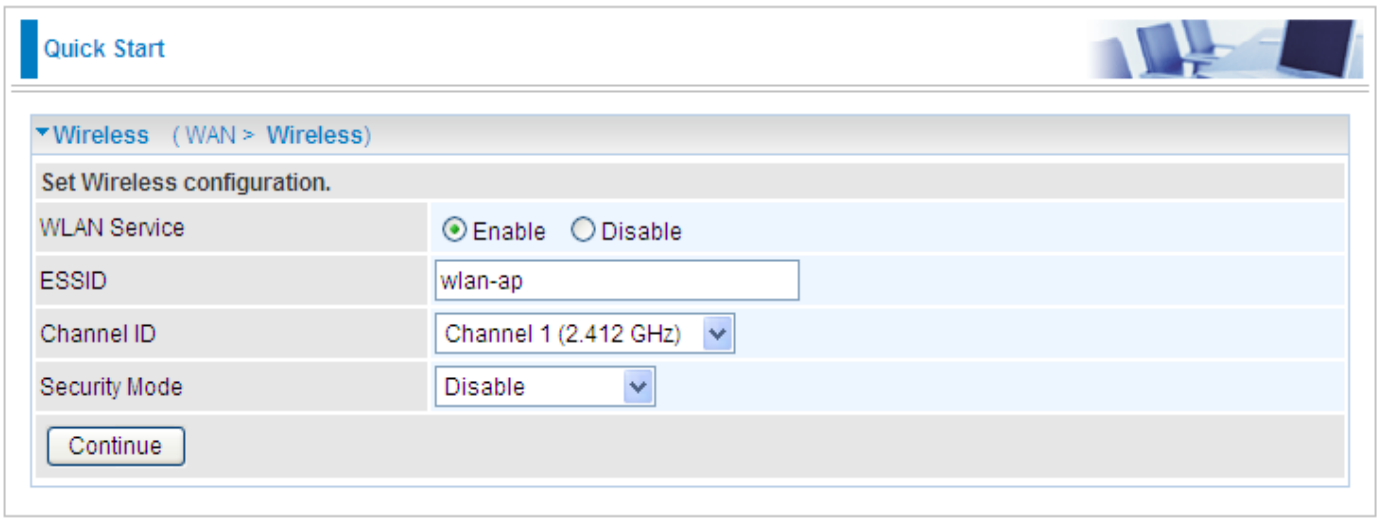
Step 5: The device will reboot and then load the new configuration.



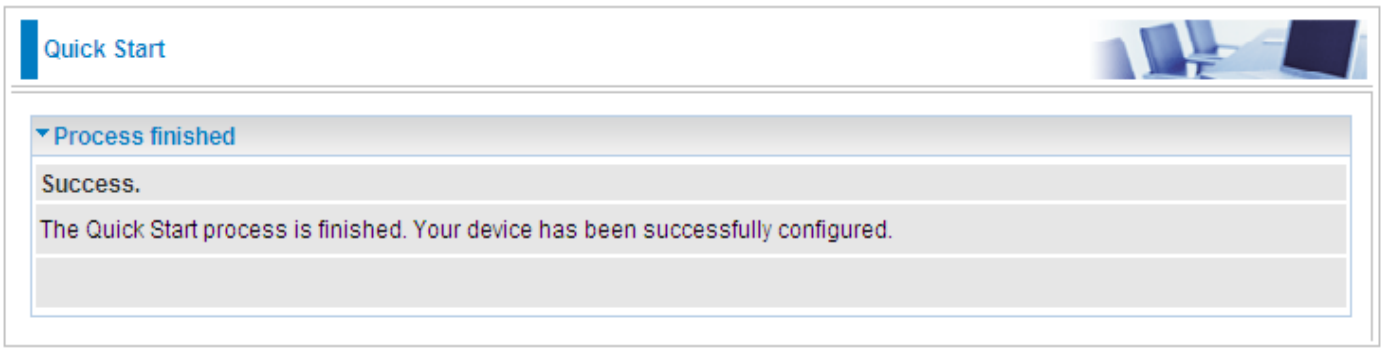
Step 6: WAN port configuration is success. And if you want contiune configuring wireless, press **Next to Wireless** button to go on.



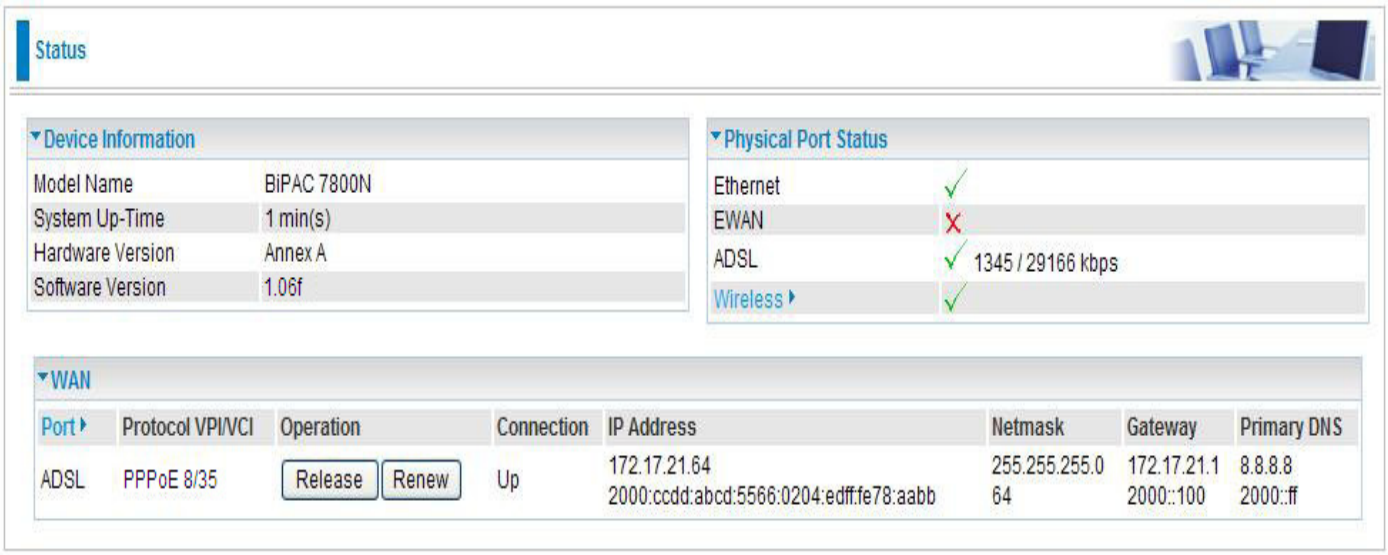
Step 7: Enter the ESSID, select the Channel ID and the Security Mode, click **Continue** to go on. For detail, please turn to **WLAN** in this manual for help.



Step 8: Quick Star is finished.



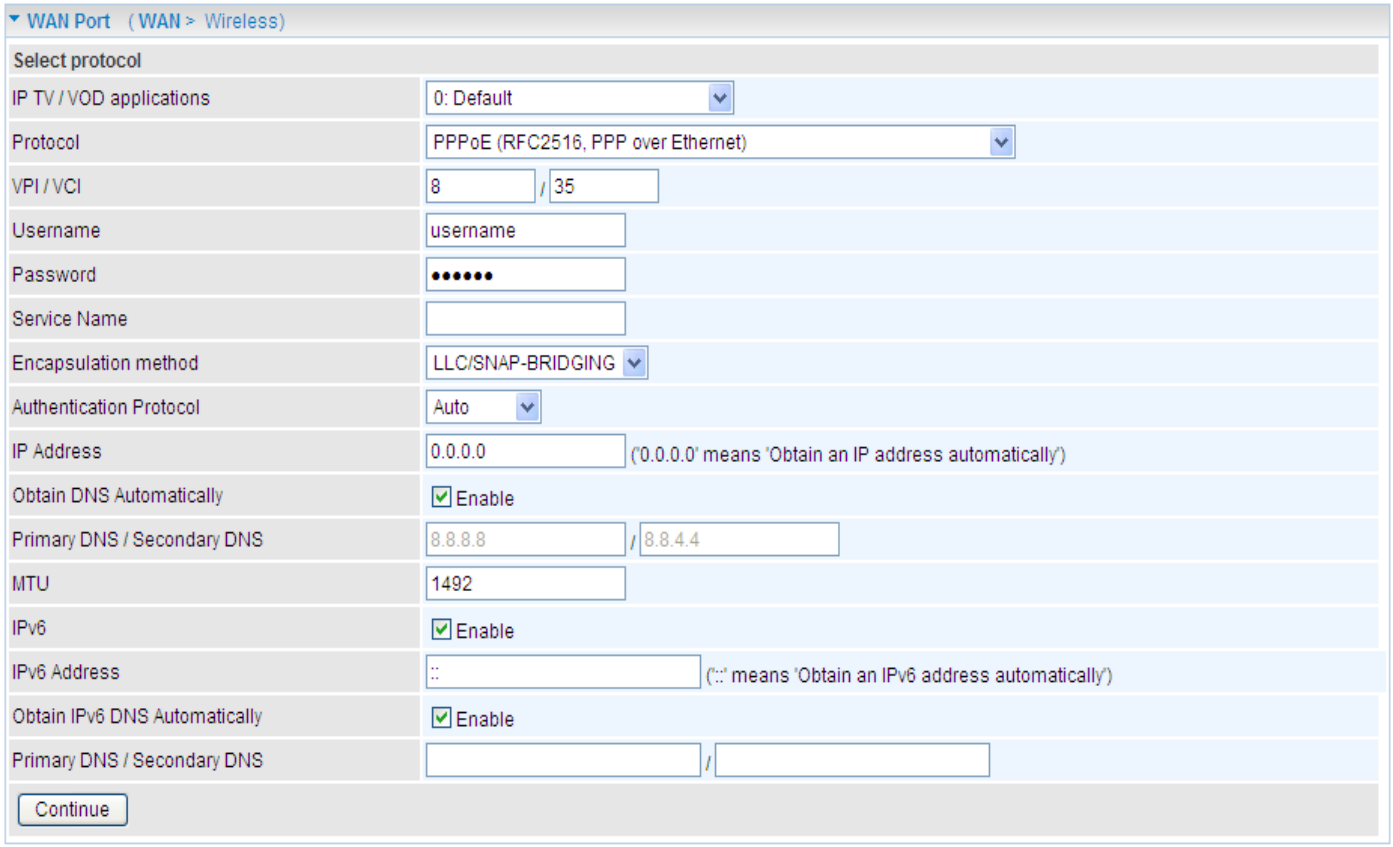
You can go to the Status and view the basic information.



ADSL Connect Mode

For ADSL connect mode there are 5 types of connection protocols: **PPPoE, PPPoA, IPoA, MPoA** and **Pure Bridge**.

PPPoE



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

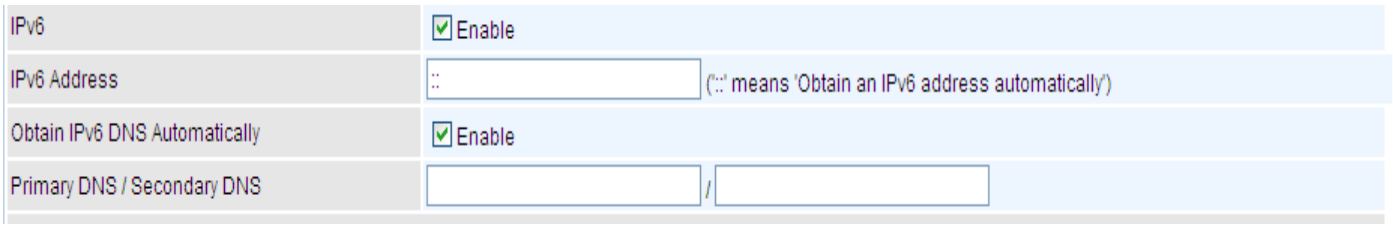
IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain DNS Automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

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

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.

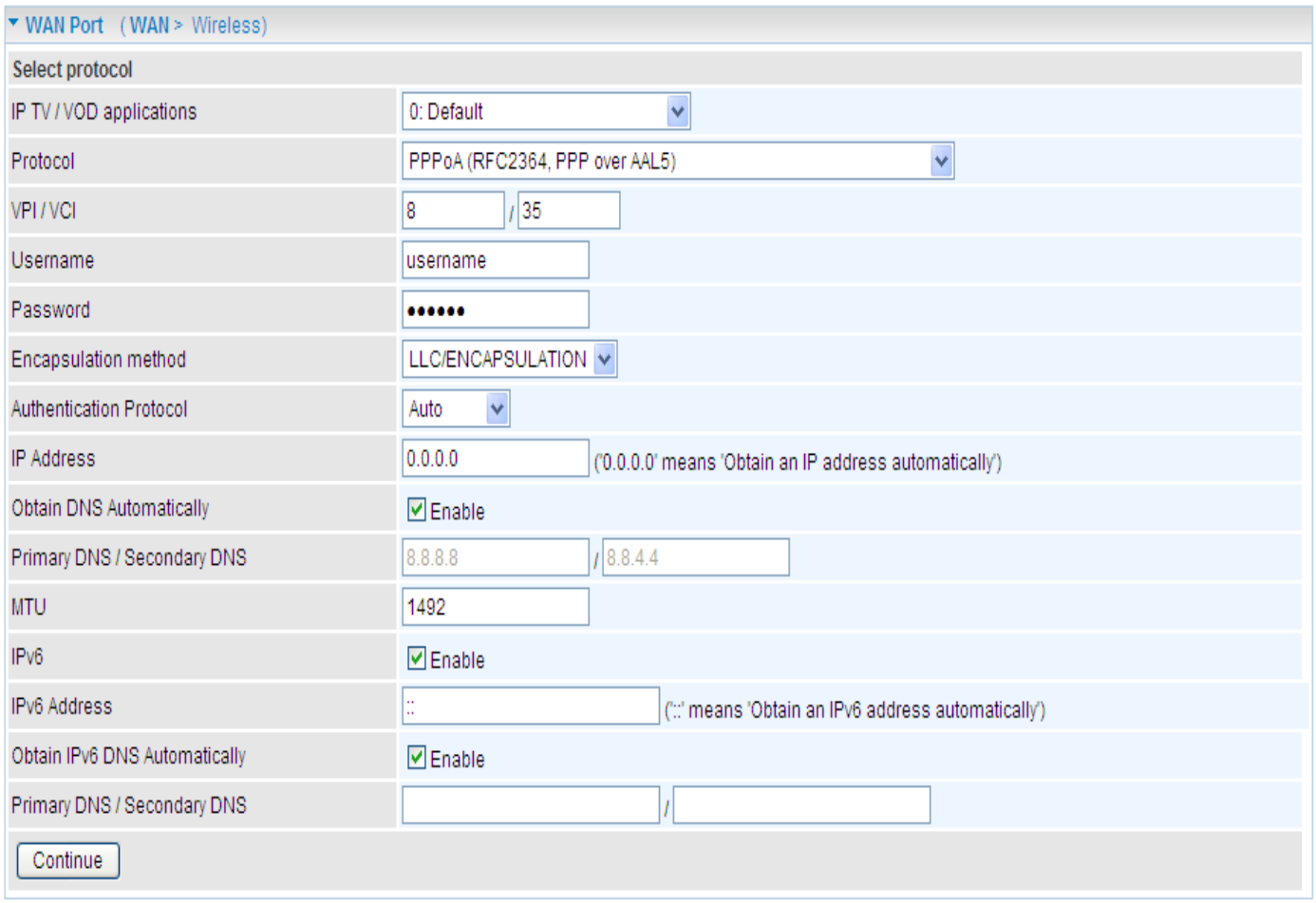


IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ”::” means to obtain IPv6

address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the exact ones in the Primary and secondary fields.

PPPoA



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

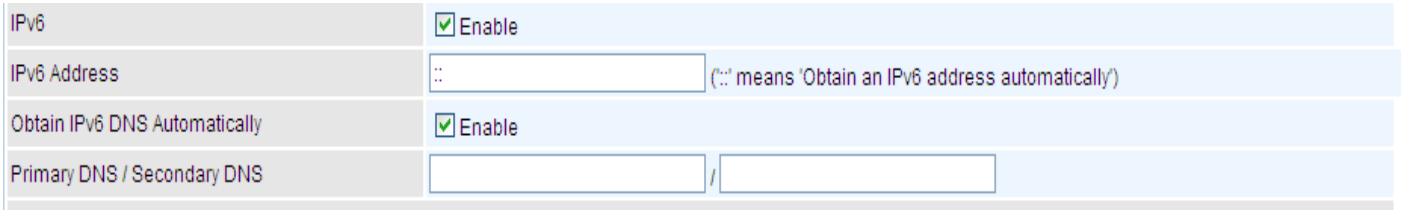
IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

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

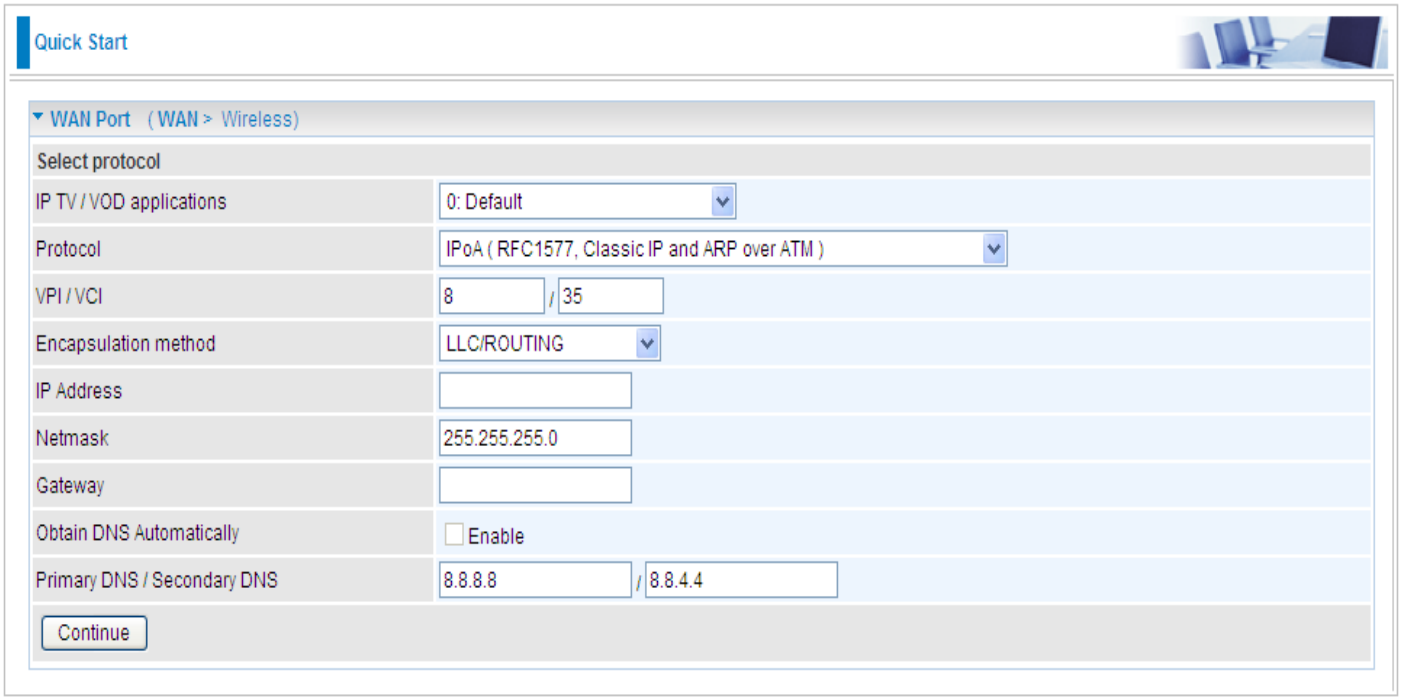
IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ”::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the exact ones in the Primary and secondary fields.

IPoA Connection



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: IPOA WAN IP address can only set fixed IP address.

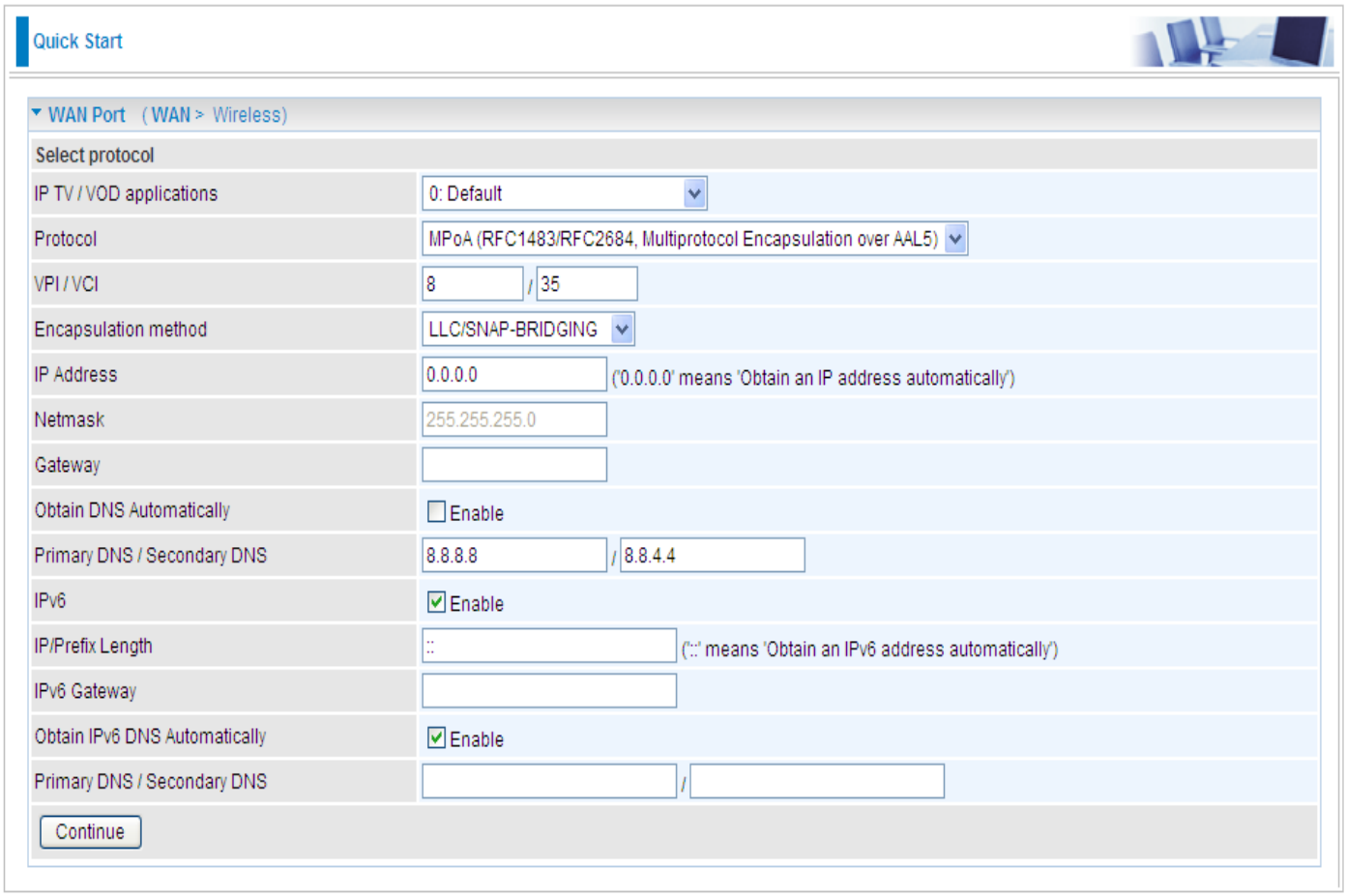
Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

MPoA Connection



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.

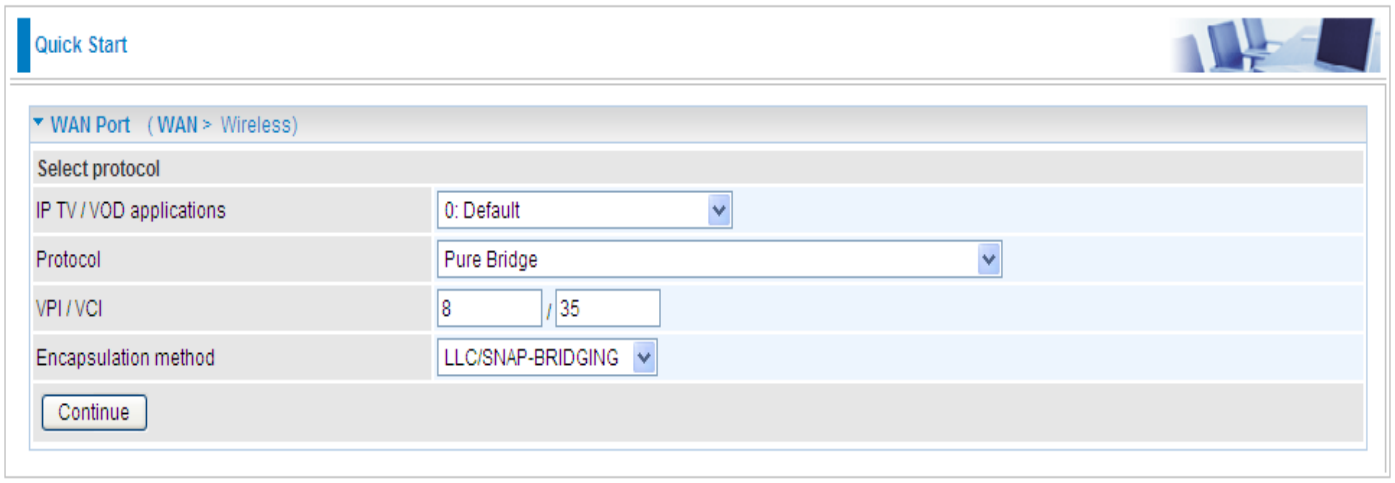
IPv6	☑ Enable
IP/Prefix Length	:: ('::' means 'Obtain an IPv6 address automatically')
IPv6 Gateway	
Obtain IPv6 DNS Automatically	☑ Enable
Primary DNS / Secondary DNS	/

IP/Prefix Length: please type the IP and the prefix length for the IPv6 address from your ISP.

IPv6 Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Pure Bridge Connection



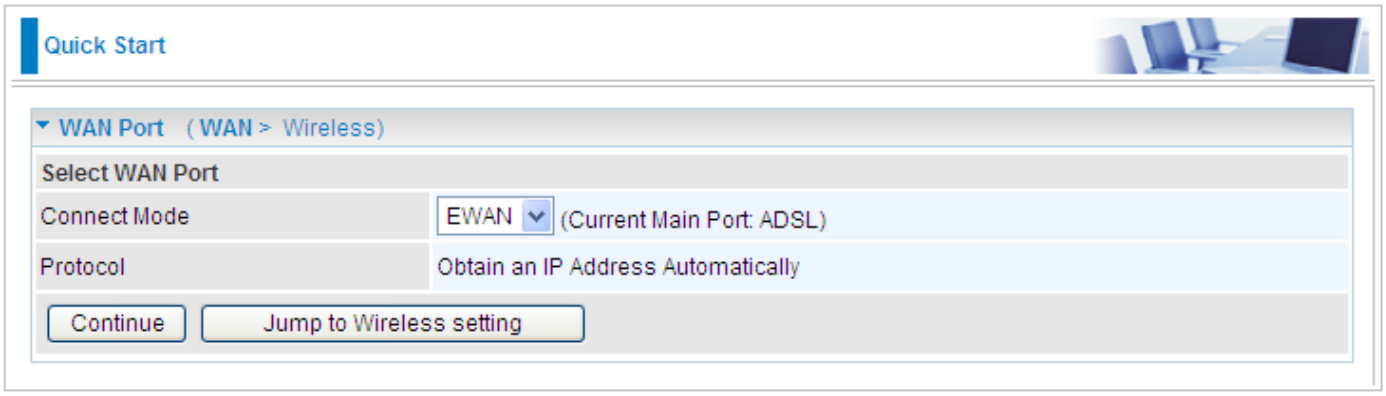
IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

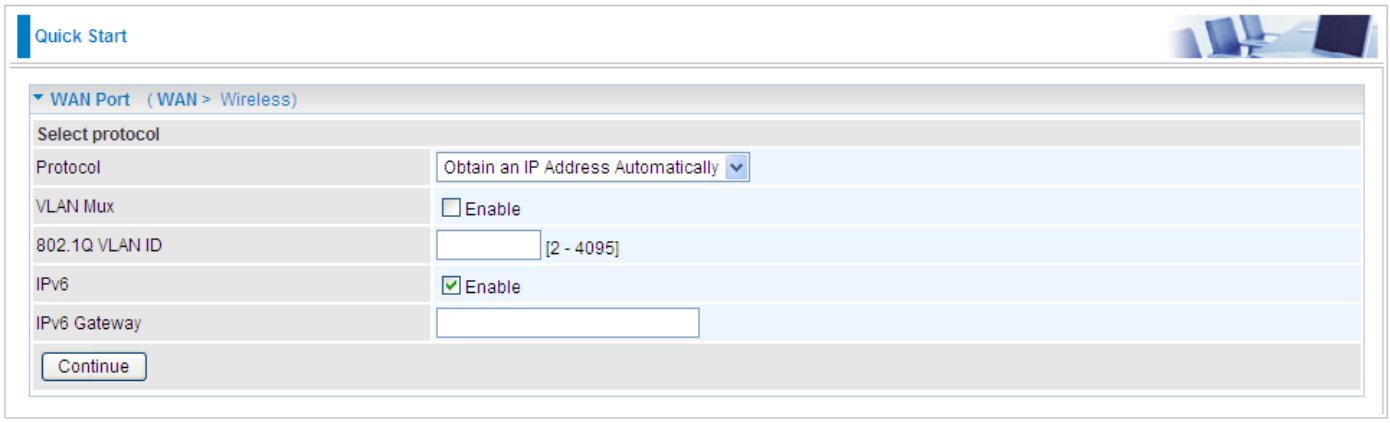
Click Apply to confirm the settings.

EWAN Mode

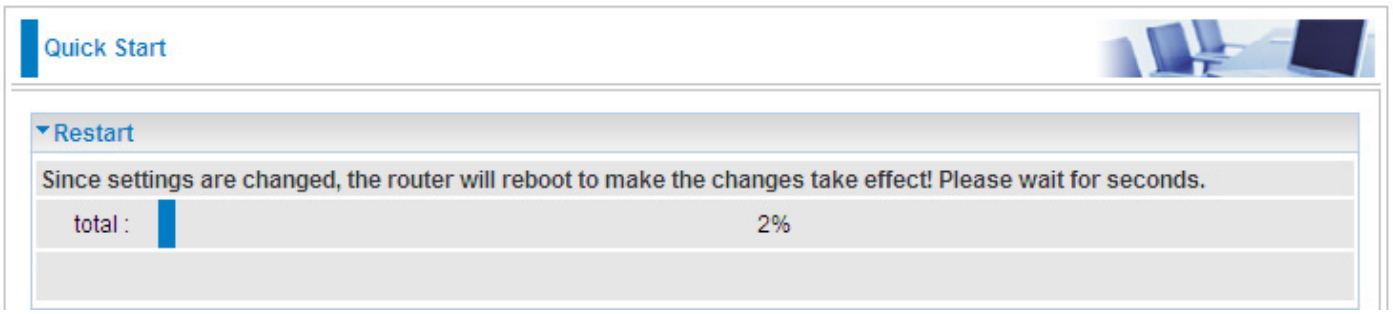


Step 1: Select WAN port connect mode from the connect mode drop down menu. There are two types of connect mode to choose from: ADSL or EWAN. Here select **EWAN** and click **Continue**. If you only want to configure Wireless, press **Jump to Wireless setting**.

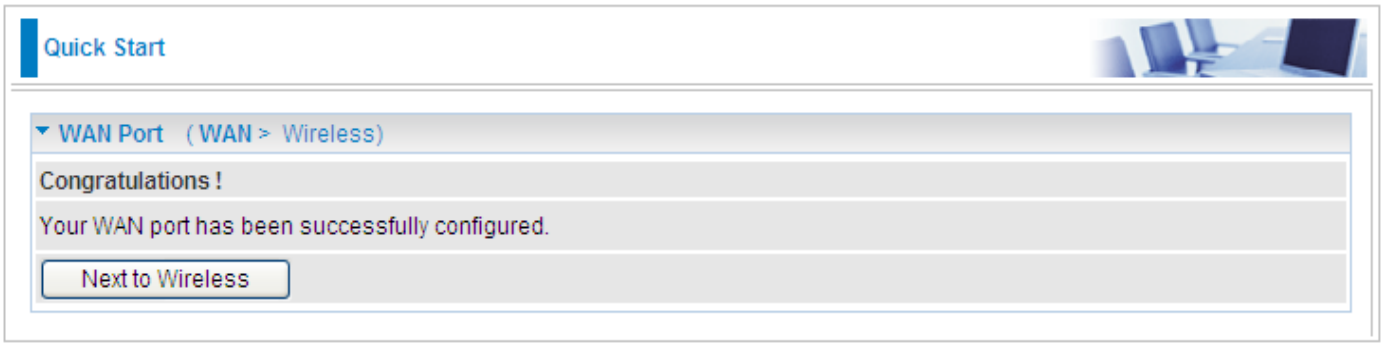
Step 2: there are four availabe protocols. ***Each protocol is described in the following sections of EWAN Connect mode.*** Select the protocol. You can enable or disable VLAN Mux feature, if enabled, you should enter the 802.1Q VLAN ID. For VLAN MUX setting, please refer to **VLAN MUX Setting** for help. Click **Continue** to go on.



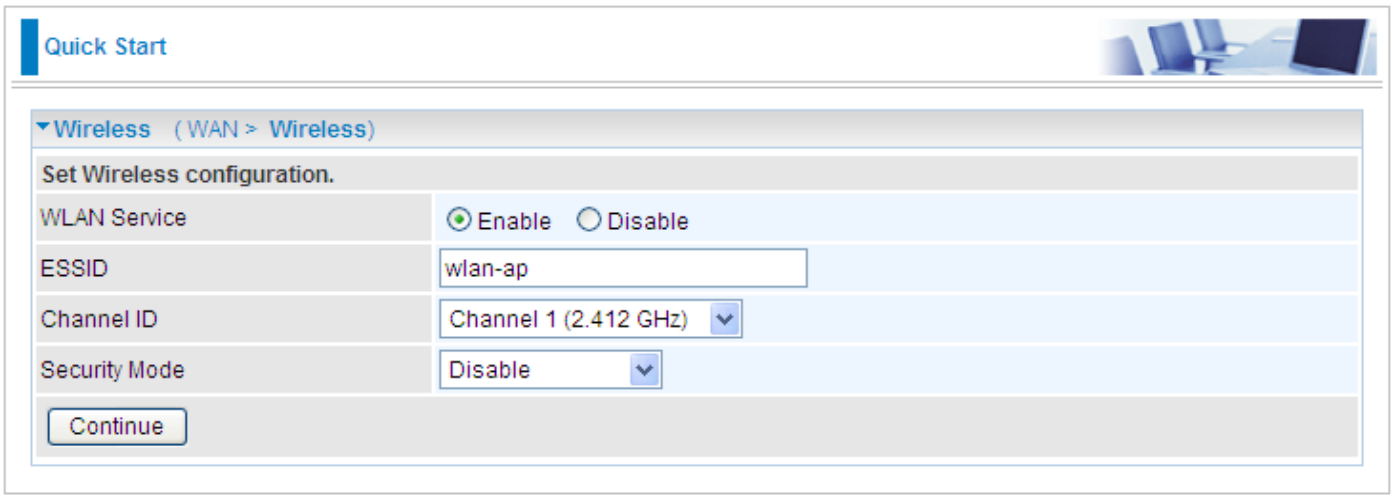
Step 3: The device will reboot and then load the new configuration.



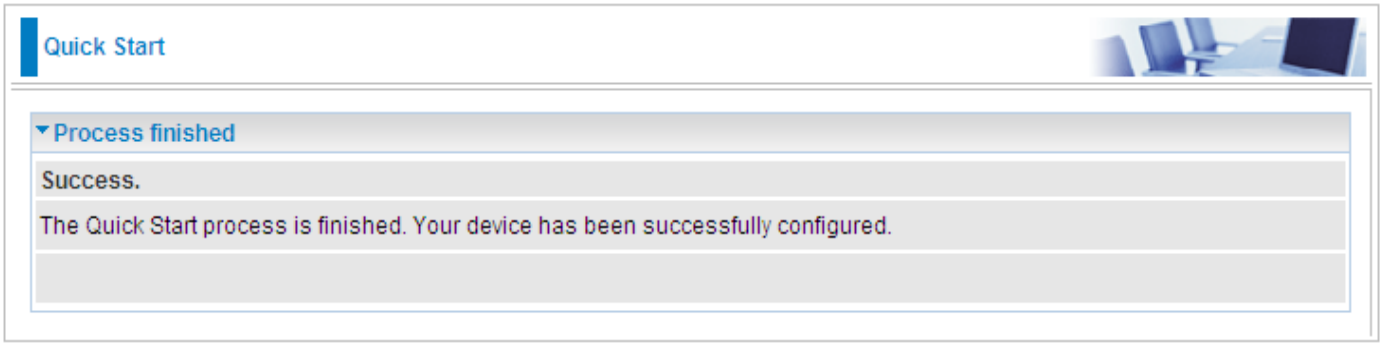
Step 4: WAN port configuration is sucess, now **Next to Wireless.**



Step 5: Enter the ESSID, select the Channel ID and the Security Mode. For security information, please turn to **WLAN** section in this manual for help.

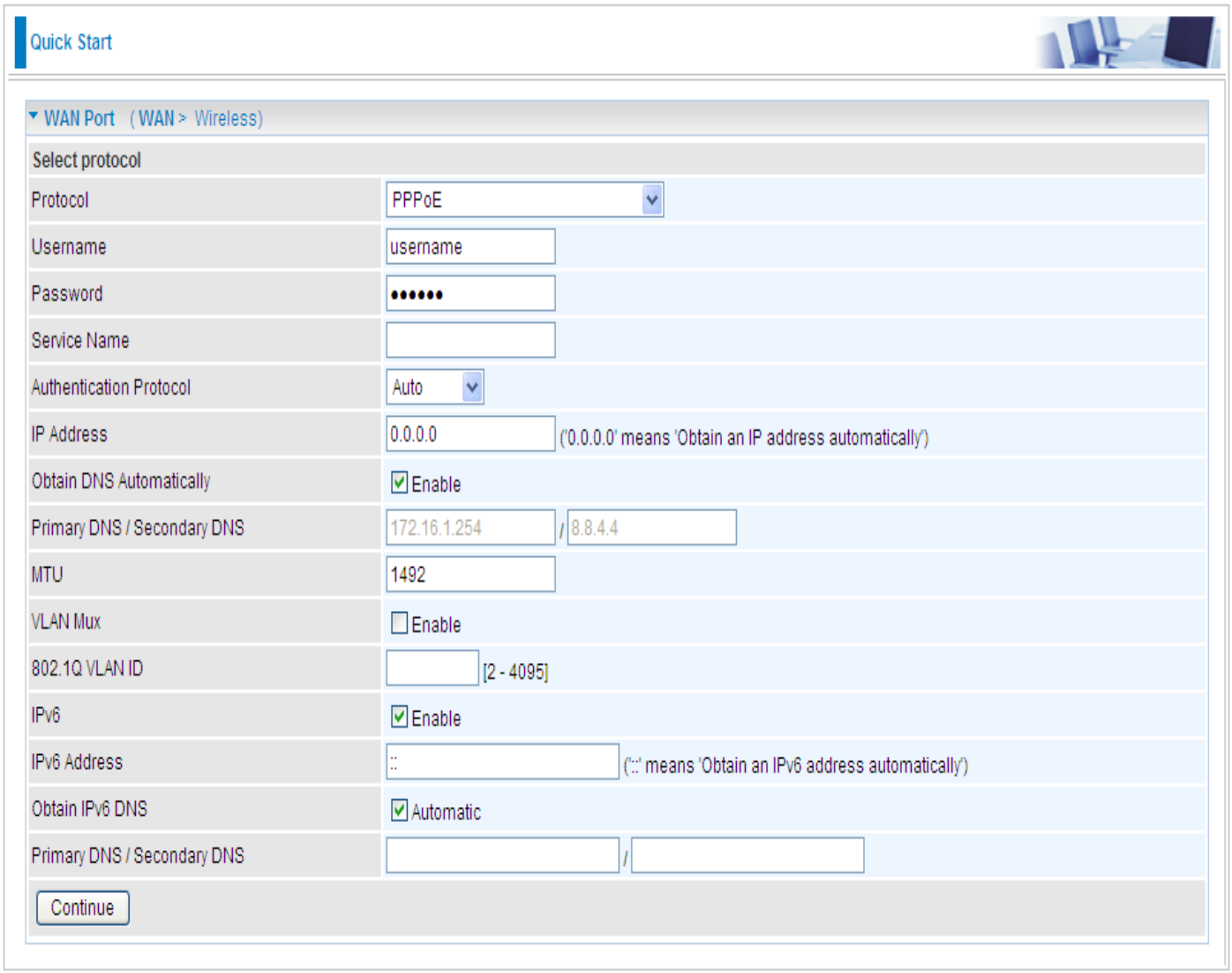


Step 6: Quick Start is finished.



EWAN Connect Mode

PPPoE connection



Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Authentication Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Enter your fixed IP address.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

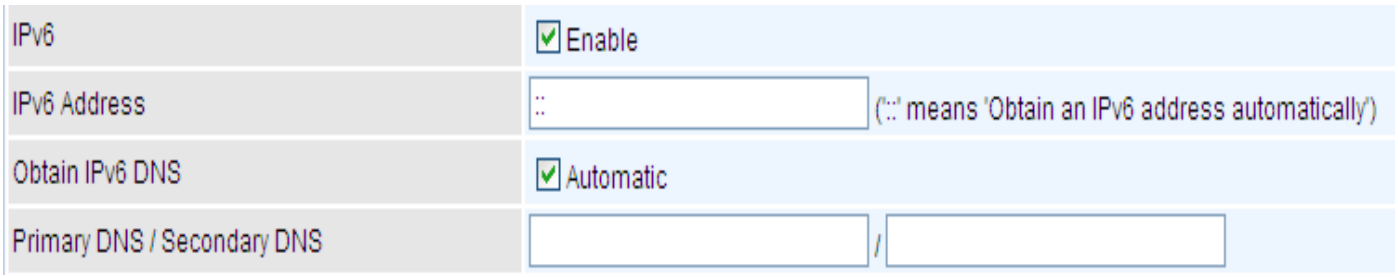
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific

headers) that IP will attempt to send through the interface.

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.

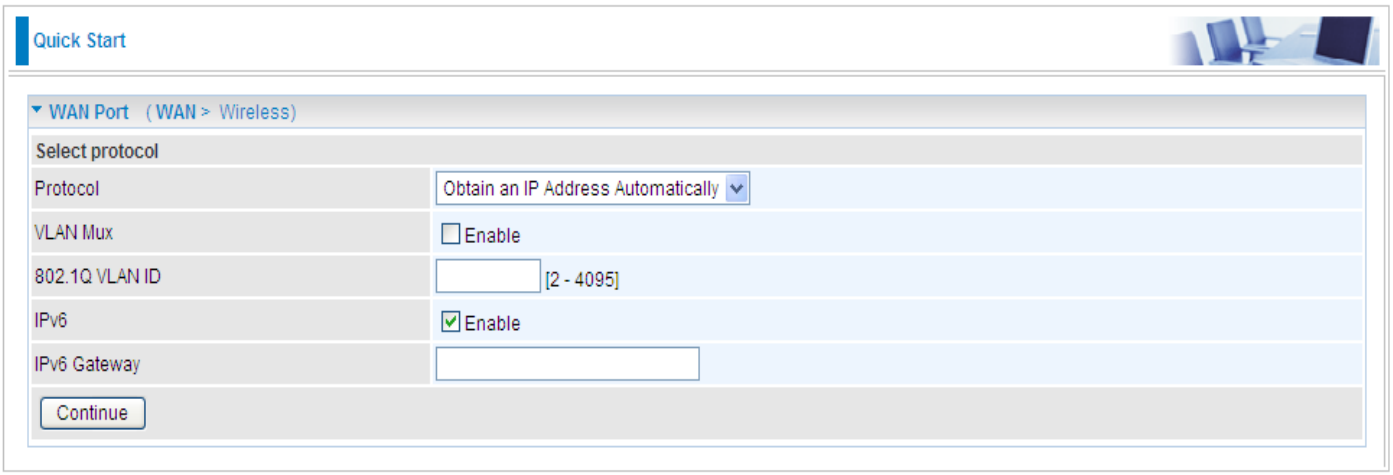


IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6

address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Obtain an IP Address Automatically



Select this protocol enables the device to automatically obtain IP address.

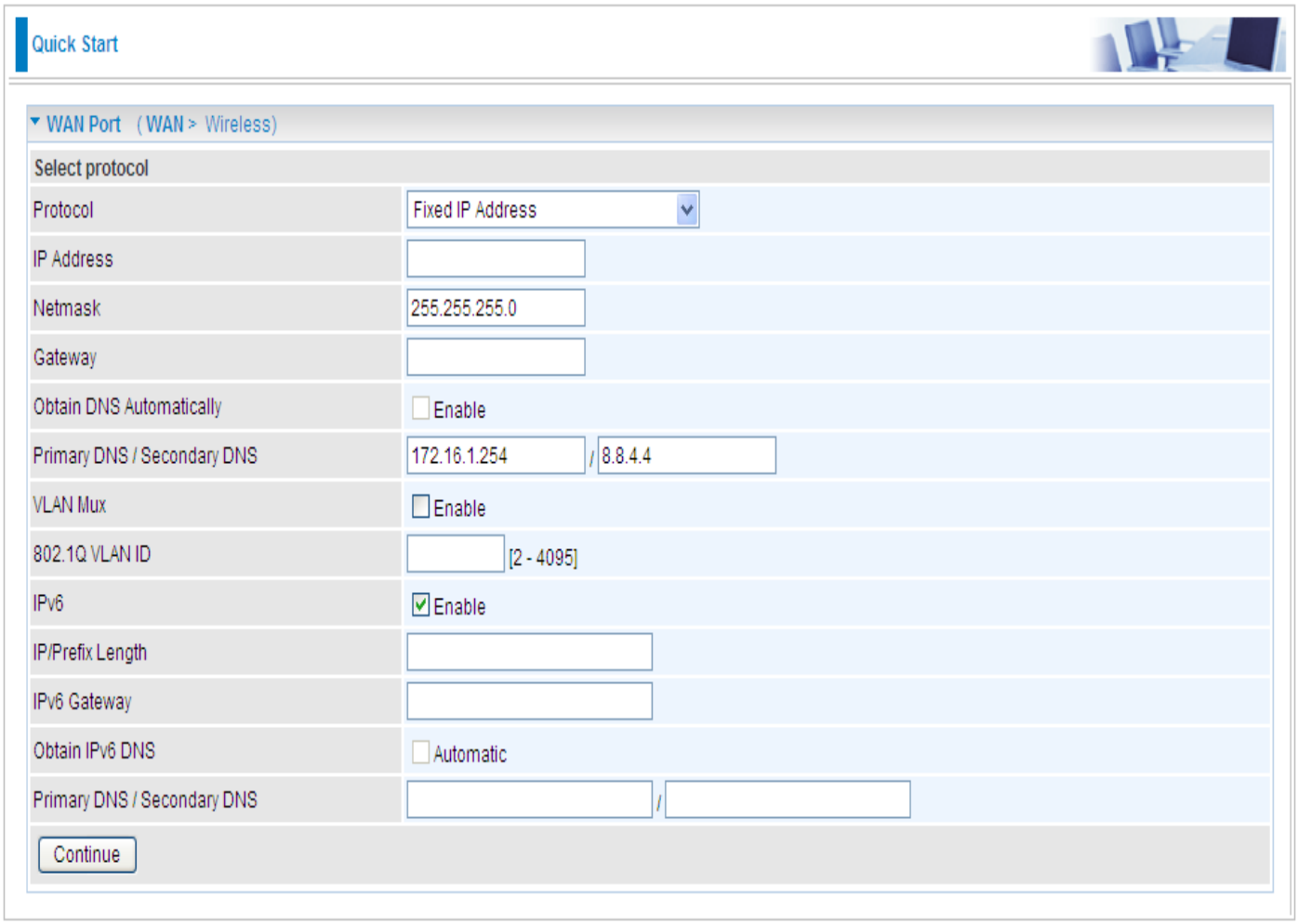
VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: Check to enble the function

IPv6 Gateway: Enter the IP address of the default IPv6 gateway.

Fixed IP Address



IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: Check to enble the function.

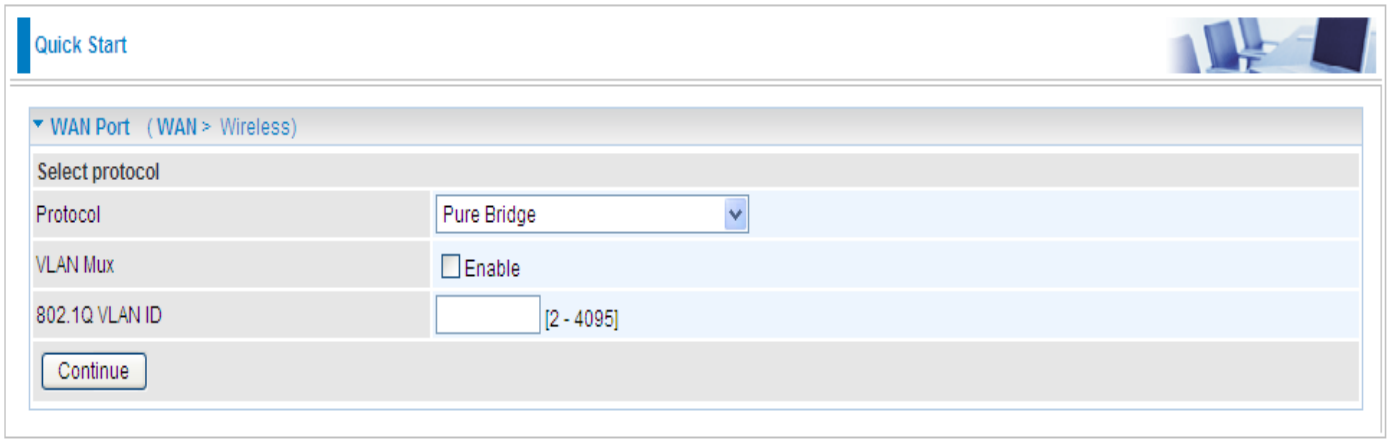
IP/Prefix Length: Enter IP Address and Prefix length.

IPv6 Gateway: Enter the IP address of the default IPv6 gateway.

Obtain IPv6 DNS: Click to activate DNS and to enable the system to automatically detect DNS.

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

Pure Bridge

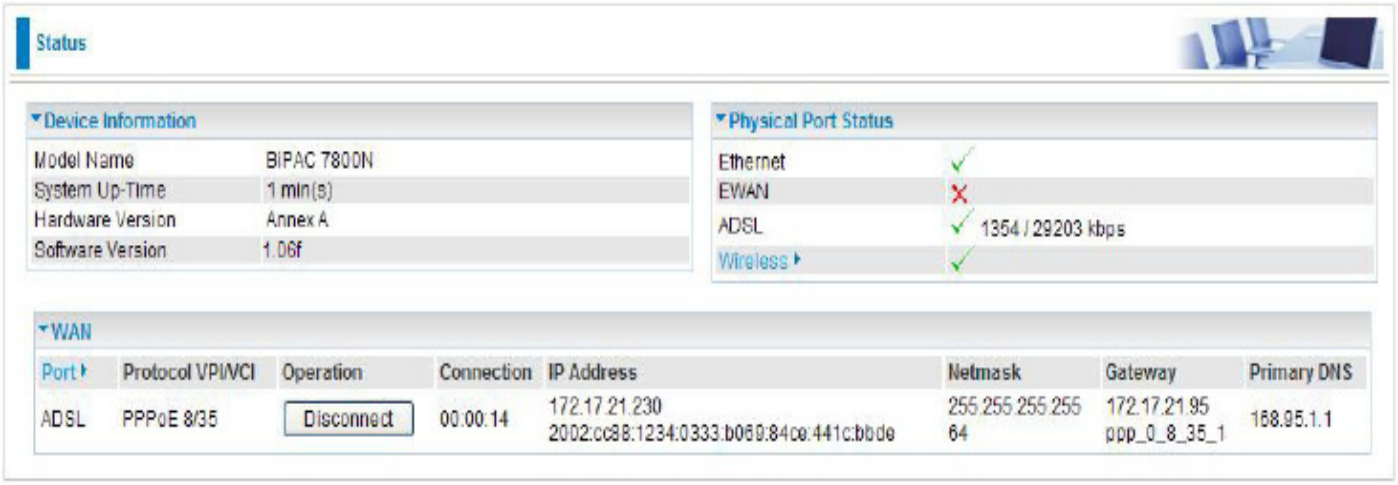


VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

Basic Configuration Mode

Status



Device Information

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

System Up-Time: Record system up-time.

Hardware Version: Device version.

Software Version: Firmware version.

Port Status

Port Status: User can look up to see if they are connected to Ethernet, EWAN, ADSL and Wireless.

WAN

Port: Name of the WAN connection.

Protocol VPI/VCI: Virtual Path Identifier and Virtual Channel Identifier.

Operation: Current status in WAN interface.

Connection: Current connection time.

IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.

Gateway: IP address of the default gateway.

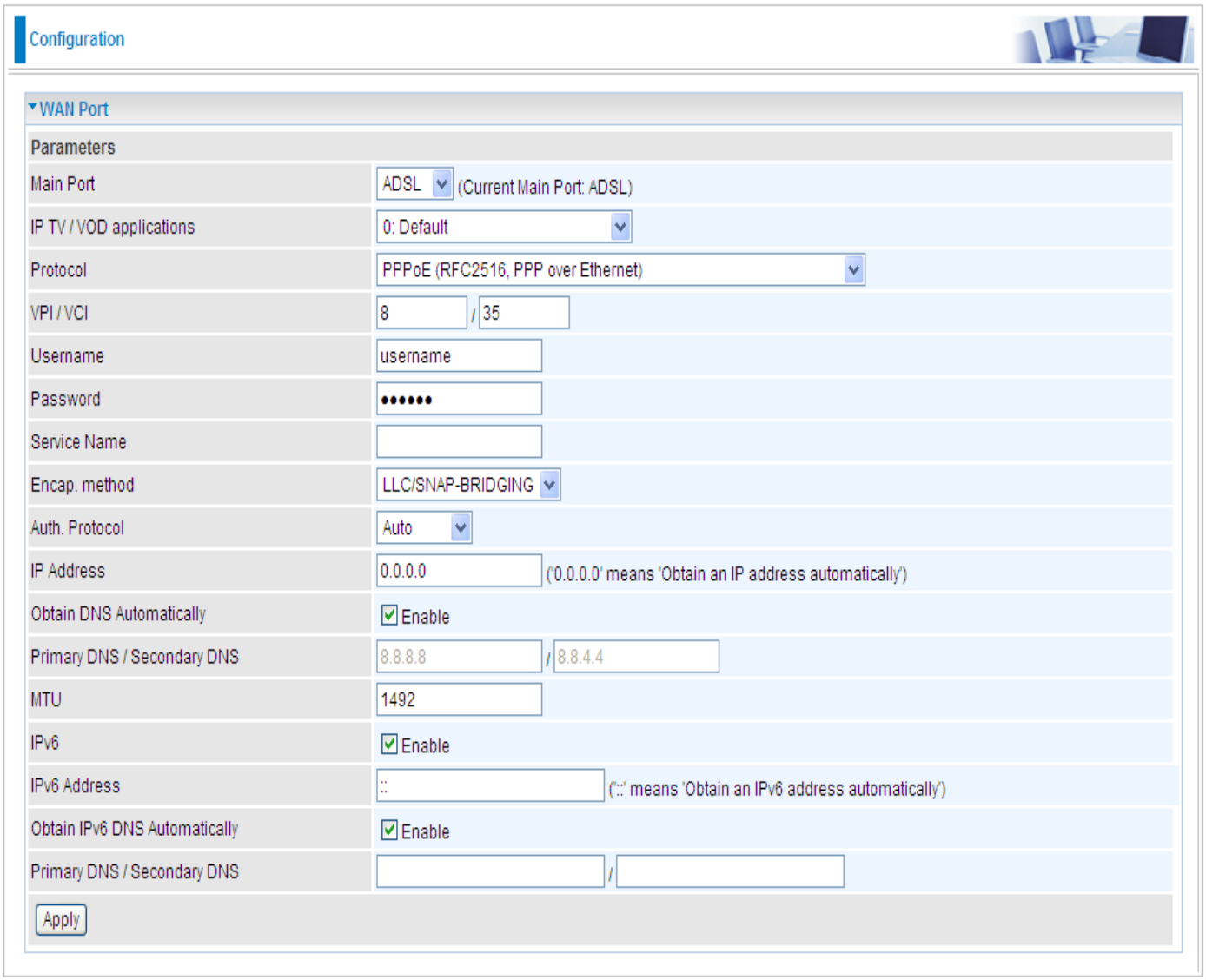
Primary DNS: IP address of the primary DNS server.

WAN – Main Port (ADSL)

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

PPPoE Connection (ADSL)

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



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

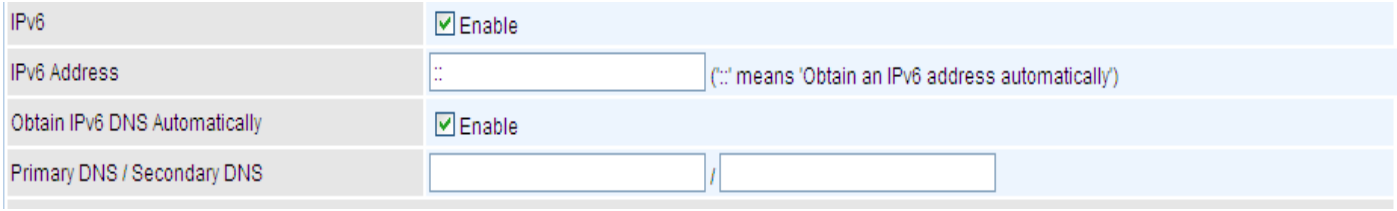
IP Address(0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

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

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ”::” means to obtain IPv6

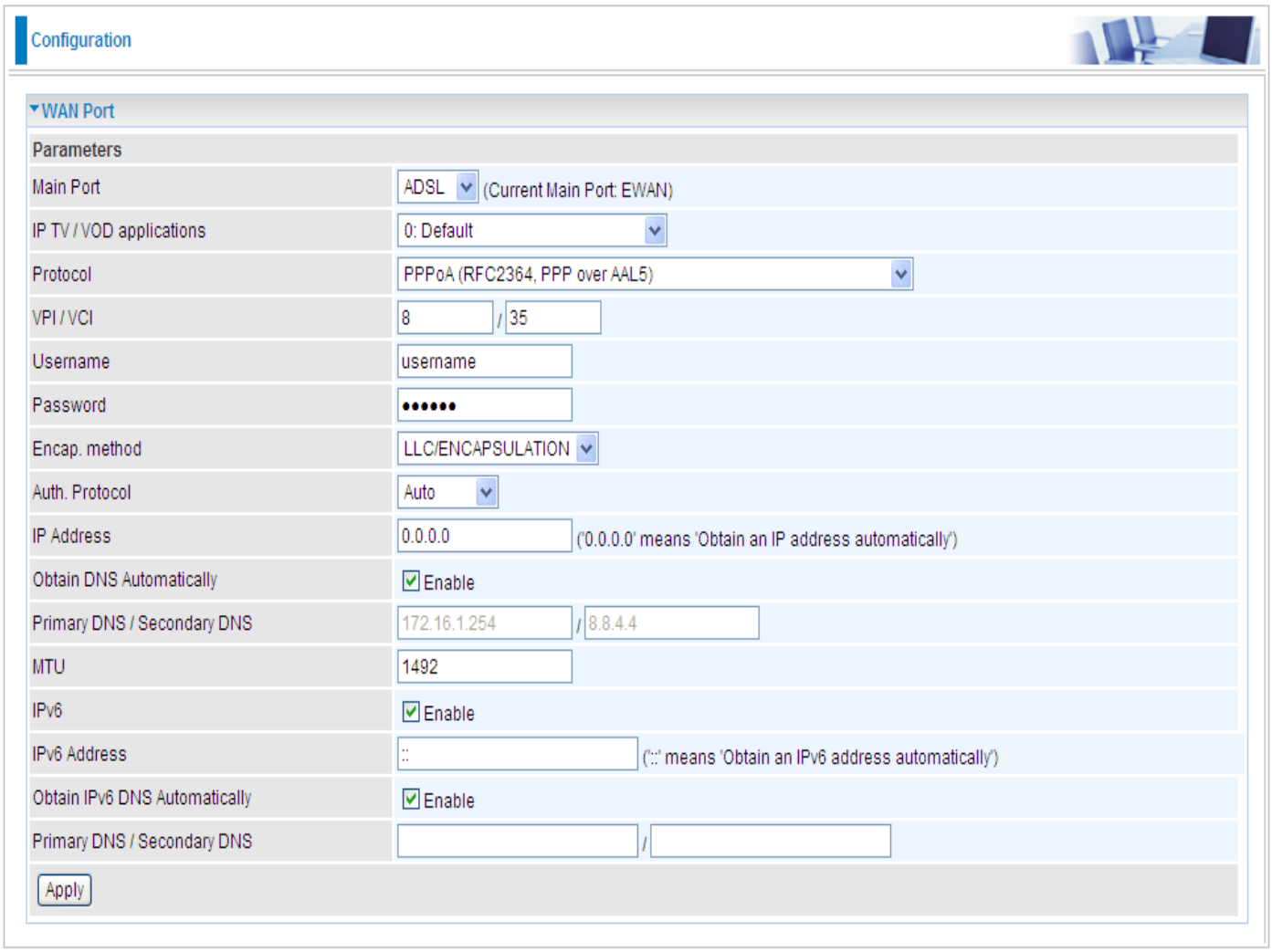
address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the exact ones in the Primary and secondary fields.

Click Apply to confirm the settings.

PPPoA Connection (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

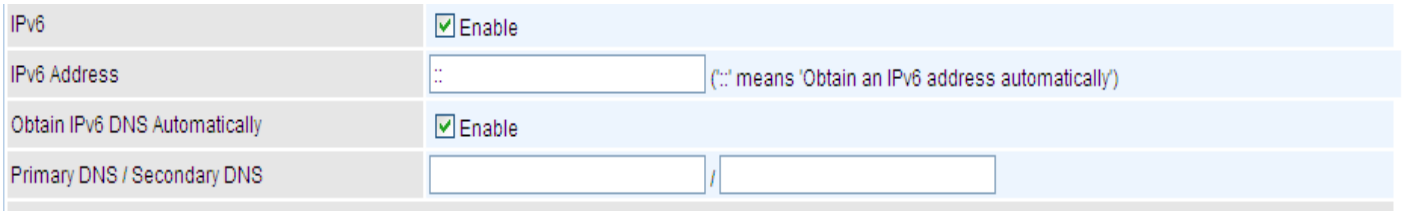
IP Address(0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

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

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.

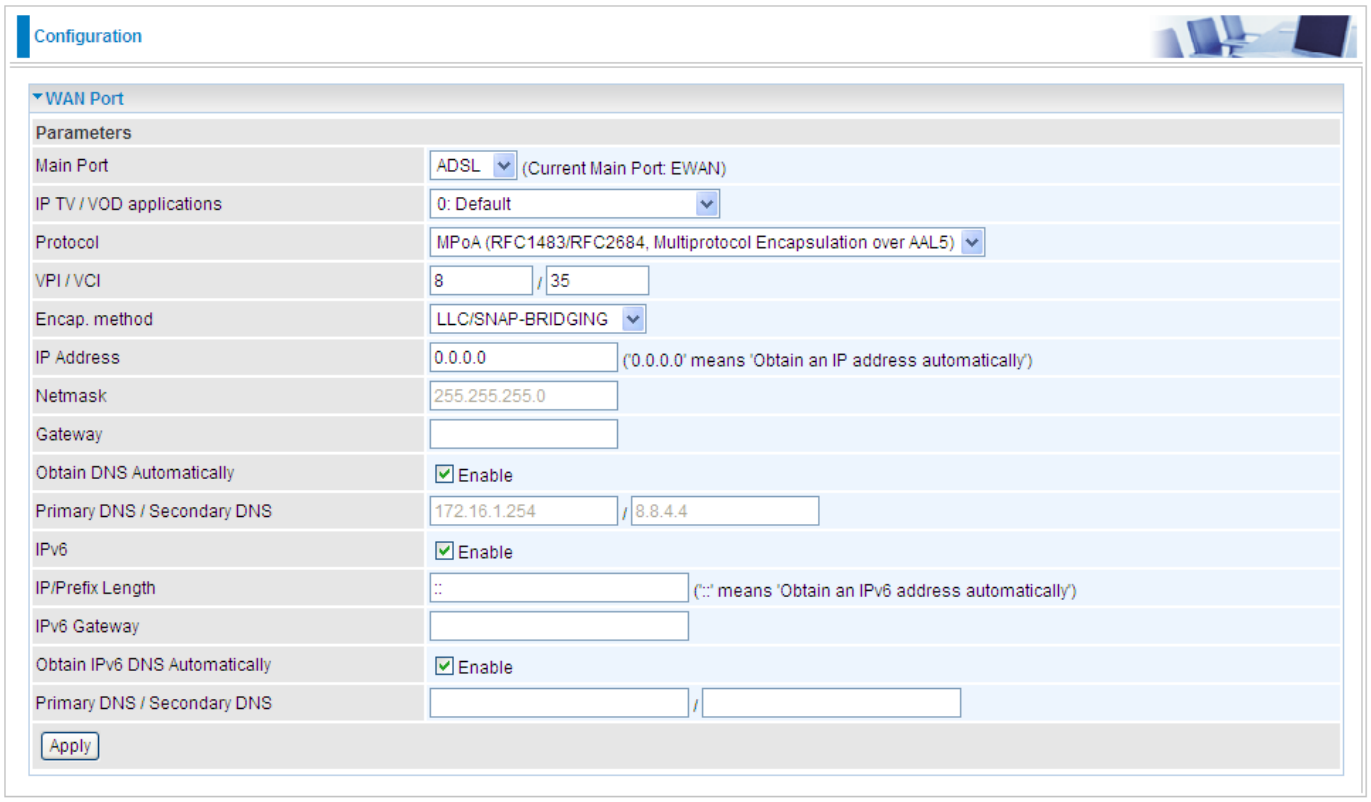


IPv6 Address: type the IPv6 address from your ISP, or get it automatically. "::" means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the exact ones in the Primary and secondary fields.

Click Apply to confirm the settings.

MPoA Connection (ADSL)



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

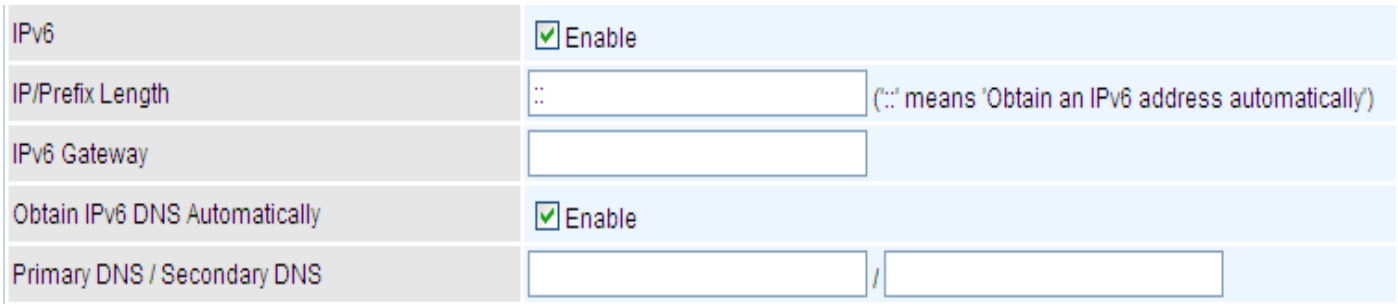
Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



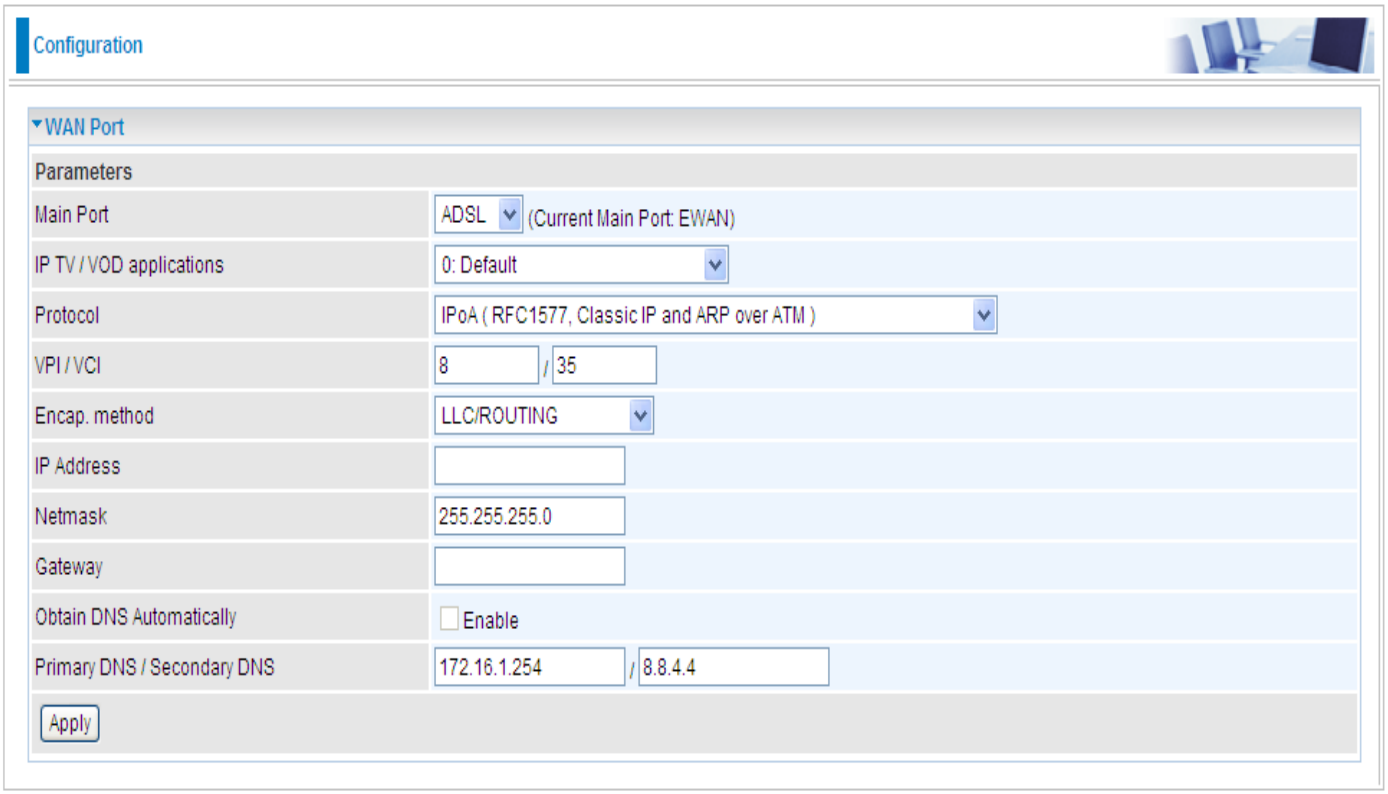
IP/Prefix Length: please type the IP and the prefix length for the IPv6 address from your ISP.

IPv6 Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Click Apply to confirm the settings.

IPoA Connections (ADSL)



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

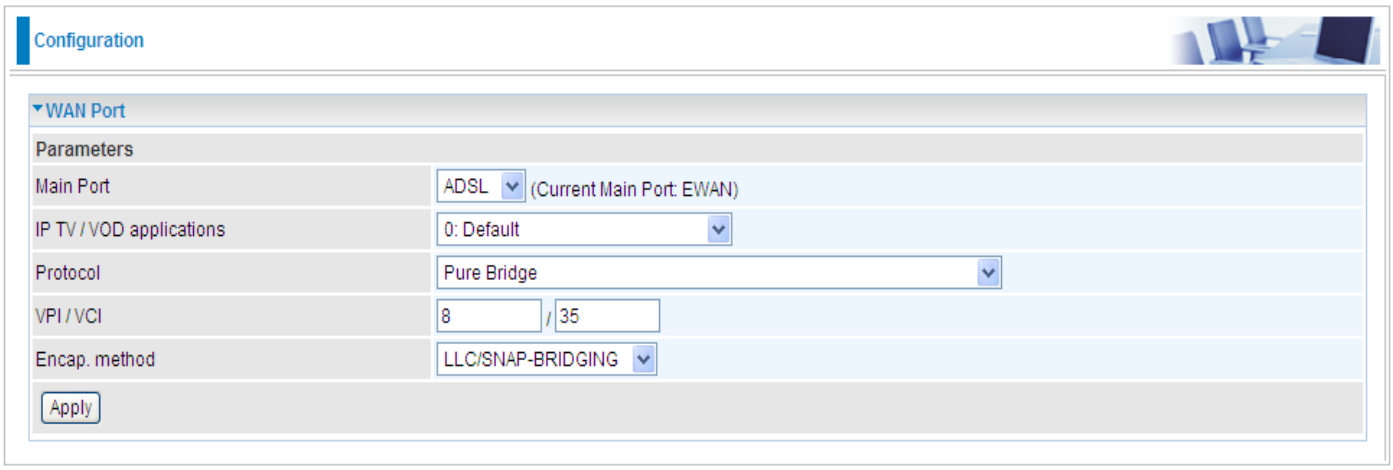
Gateway: Enter the IP address of the default gateway.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

Click Apply to confirm the settings.

Pure Bridge Connections (ADSL)



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

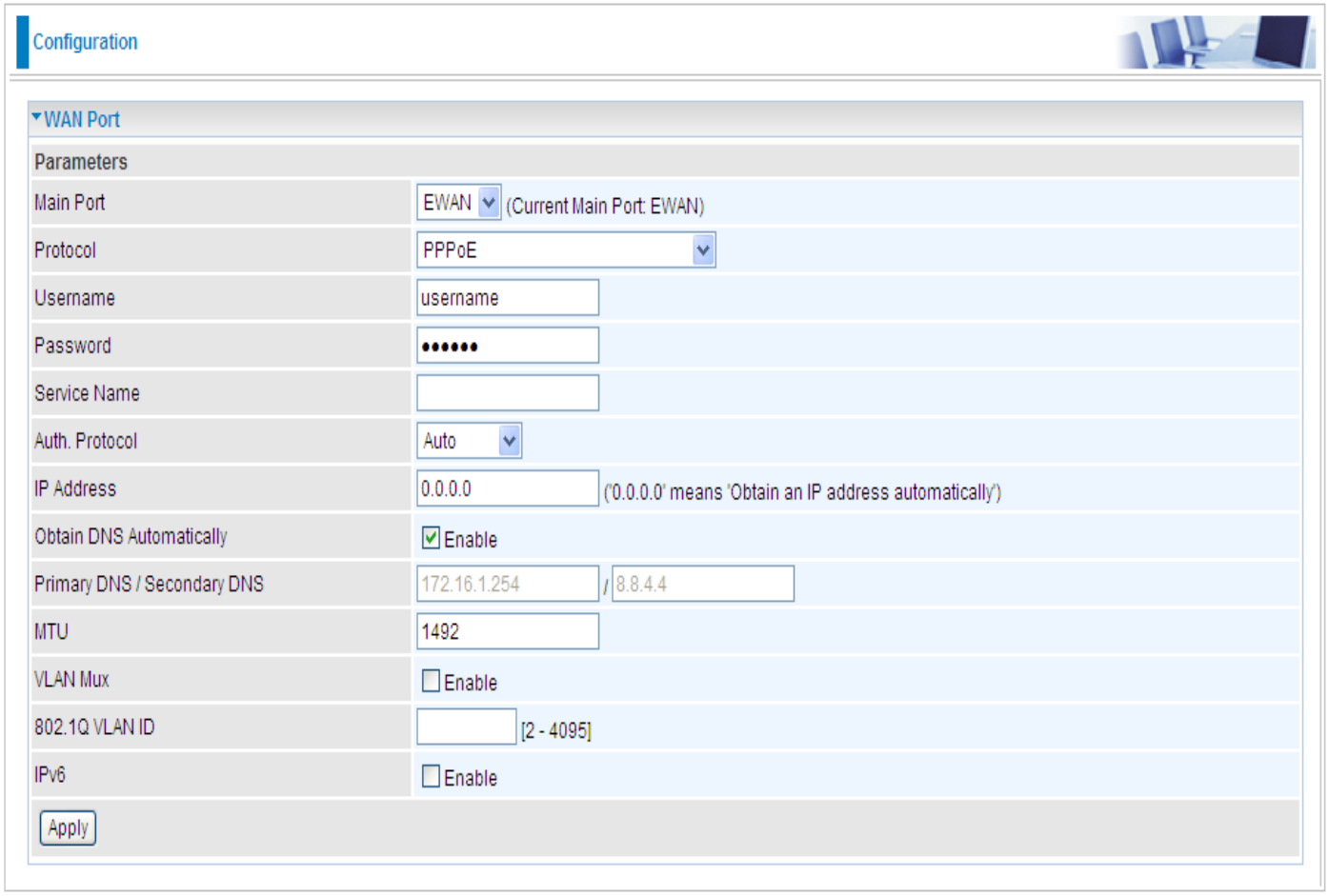
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Click Apply to confirm the settings.

WAN – Main Port (EWAN)

Besides using ADSL to get connected to the Internet, EWAN port of BiPAC 7800(N) can be used as an alternative to connect to Cable Modems, VDSL and fiber optic lines. This alternative not only provides faster connection to the Internet, it also provides users with more flexibility to get online.

PPPoE (EWAN)



Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Enter your fixed IP address.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

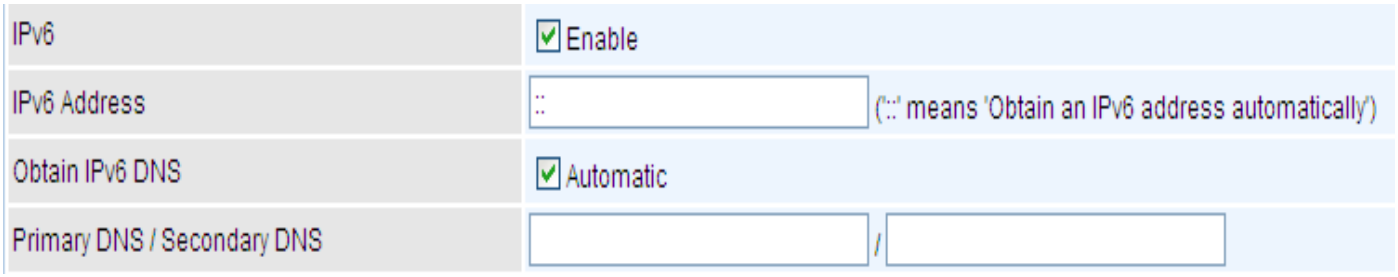
Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

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

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.



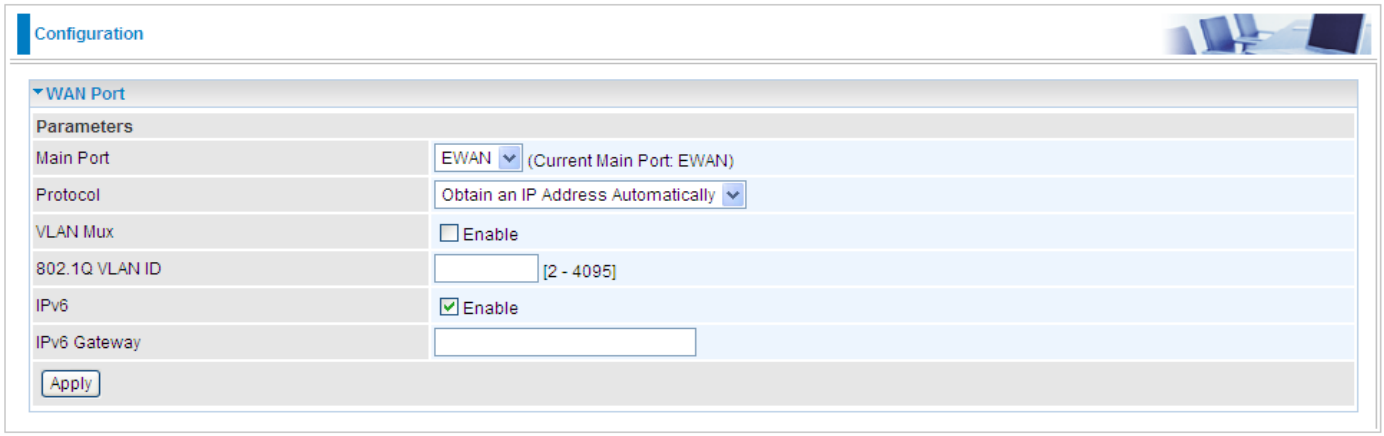
IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6

address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Click Apply to confirm the settings.

Obtain IP Address Automatically (EWAN)



Select this protocol enables the device to automatically retrieve IP address.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

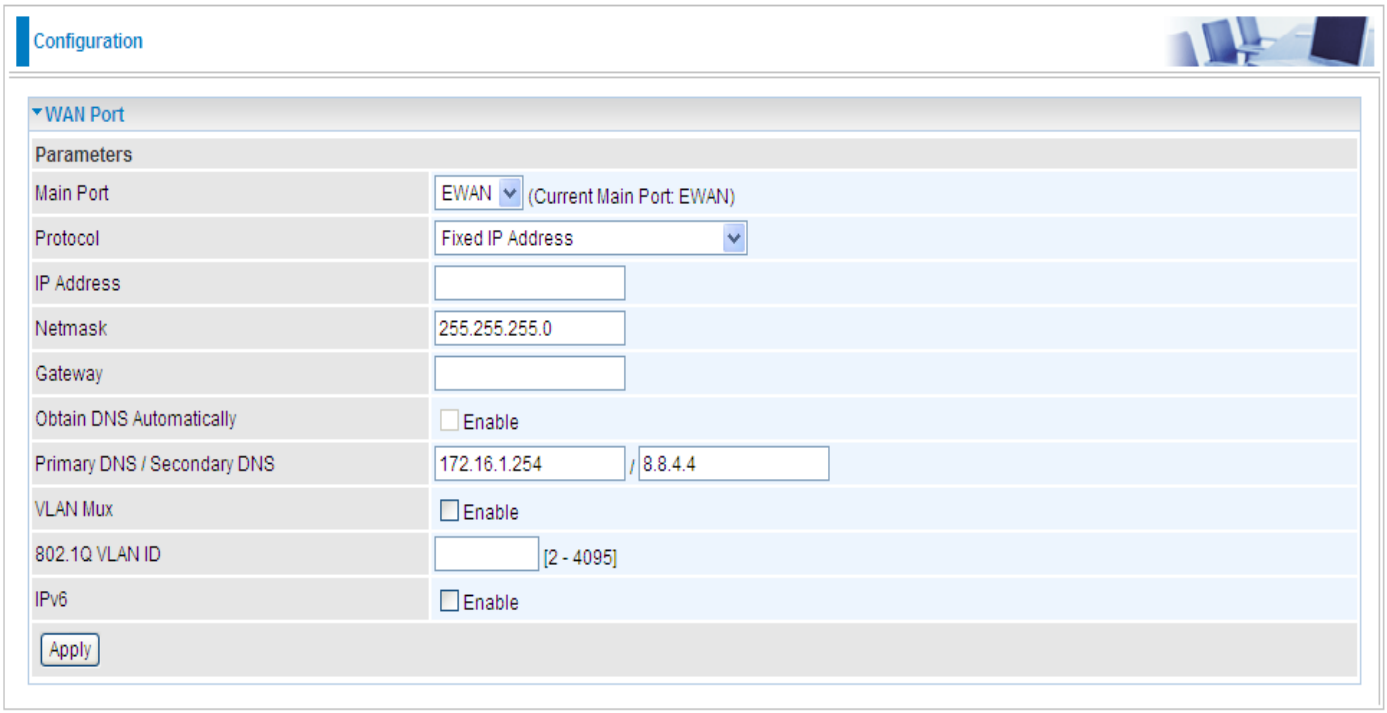
VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: Check to enble the function

IPv6 Gateway: Enter the IP address of the default IPv6 gateway.

Fixed IP Address (EWAN)



IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

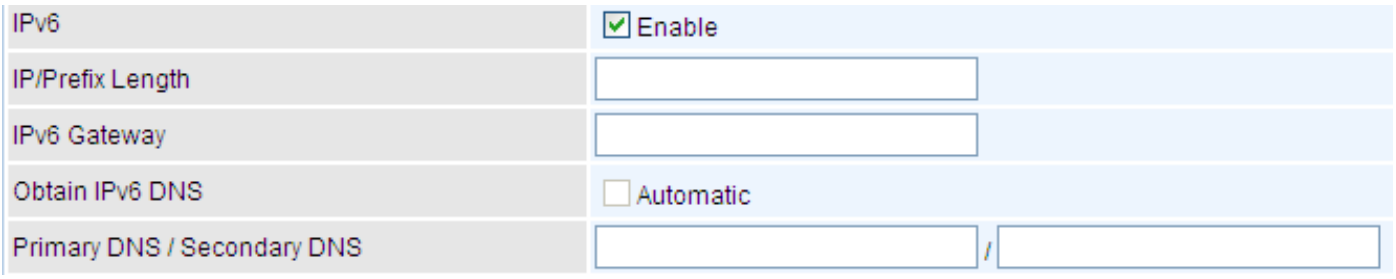
Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: Check to enble the function.

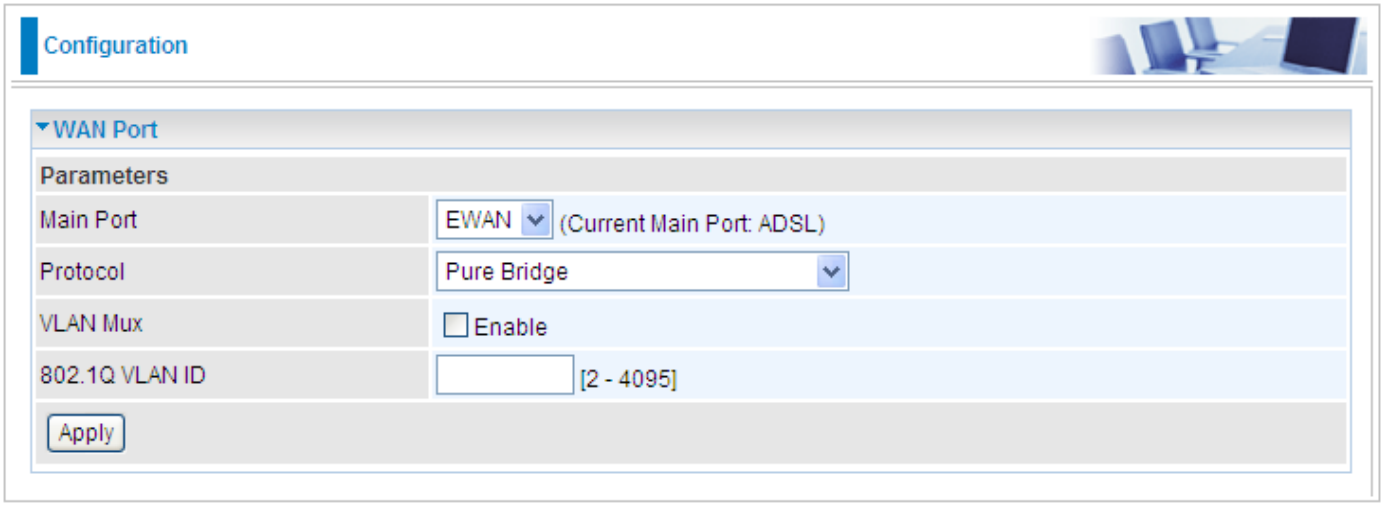


IP/Prefix Length: Enter IP Address and Prefix length.

IPv6 Gateway: Enter the IP address of the default IPv6 gateway.

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

Pure Bridge (EWAN)



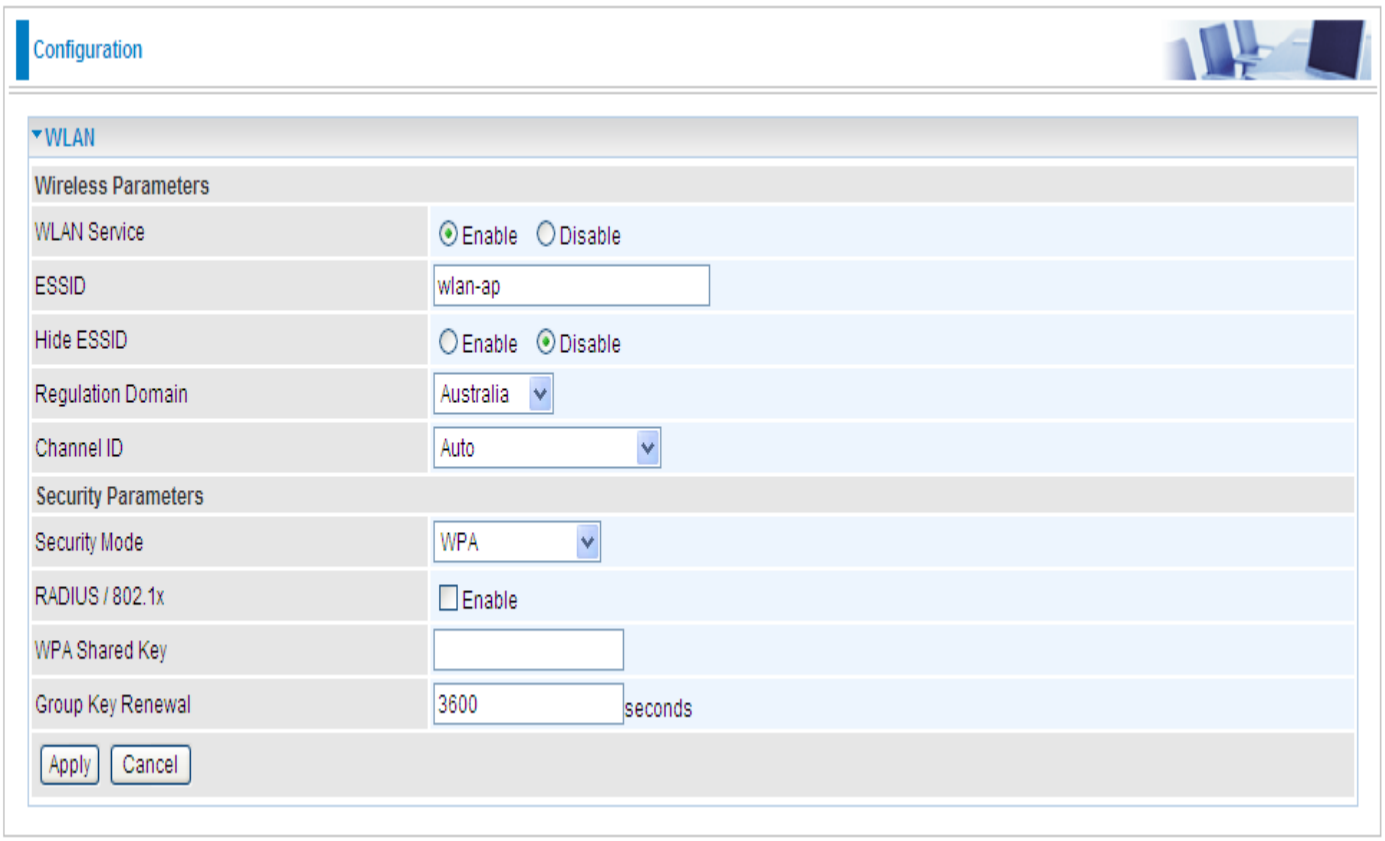
VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

Click Apply to confirm the settings.

WLAN (only for BiPAC 7800N)

WPA / WPA2



Wireless Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

Security Parameters

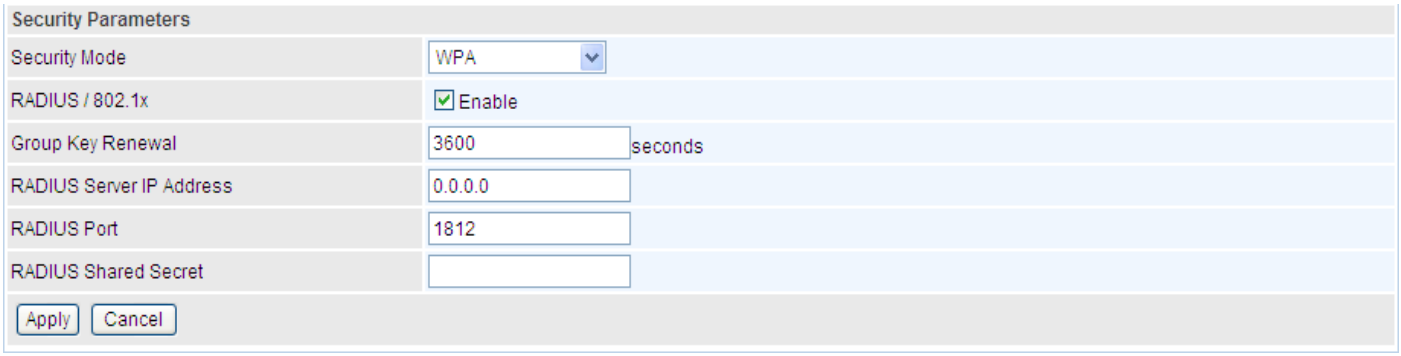
Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.

RADIUS/802.1x: You can disable or enable the RADIUS service.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3**600** seconds.

If you want to enable the RADIUS function, check **Enable** and then do the following settings.



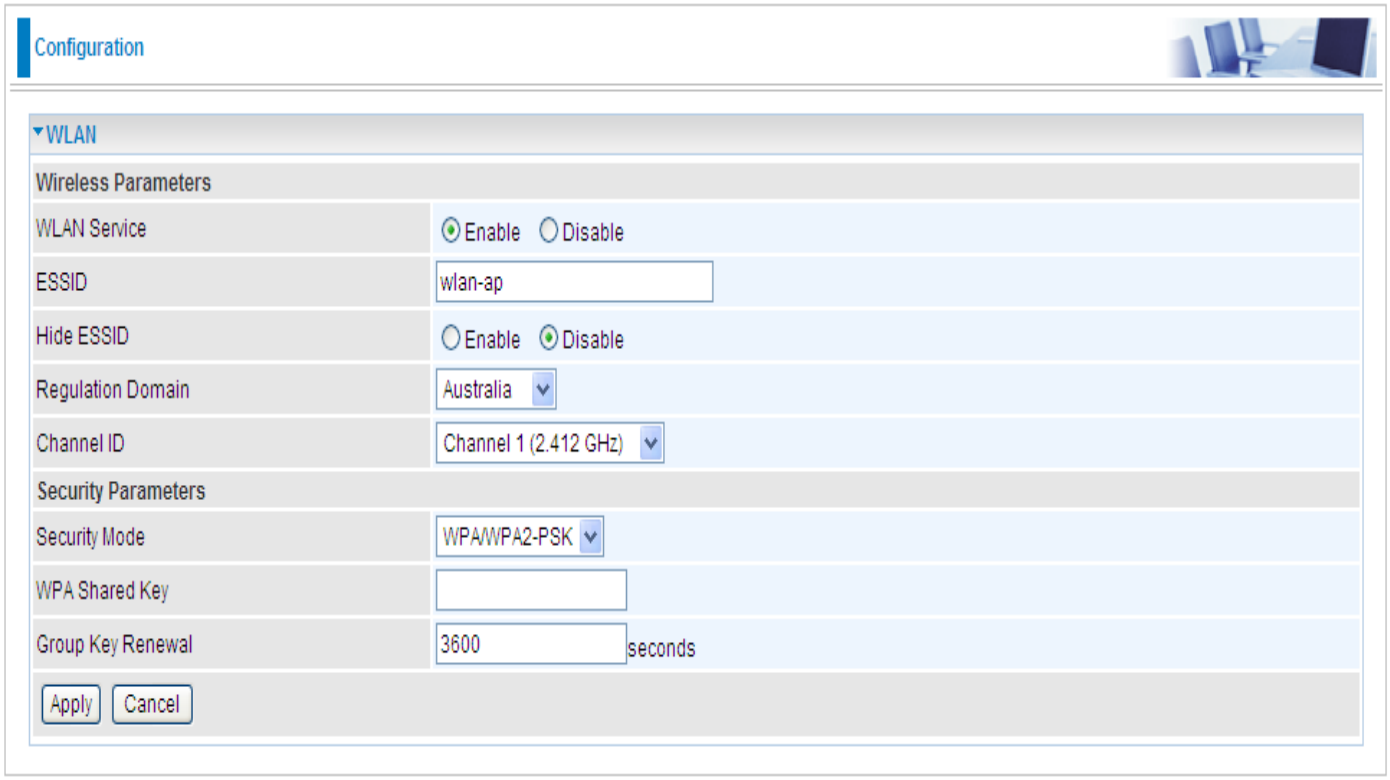
RADIUS Server IP Address: The IP address of RADIUS authentication server.

RADIUS Server Port: The port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: The password of RADIUS authentication server.

Click Apply to confirm the settings.

WPA/WPA2 Pre-Shared Key



Wireless Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

Security Parameters

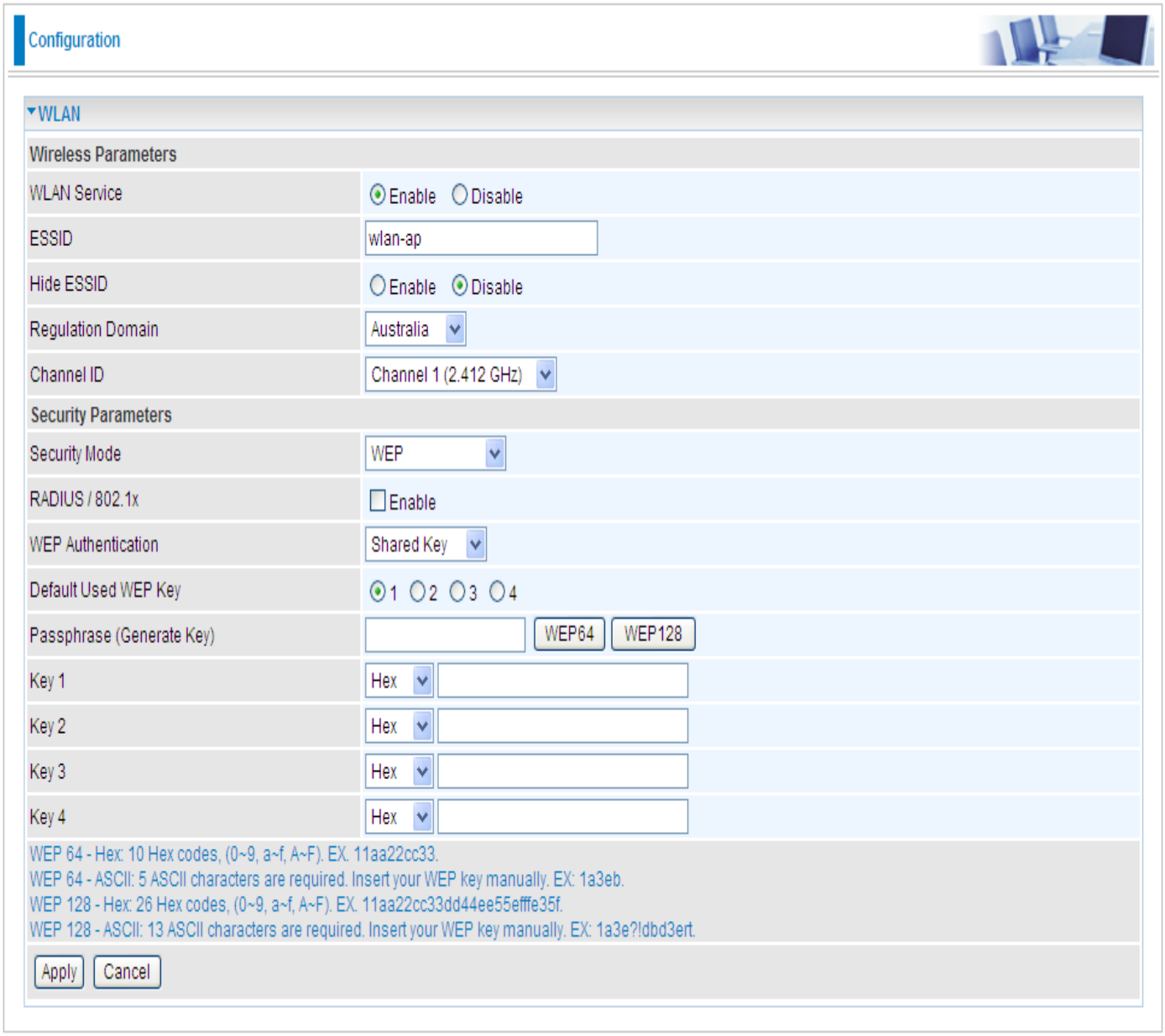
Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3**600** seconds.

Click Apply to confirm the settings.

WEP



Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

Security Parameters

Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.

RADIUS / 802.1x: You can disable or enable the RADIUS service.

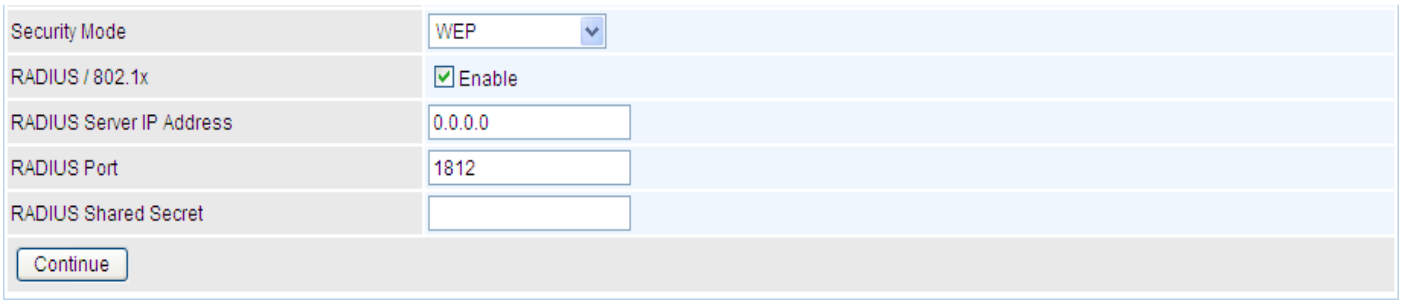
WEP Authentication: To prevent an unauthorized wireless station from accessing the data transmitted over the network, the router offers a secure data encryption, known as WEP. There are 3 options to select from: **Open System, Shared key** or **both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be either HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS function, check **Enable** and then do the following settings.



RADIUS Server IP Address: The IP address of RADIUS authentication server.

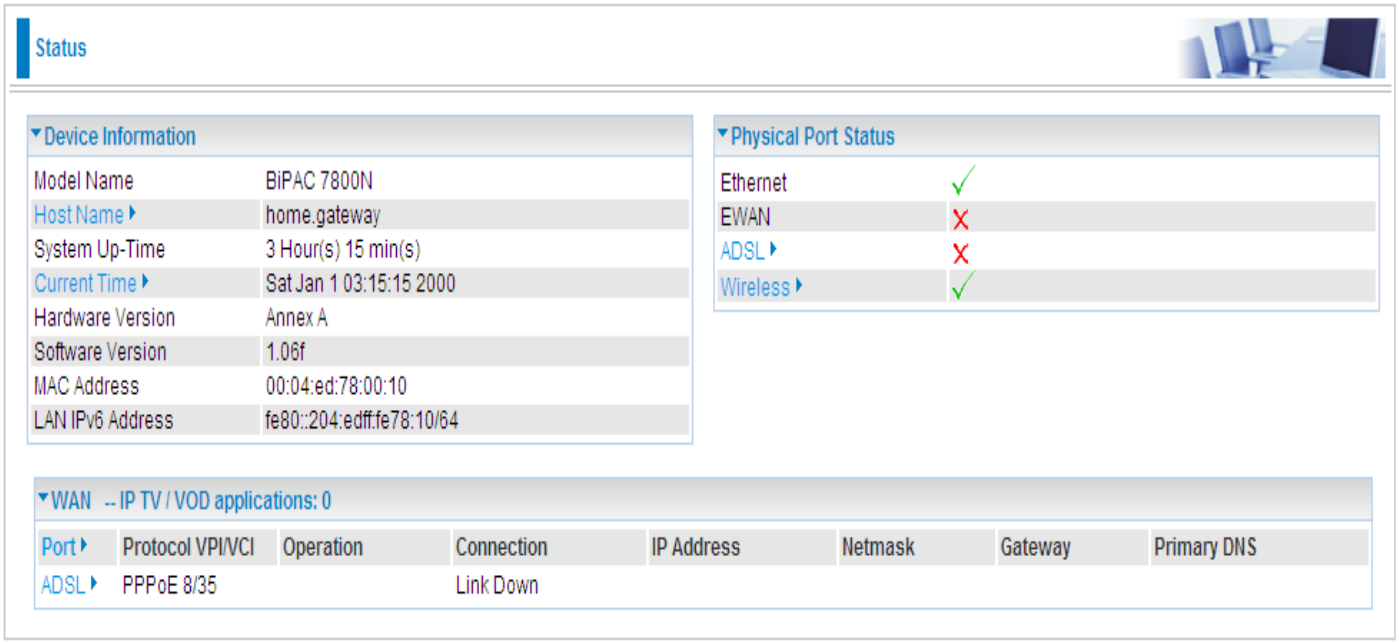
RADIUS Server Port: The port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: The password of RADIUS authentication server.

Click Apply to confirm the settings.

Advanced Configuration Mode

Status



Device Information

Model Name: Displays the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name.

System Up-Time: Records system up-time.

Current time: Set the current time. See the Time Zone section for more information.

Hardware Version: Device version.

Software Version: Firmware version.

MAC Address: The LAN MAC address.

LAN IPv6 Address: Show the IPv6 Address

Port Status

Port Status: User can look up to see if they are connected to Ethernet, EWAN, ADSL and Wireless.

WAN

Port: Name of the WAN connection.

Protocol VPI/VCI: Virtual Path Identifier and Virtual Channel Identifier

Operation: The current status in WAN interface.

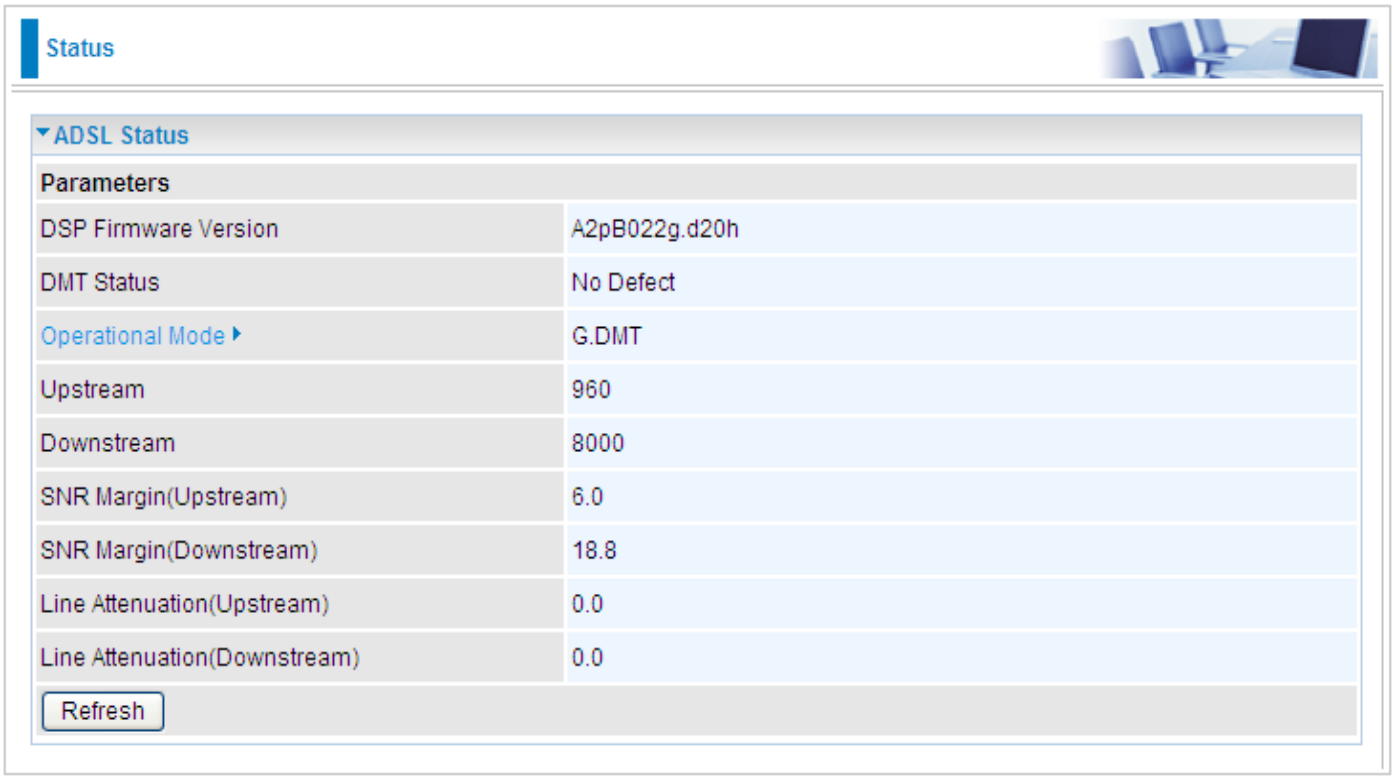
Connection: The current connection status.

IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.**Gateway:** The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

ADSL



DSP Firmware Version: DSP code version.

DMT Status: Current DMT Status.

Operational Mode: Display the ADSL state when the connect mode is set to AUTO.

Upstream: Upstream rate.

Downstream: Downstream rate.

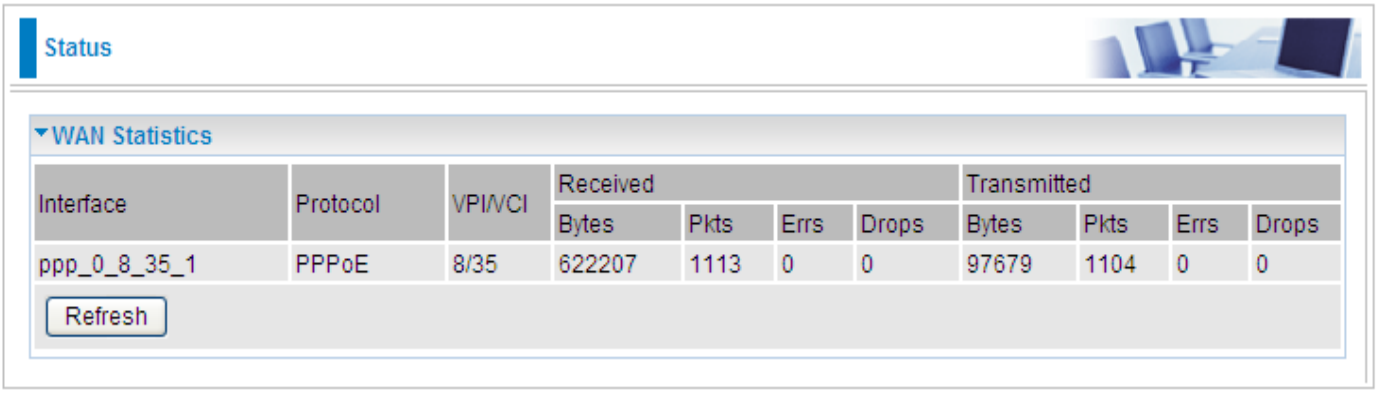
SNR Margin (Upstream): This shows the SNR margin for upstream rate.

SNR Margin (Downstream): This shows the SNR margin for downstream rate.

Line Attenuation (Upstream): This is attenuation of signal in upstream.

Line Attenuation (Downstream): This is attenuation of signal in downstream.

WAN Statistics



Protocol: Service name that is used for connection.

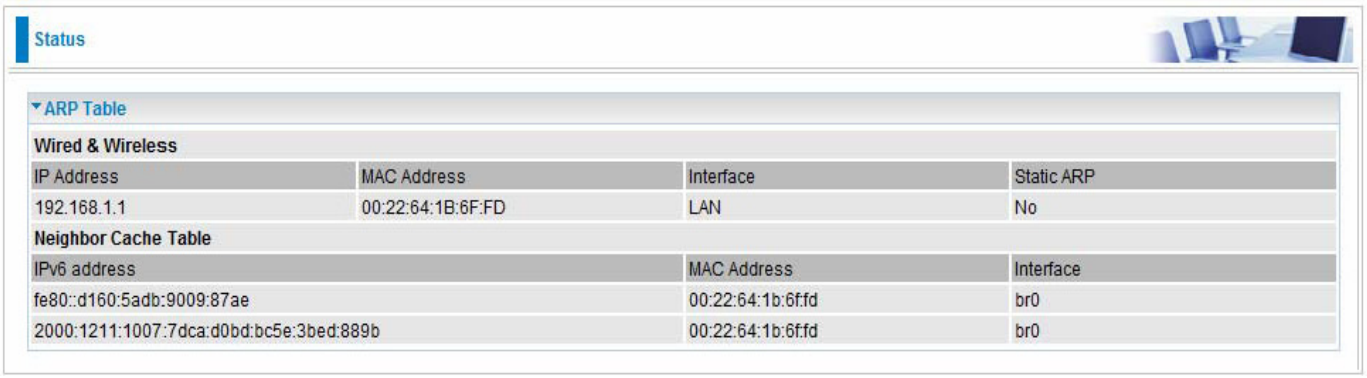
VPI/VCI: It is provided by ISP.

Received: Include received Bytes, Pkts, Errs and Drops.

Transmitted: Include transmitted Bytes, Pkts, Errs and Drops.

ARP

This table stores mapping information that the device uses to find the Layer 2 Media Access Control (MAC) address that corresponds to the Layer 3 IP address of the device via the Address Resolution Protocol (ARP) feature.



ARP Table

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

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

Interface: The interface name (on the router) that this IP address connects to.

Static ARP: Shows the status of static ARP.

Neighbor Cache Table

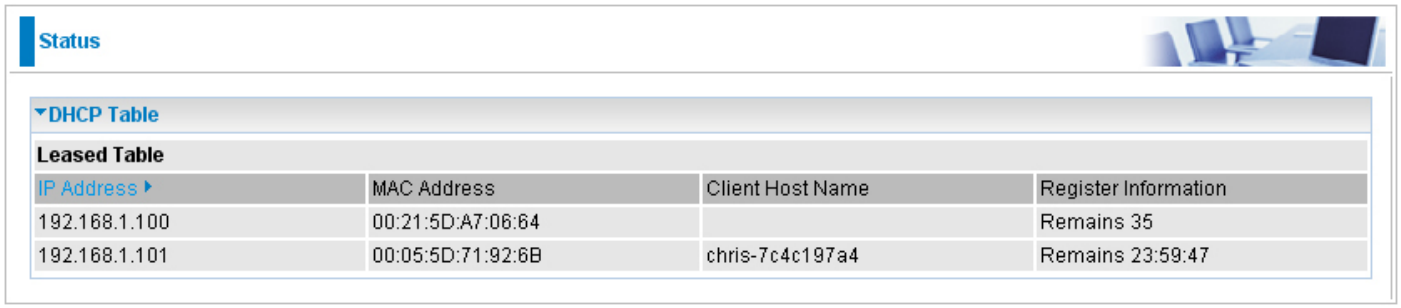
IPv6 address: Shows the IPv6 Address of the device that the MAC address maps to.

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. For example, the Clients in LAN, here displays “br0”.

DHCP

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



IP Address: This is the IP address that is assigned to the host with this MAC address.

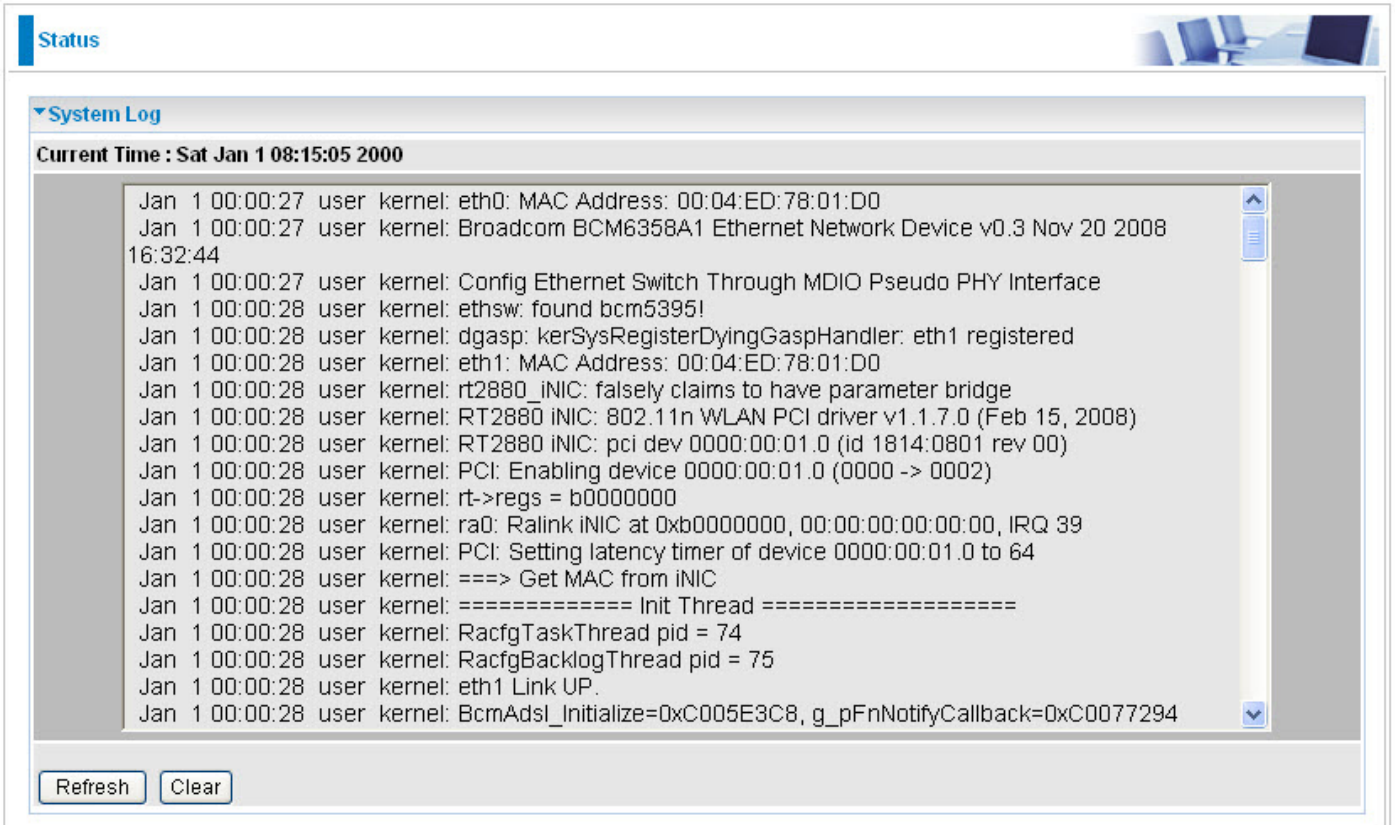
MAC Address: The MAC Address of internal dhcp client host.

Client Host Name: The Host Name of internal dhcp client.

Register Information: Shows the information provided during registration.

System Log

Display system logs accumulated up to the present time. You can trace its historical information with this function.



Refresh: Click to update the system log.

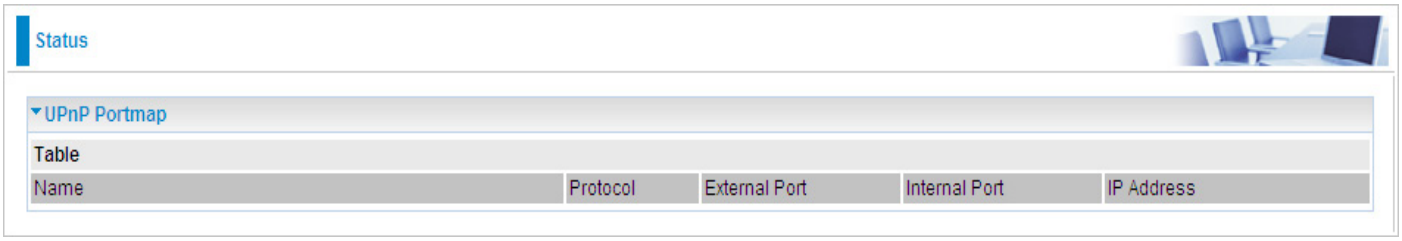
Clear: Click to clear the current log from the screen.

Firewall Log

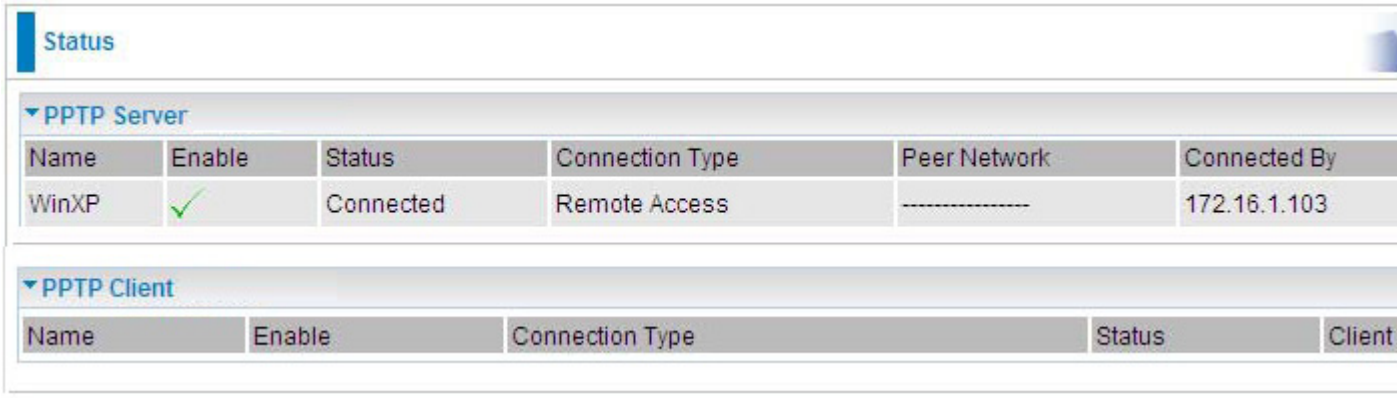
Firewall Log displays a log that contains information of any unexpected actions that occur to your firewall settings.

UPnP Portmap

This section lists all the established port-mapping using UPnP (Universal Plug and Play). See the Advanced section of this manual for more details on UPnP and the router UPnP configuration options.



PPTP Satus



PPTP Client

Name: the name for your PPTP Client connection.

Enable: Whether the PPTP connection is currently Enable or not.

Connection Type: Whether the Connection type is Remote Access or LAN to LAN.

Status: Displays Not Connected or Connected.

Client IP: Assigned by PPTP server.

PPTP Server

Name: The name you assigned to the particular PPTP entry.

Enable: Whether the PPTP connection is currently Enable or Disable.

Status: Whether the PPTP is Active, Inactive or Disable.

Connection Type: Whether the Connection type is Remote Access or LAN to LAN.

Peer Network: The Remote subnet for LAN to LAN as connection type.

Connect by: The remote address when connected.

Action: Manually drop the tunnel.

Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your GPON router.

LAN, **WAN**, **System**, **Firewall**, **QoS**, **Virtual Server, Wake on LAN, Certificate, Time Schedule** and **Advanced**.

The function of each configuration sub-item is described in the following sections.

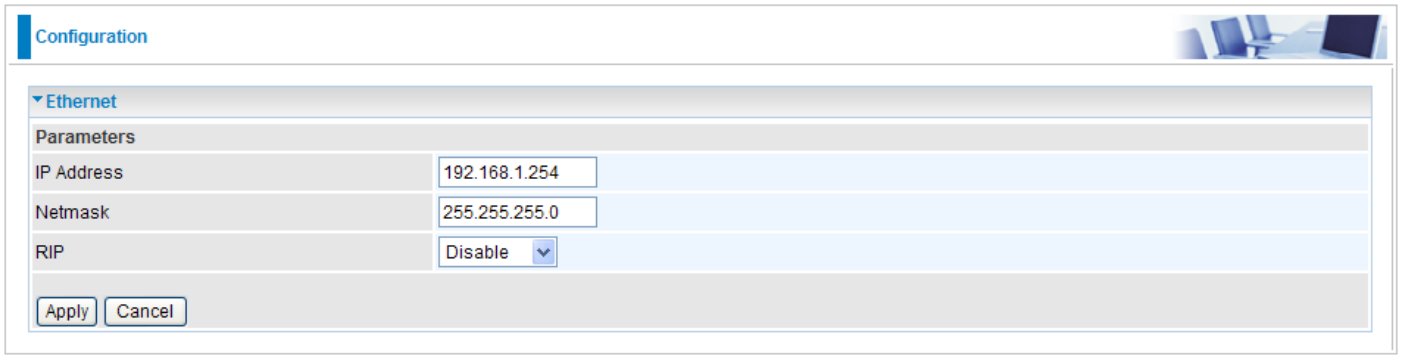
LAN

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 or just within the same storey of a building. There are 5 items within the LAN section: **Ethernet**, **IP Alias**, **IPv6 Autofconig**, **Wireless (7800N only)**, **Wireless Security (7800N only)**, **WPS(7800N only)** and **DHCP Server**.

Ethernet

The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.

IP Address: The default IP on this router.



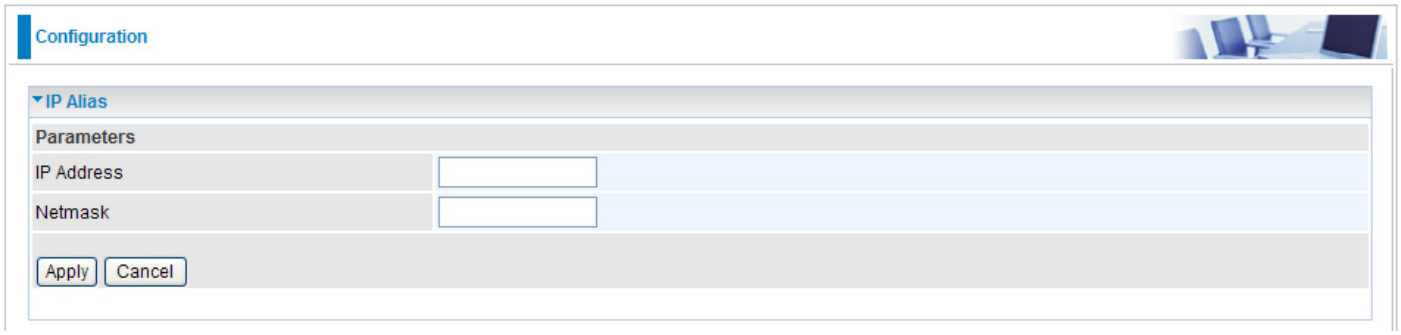
Netmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2 & RIP v1+v2.

Click Apply to confirm the settings.

IP Alias

This function allows the addition an IP alias to the network interface. This further allows user the flexibility to assign a specific function to use this IP.



IP Address: Enter the IP address to be added to the network.

Netmask: Specify a subnet mask for the IP to be added.

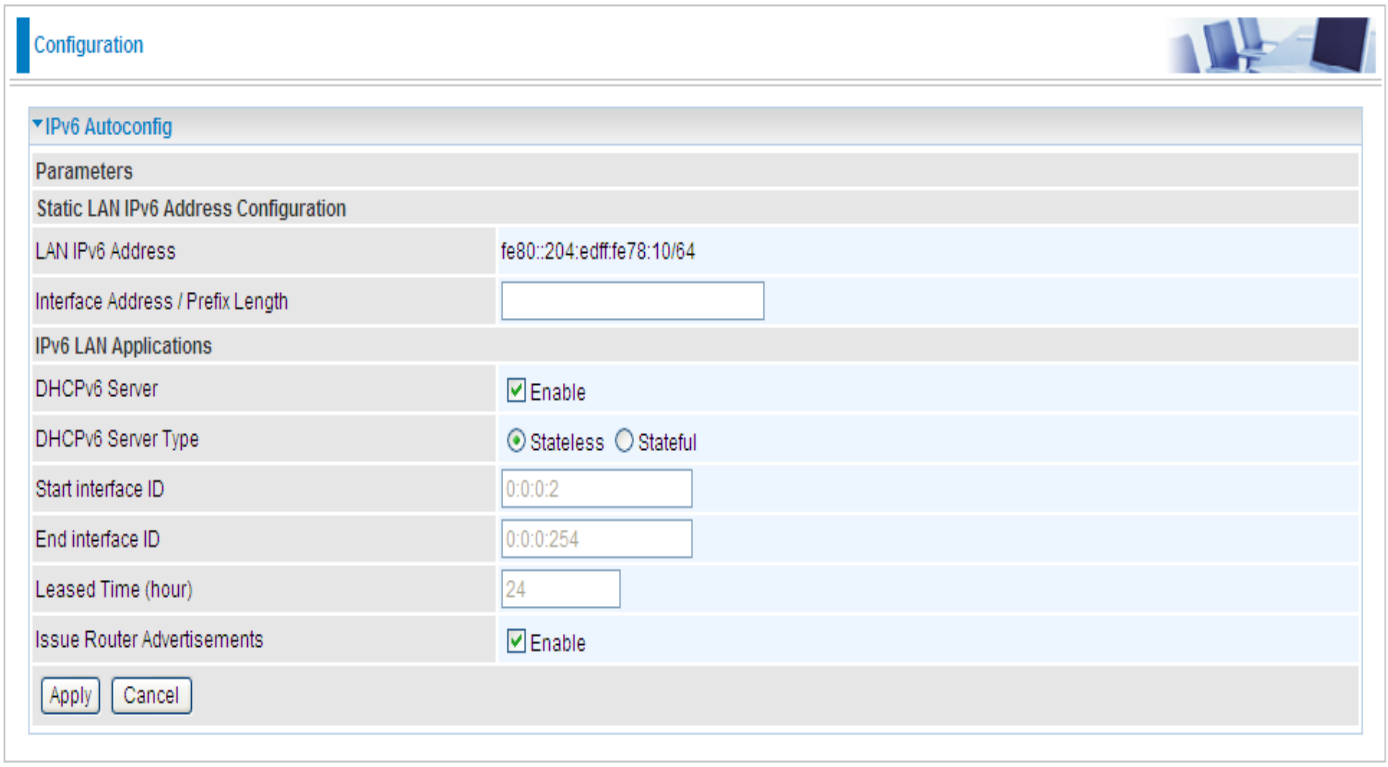
Click Apply to confirm the settings.

IPv6 Autoconfig

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

There are two ways to dynamically configure IPv6 address on hosts. One is statefull configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful autoconfiguration 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.



Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: enter the static LAN IPv6 address, we suggest leave the field empty because when setted wrong, it will result in LAN devices not being able to access other IPv6 device through internet. Router will take the same WAN's prefix to LAN side if the field is empty.

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

from DHCPv6 server.

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.

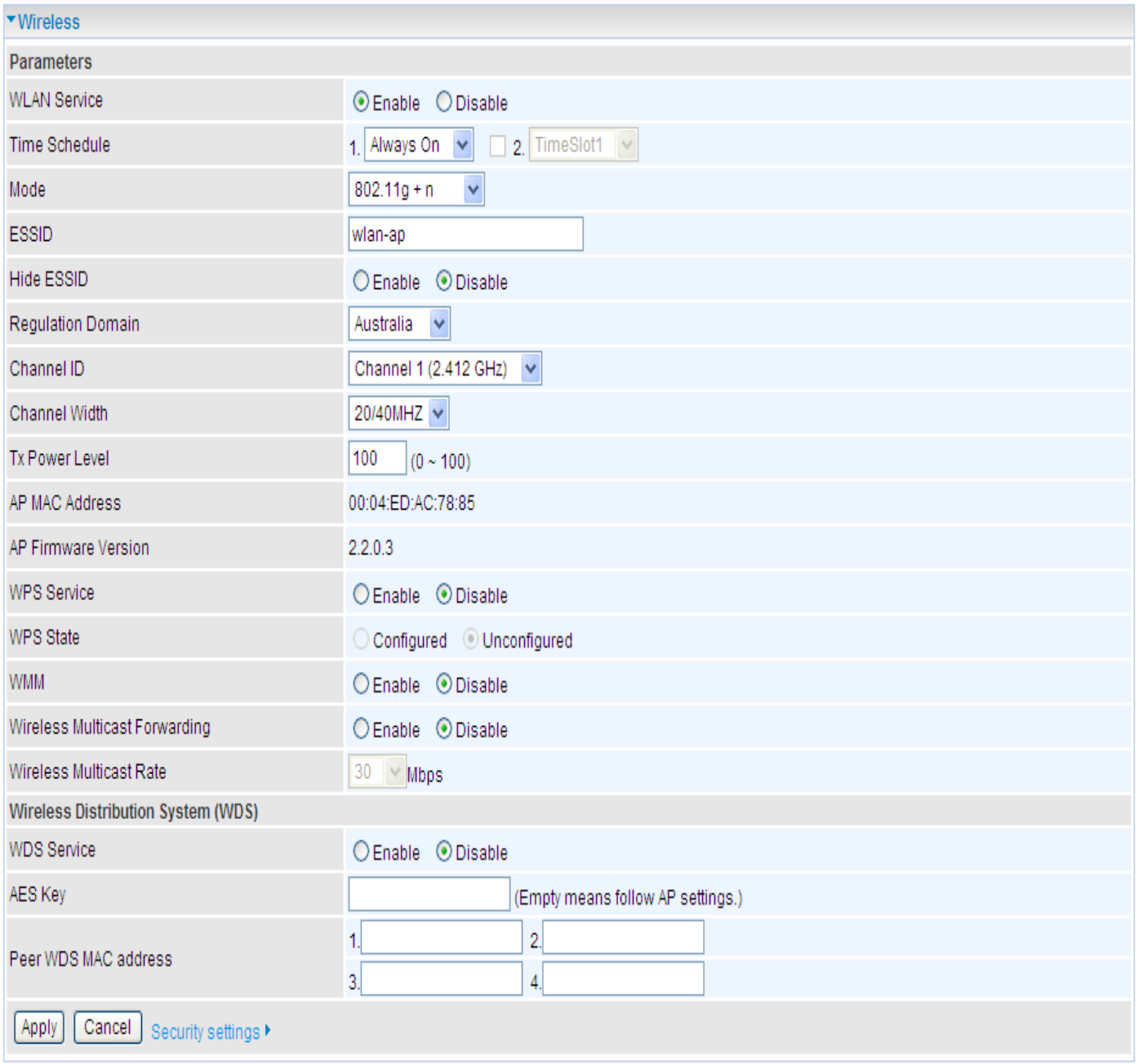
Note: Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.

For example: Please enter "0:0:0:2" instead of "::2".

Leased Time (hour): the leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, 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. Router will multicast the v6 Prefix information (similar to v4 network number 192.168.1.0) to all LAN devices if the field is enabled. We suggest enabling this field.

Wireless (only for BiPAC 7800N)



Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable. Time Schedule:

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy.

Here we provide two groups of Time Schedule setting. You can flexibly set the time you want the wireless connection works.

If you select Always On in group1, then the group2 is disabled.

While if you select any other item from the group1 drop-down menu, the group2 will be activated.

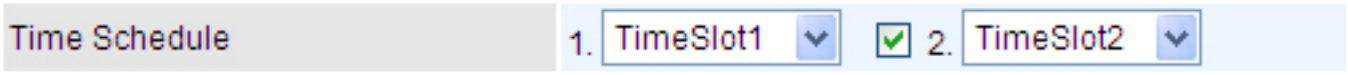
Select the timeslot you want, then the wireless will work according to the time of the two time schedule settings. You can set two timeslots, let wireless works to the two timeslots time you set.

For example: you want your wireless to work at 08:00-18:00 Sunday and 01:00-02:00 Monday, you

can set like this:

TimeSlot1	Smtwtfs	08:00	18:00
TimeSlot2	sMtwtfs	01:00	02:00

the timesolts



setting

For timeslots setup and detail, refer to Time Schedule section.

Mode: The default setting is 802.11g+n. If you do not know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b. And if you have 11n card, you can select 802.11n.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

Channel width: Select either 20 MHz or 20/40 MHz for the channel bandwidth. The higher the bandwidth the better the performance will be.

TX PowerLevel: It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: The Power Level maybe different in each access network user premise environment, choose the most suitable level for your network.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

WPS Service: Select Enable if you would like to activate WPS service.

WPS State: This column allows you to set the status of the device wireless setting whether it has been configured or unconfigured. For WPS configuration please refer to the section on **Wi-Fi Network Setup** for detail.

WMM: This feature is used to control the prioritization of traffic according to 4 Access categories:

Voice, Video, Best Effort and Background. Default is set to disable.

Wireless Multicast Forwarding: select Enable to enbale wireless multicasr forwarding feature. Then you can set the wireless multicast rate to give control to wireless multicast.

Wireless Multicast Rate: specifies the rate at which multicast packets are transmitted by the access point on your wireless network. Specifying a high multicast rate may improve performance of multicast features.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantages of the cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

WDS Service: The default setting is **Disabled.** Check **Enable** radio button to activate this function.

1. **Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
2. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.
3. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

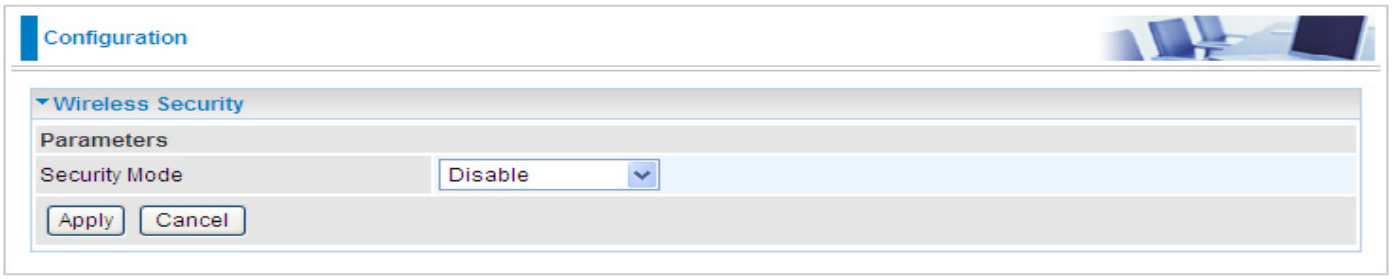
Note: For MAC Address, the format can be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click Apply to confirm the settings.

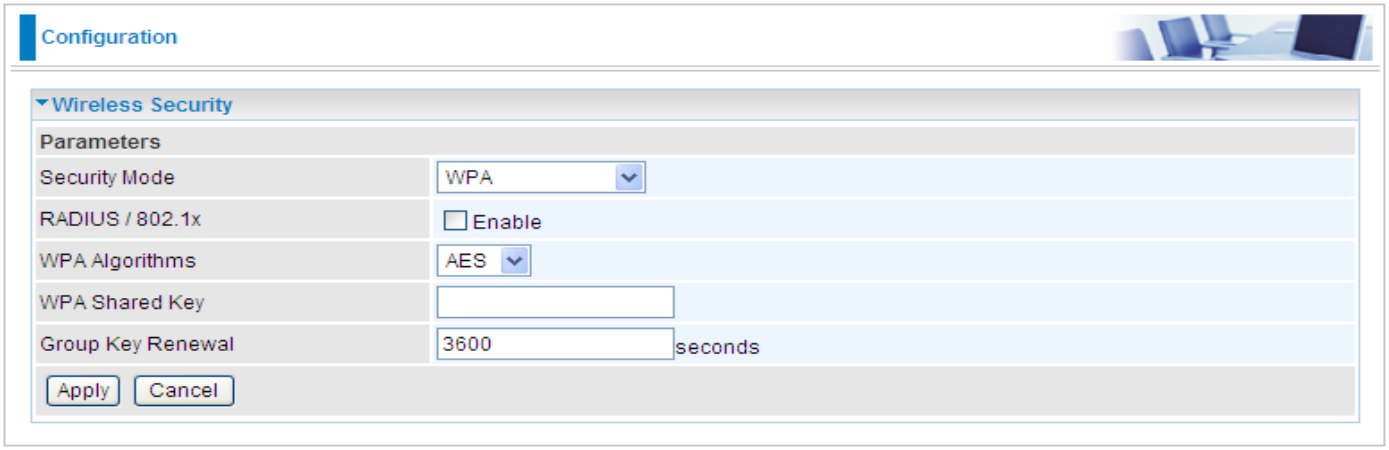
You can click Security settings link next to Cancel button to go to Wireless Security screen (see **Wireless Security** section).

Wireless Security (only for BiPAC 7800N)

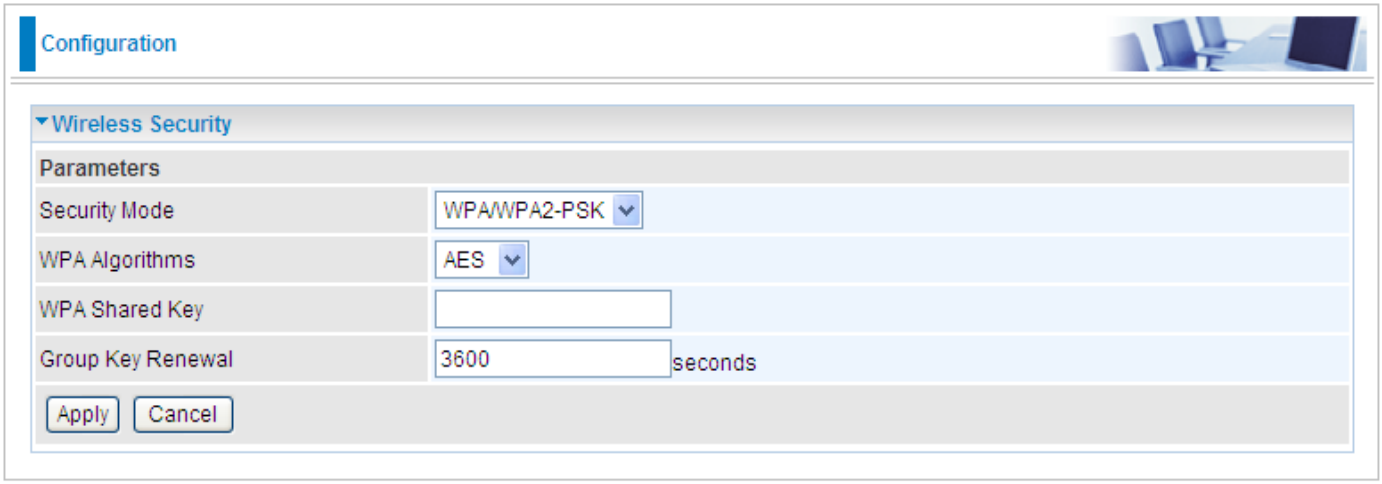
You can disable or enable wireless security with WPA or WEP for protecting wireless network. The default mode of wireless security is disabled.



WPA / WPA2



WPA/WPA2 Pre-Shared Key



RADIUS/802.1x: Whether to enable RADIUS function or not (For WPA/WPA2/WEP encryption).

Security Mode: You can choose the type of security mode you want to apply from the drop down menu.

WPA Algorithms: There are 3 types of the WPA-PSK, WPA2-PSK & WPA/WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

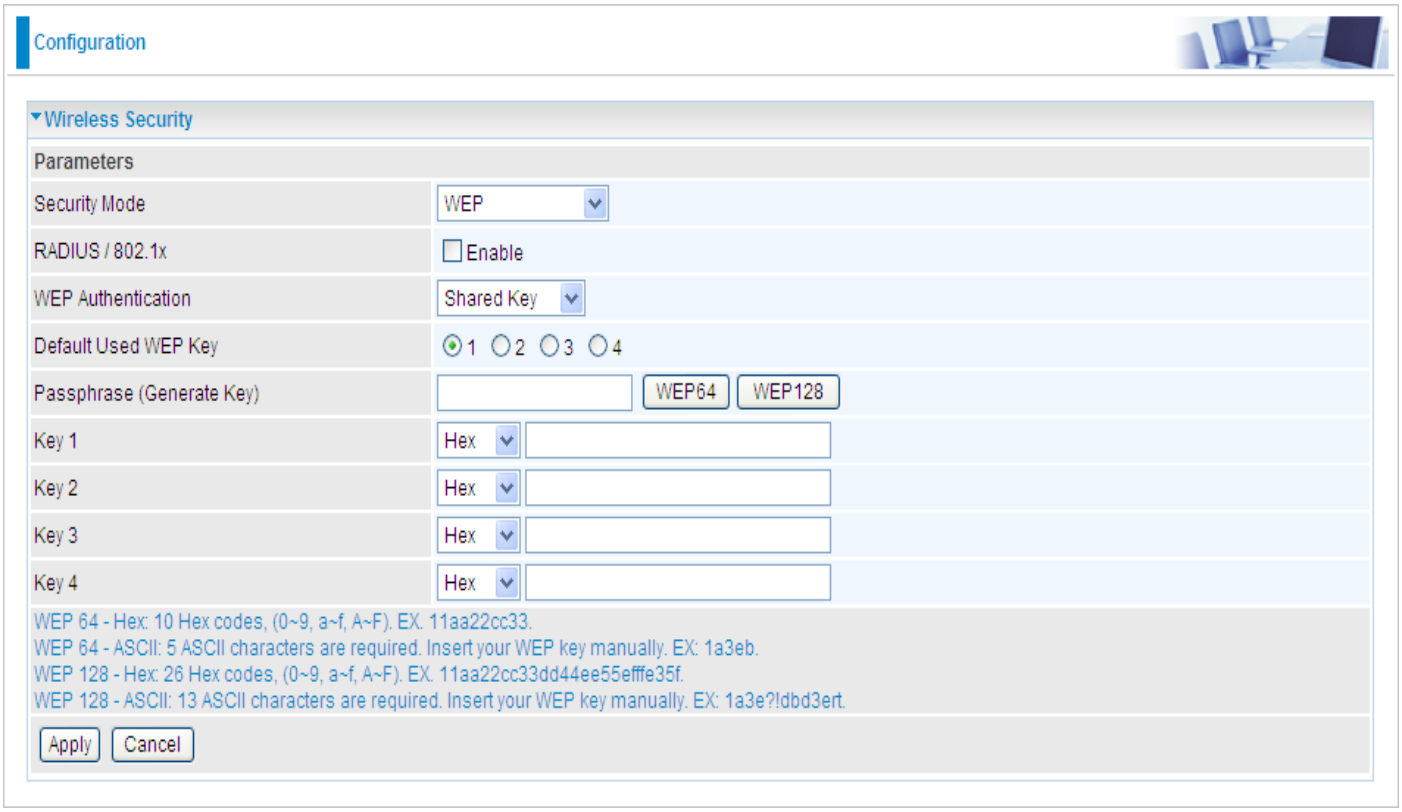
WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically

between wireless client and Access Point (AP). Default value is 3600 seconds.

Click Apply to confirm the settings.

WEP



RADIUS / 802.1x: Whether to enable RADIUS / 802.1x.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. There are 3 options to select from: **Open System, Shared key** or **both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

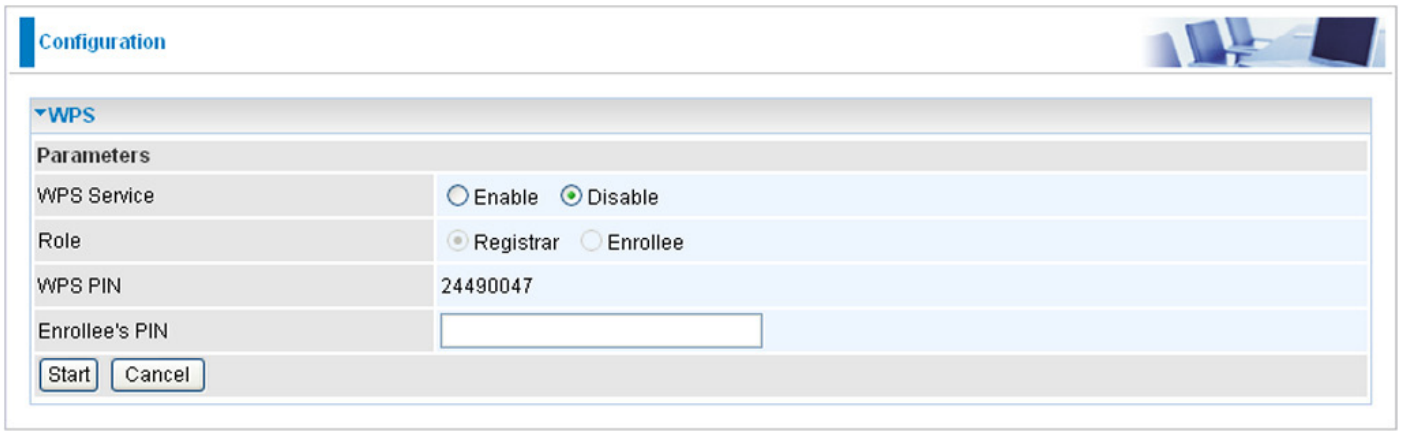
Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be either HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

Click Apply to confirm the settings.

Note: For information about settling Radius/802.1x, please refer to **WLAN** *setup section.*

WPS (only for BiPAC 7800N)

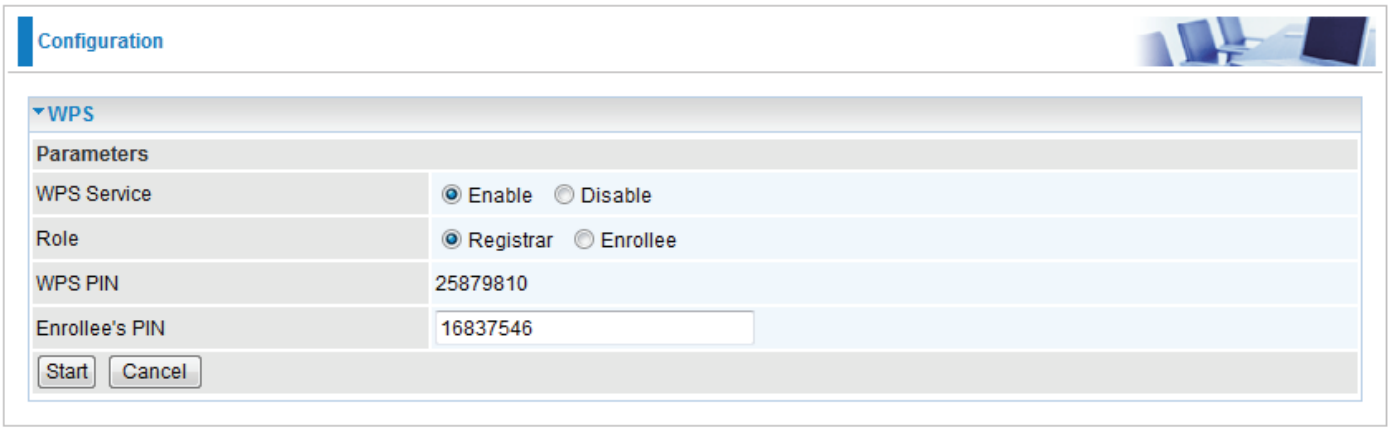
WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi networks for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.



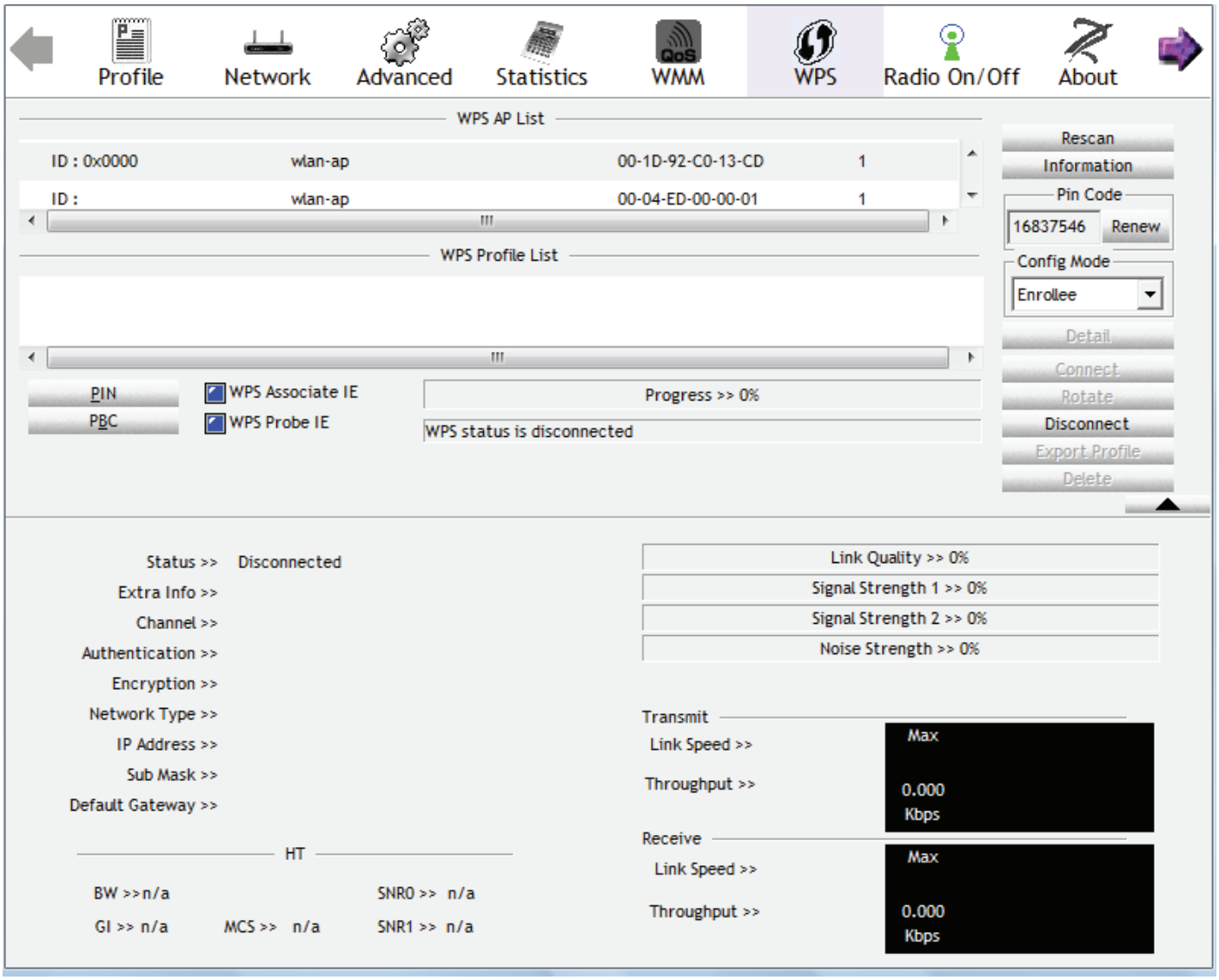
Wi-Fi Network Setup (only for BiPAC 7800N)

PIN Method: Configure AP as Registrar

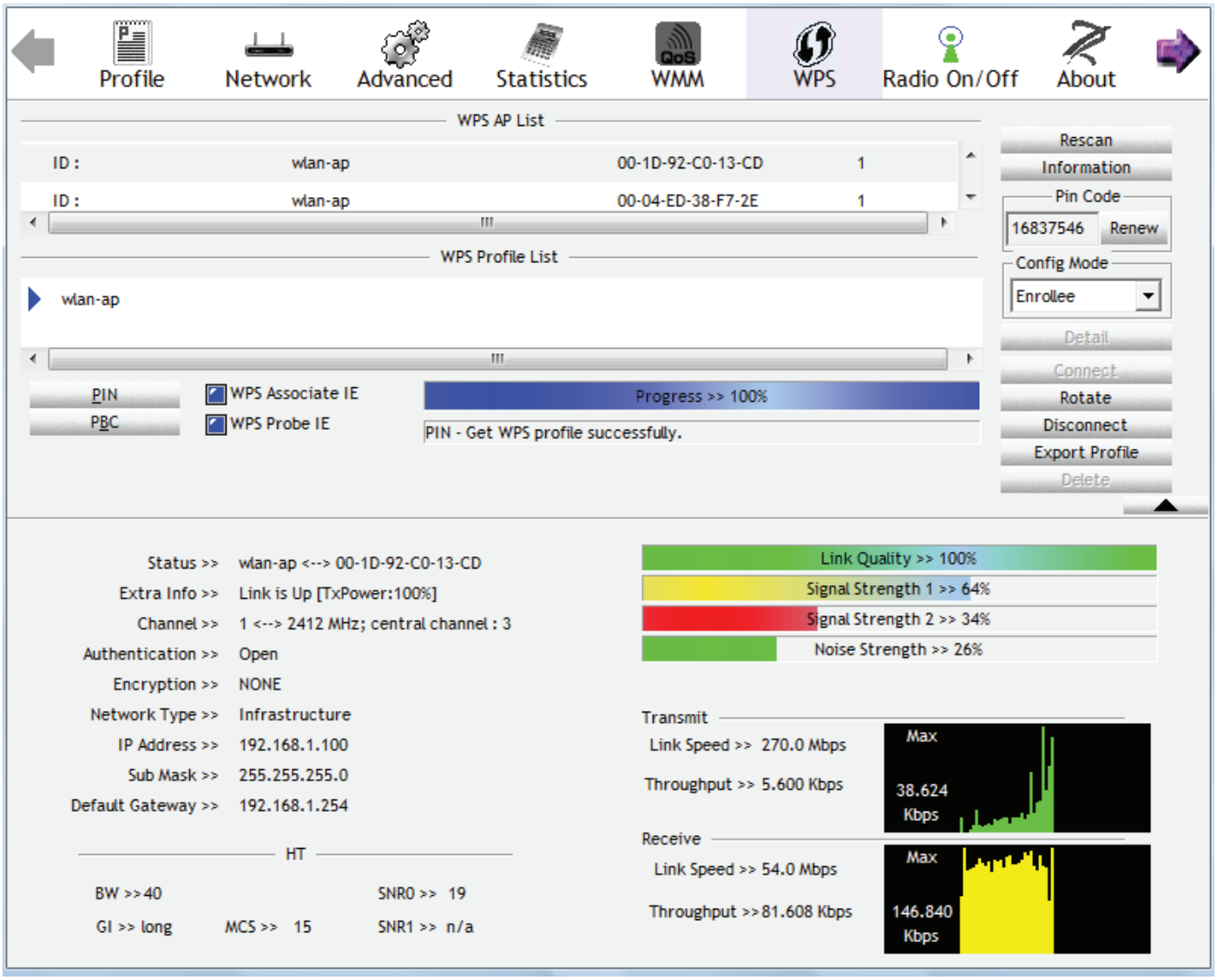
1. Jot down the client's Pin (eg. 16837546).



2. Enter the Enrollee's PIN number and then press Start.
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

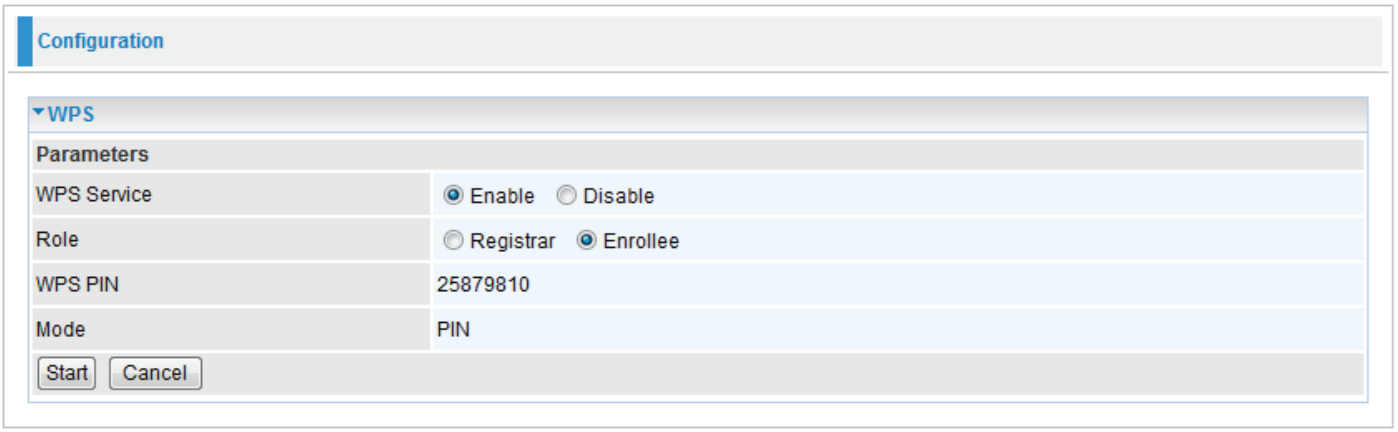


4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.

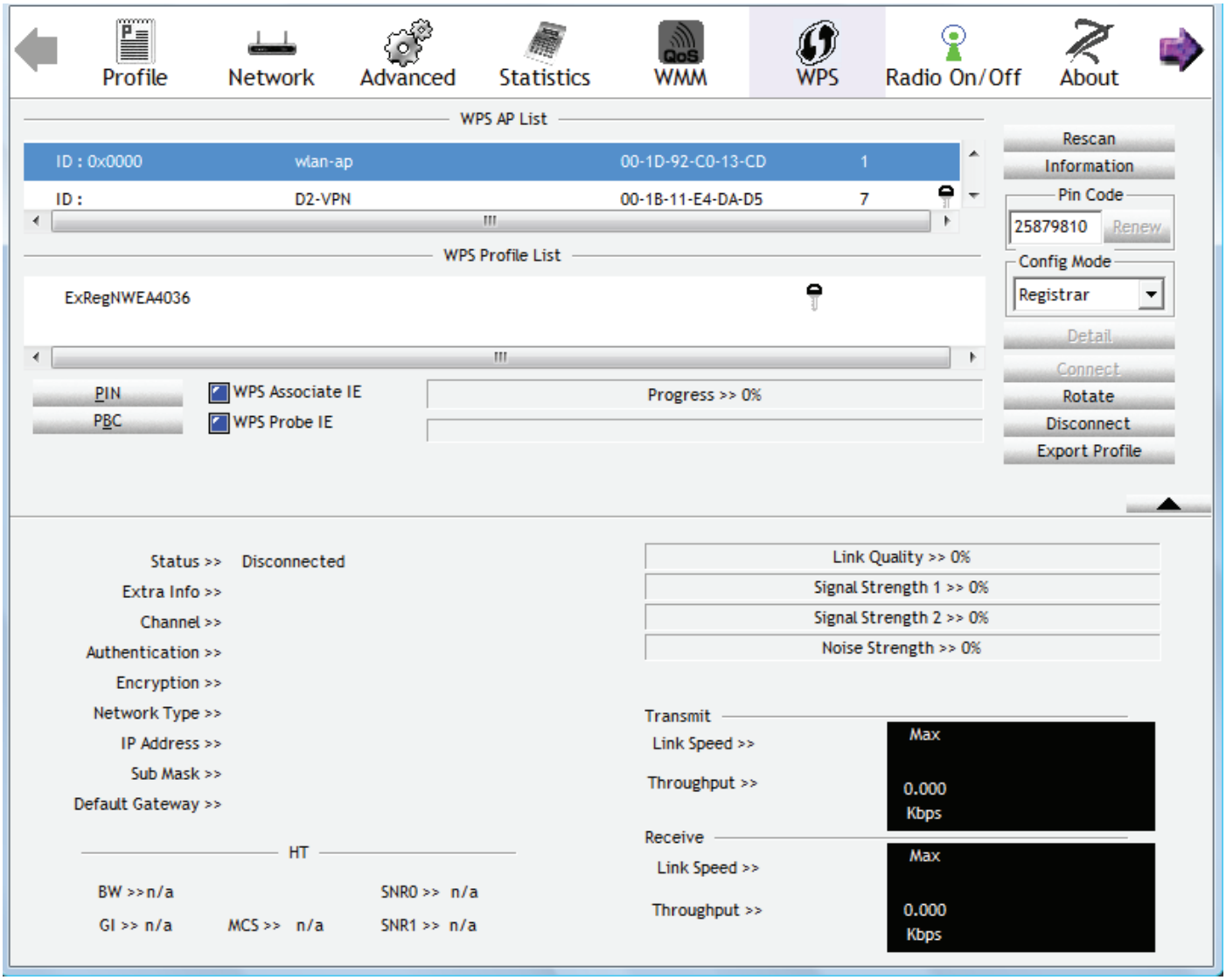


PIN Method: Configure AP as Enrollee

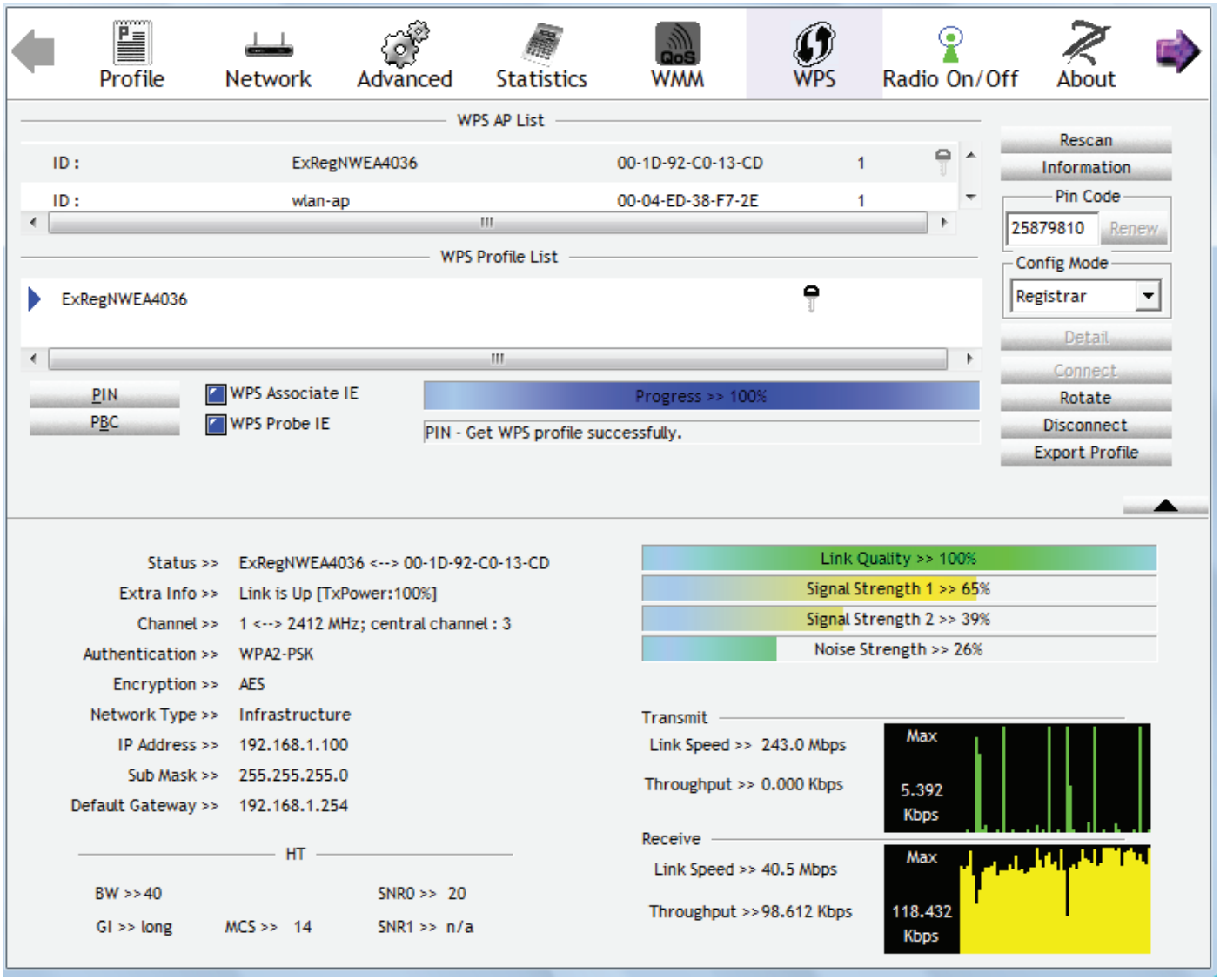
1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (eg. 25879810).



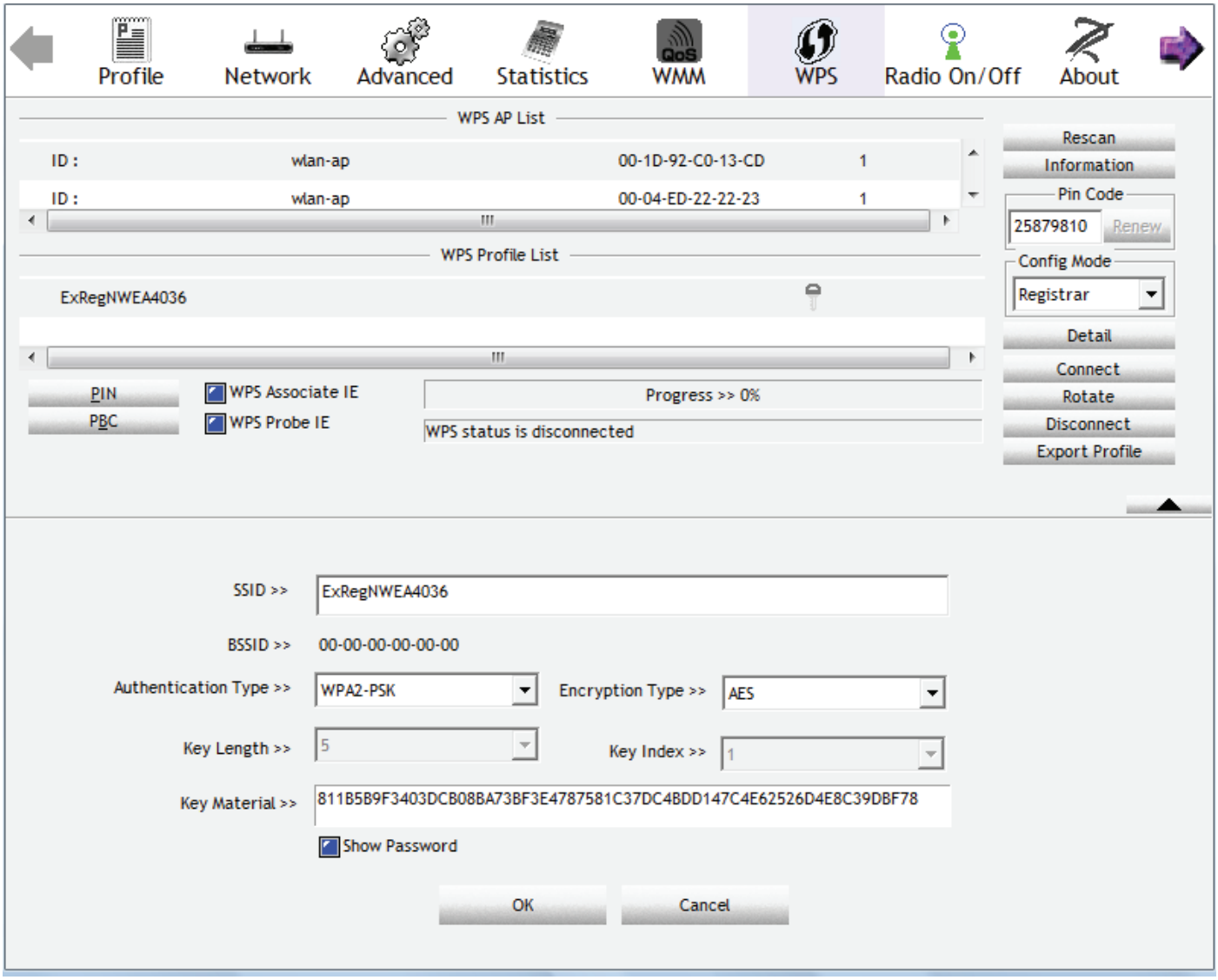
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

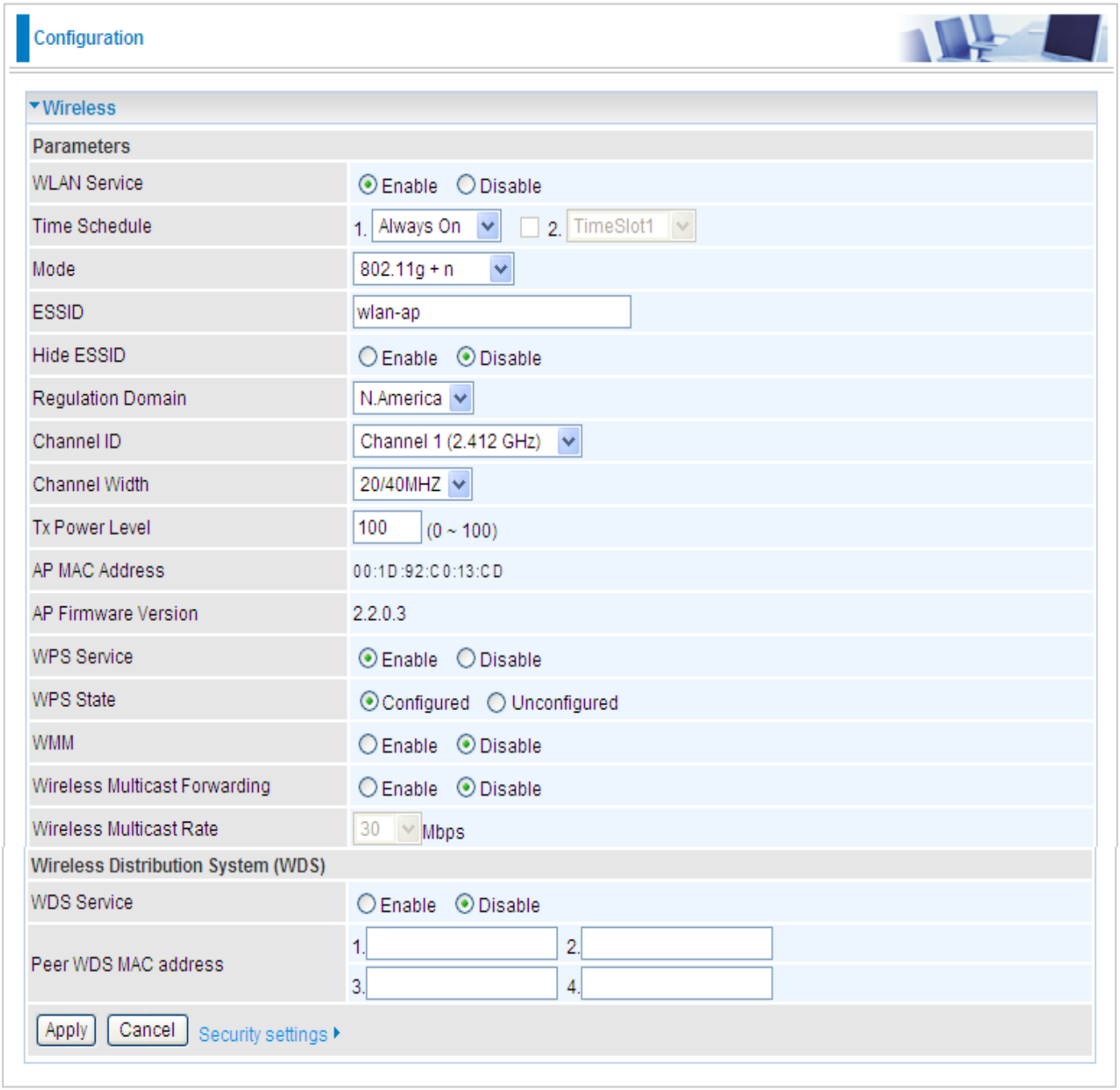


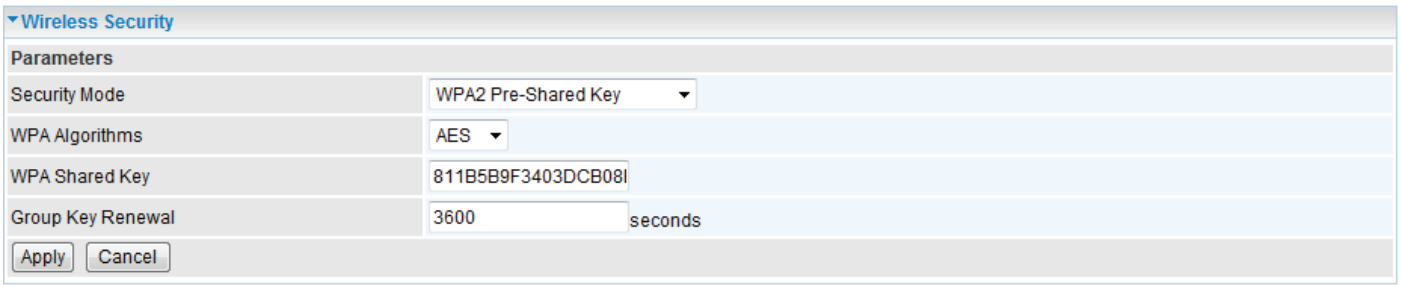
4. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.

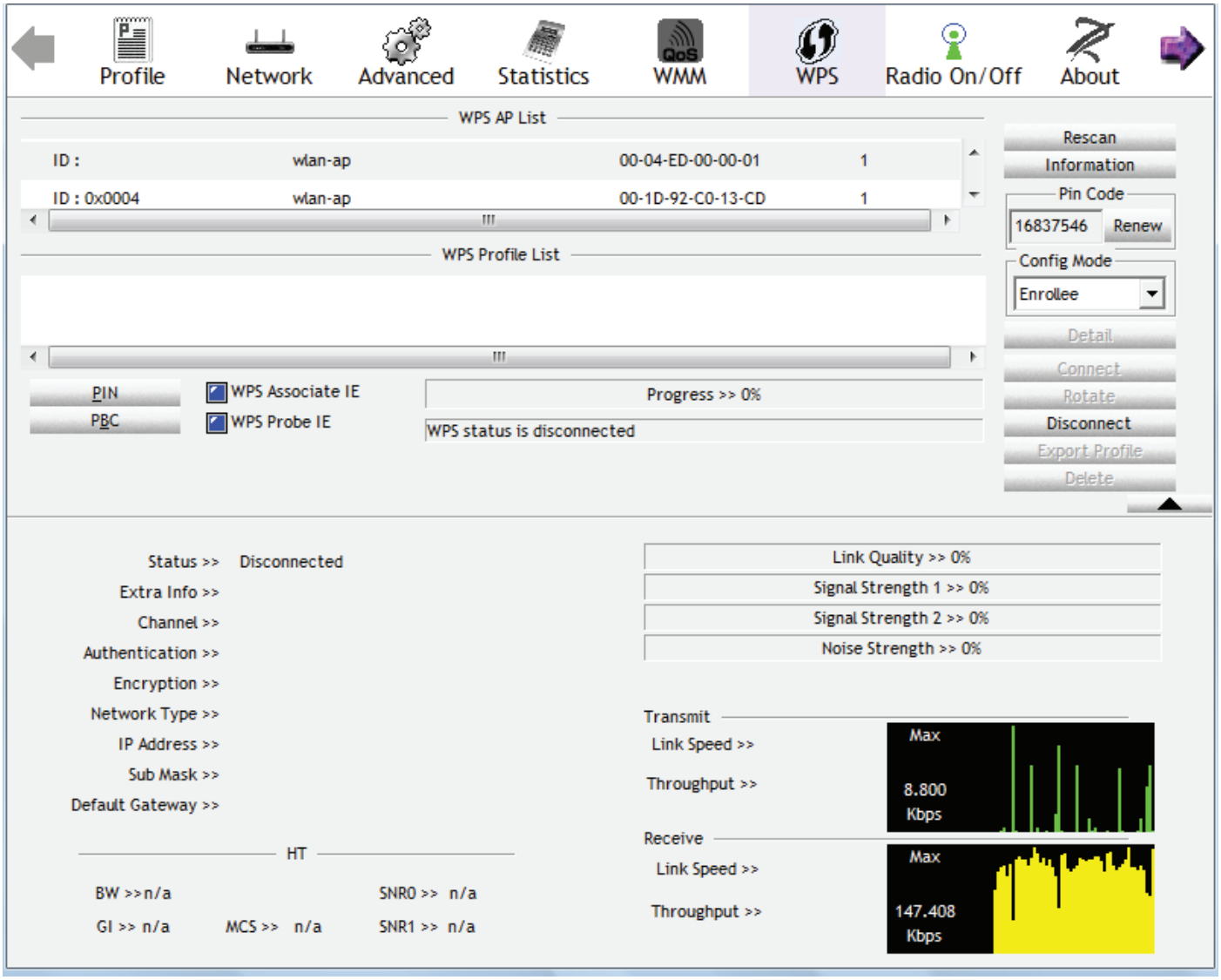



Configuration
Wireless
Parameters
WLAN Service
Enable
Disable
Time Schedule
1.
Always On
2.
TimeSlot1
Mode
802.11g + n
ESSID
wlan-ap
Hide ESSID
Enable
Disable
Regulation Domain
N.America
Channel ID
Channel 1 (2.412 GHz)
Channel Width
20/40MHZ
Tx Power Level
100
(0 ~ 100)
AP MAC Address
00:1D:92:C0:13:CD
AP Firmware Version
2.2.0.3
WPS Service
Enable
Disable
WPS State
Configured
Unconfigured
WMM
Enable
Disable
Wireless Multicast Forwarding
Enable
Disable
Wireless Multicast Rate
30
Mbps
Wireless Distribution System (WDS)
WDS Service
Enable
Disable
Peer WDS MAC address
1.
2.
3.
4.
Apply
Cancel
Security settings

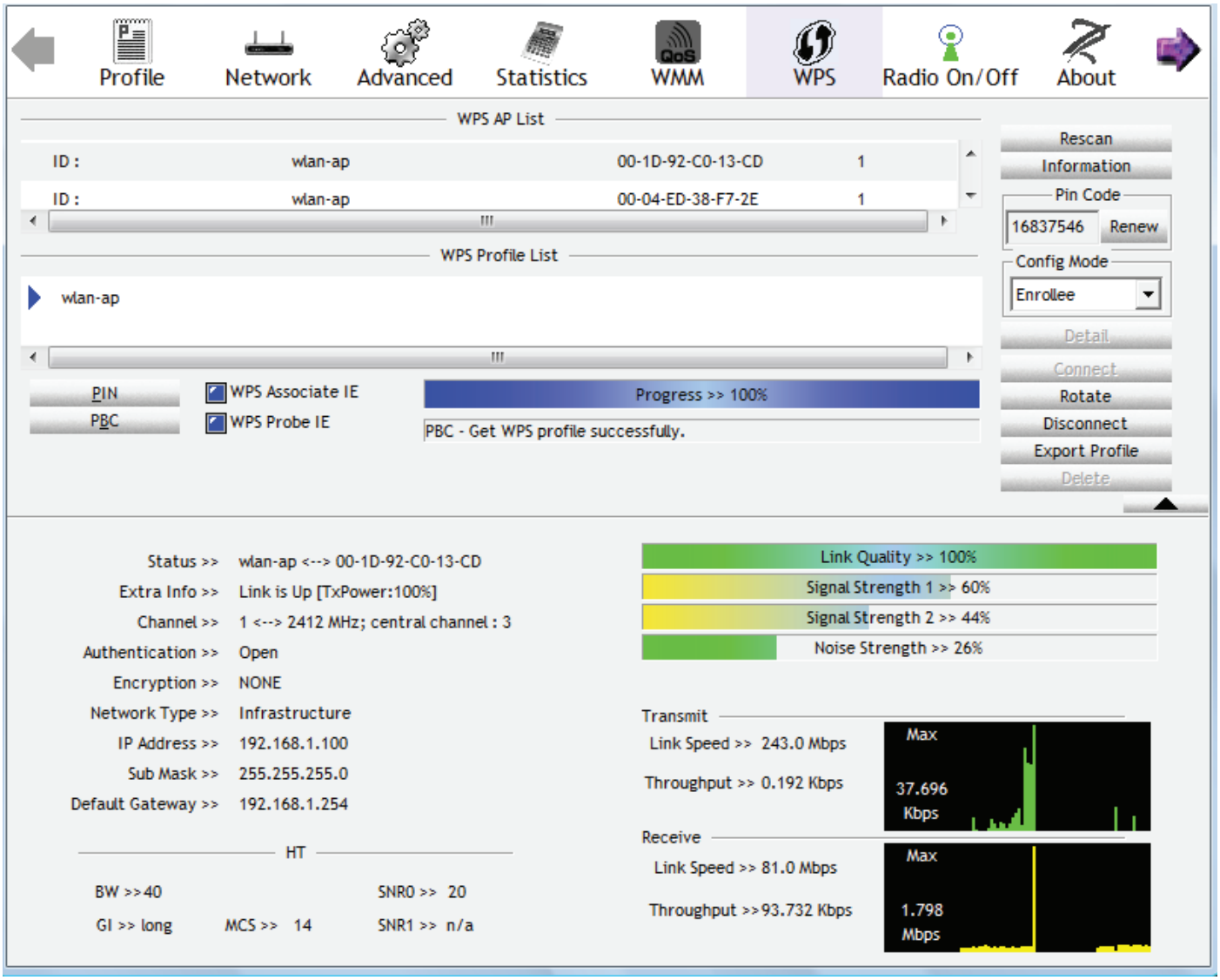

Wireless Security
Parameters
Security Mode
WPA2 Pre-Shared Key
WPA Algorithms
AES
WPA Shared Key
811B5B9F3403DCB08I
Group Key Renewal
3600
seconds
Apply
Cancel

PBC Method:

1. Press the PBC button of the AP.
2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.

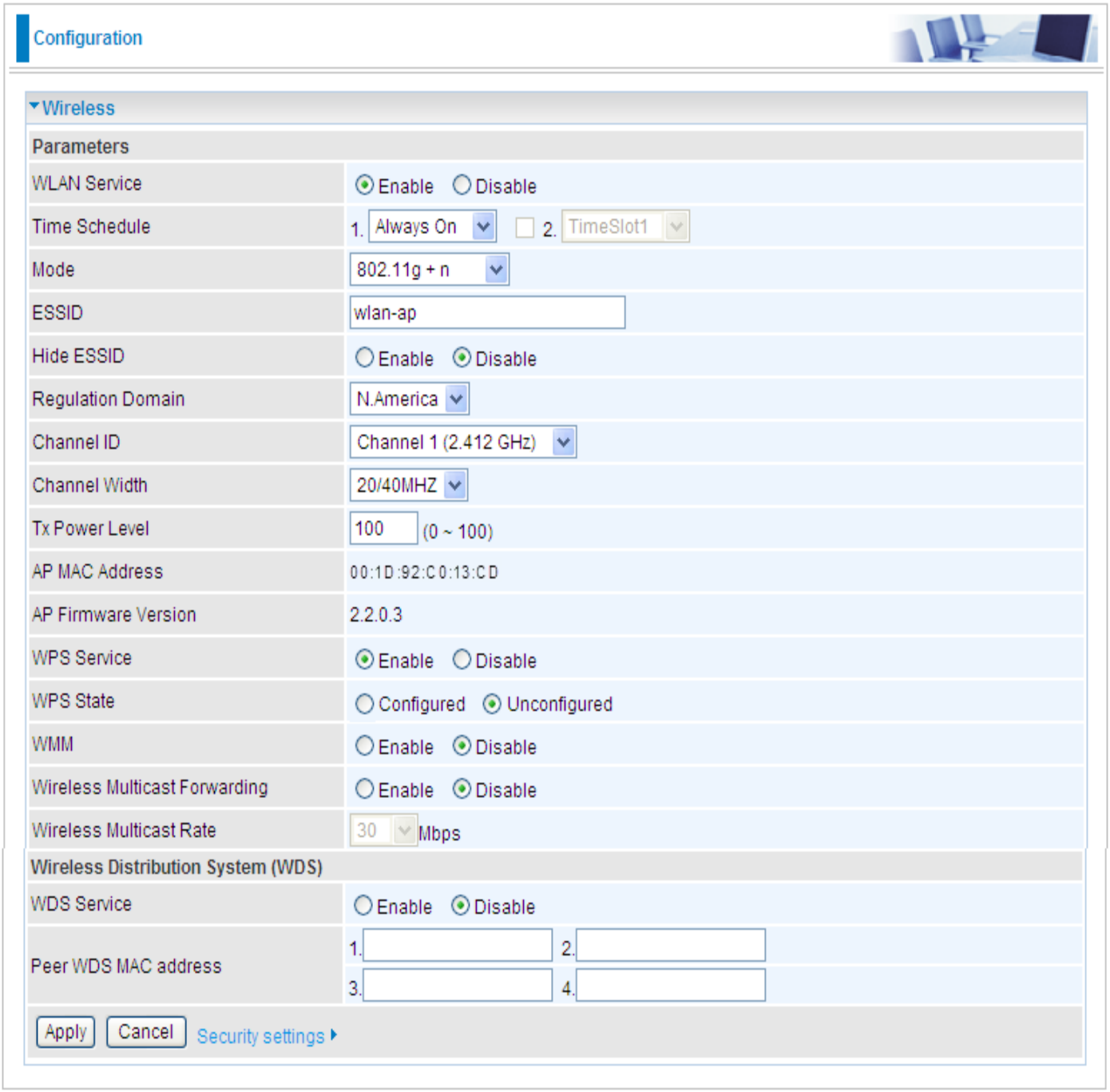


3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

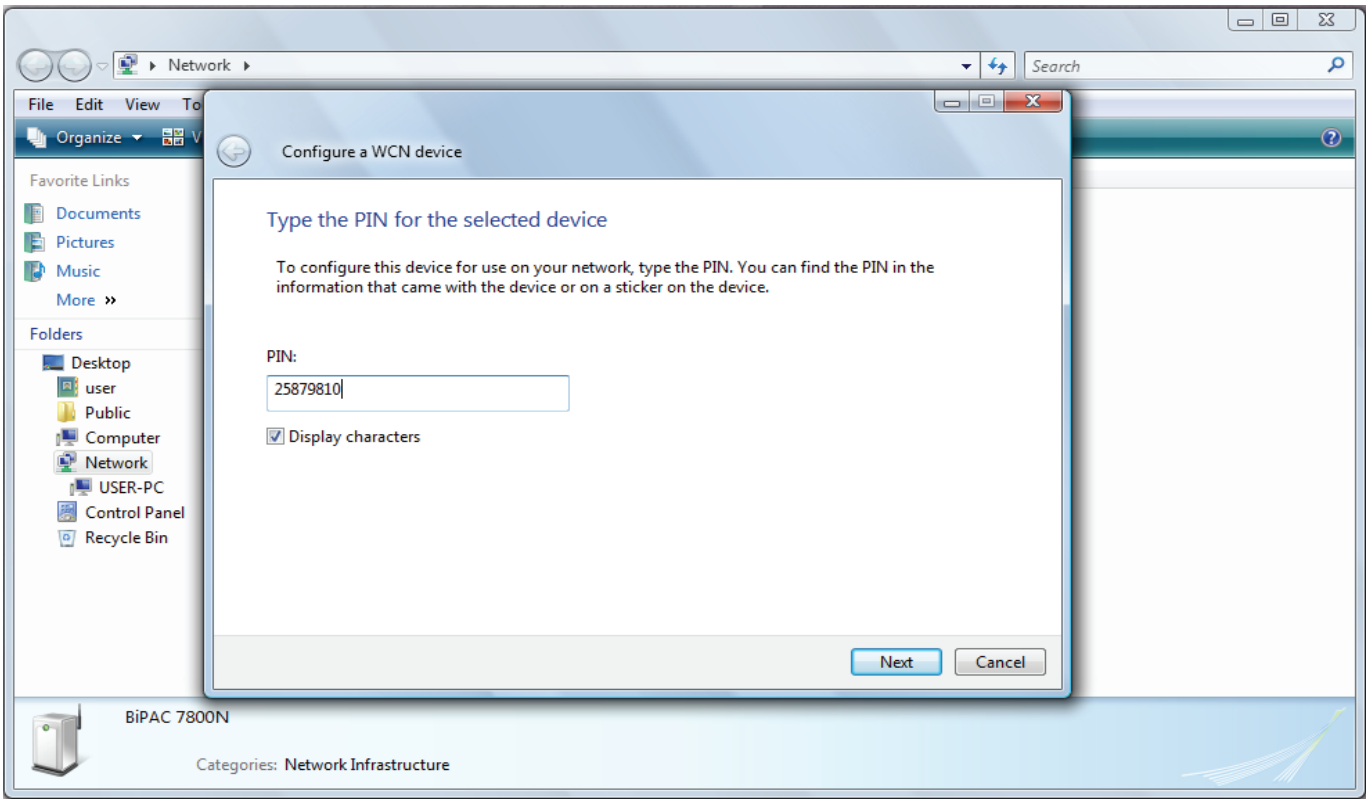


Wi-Fi Network Setup with Windows Vista WCN:

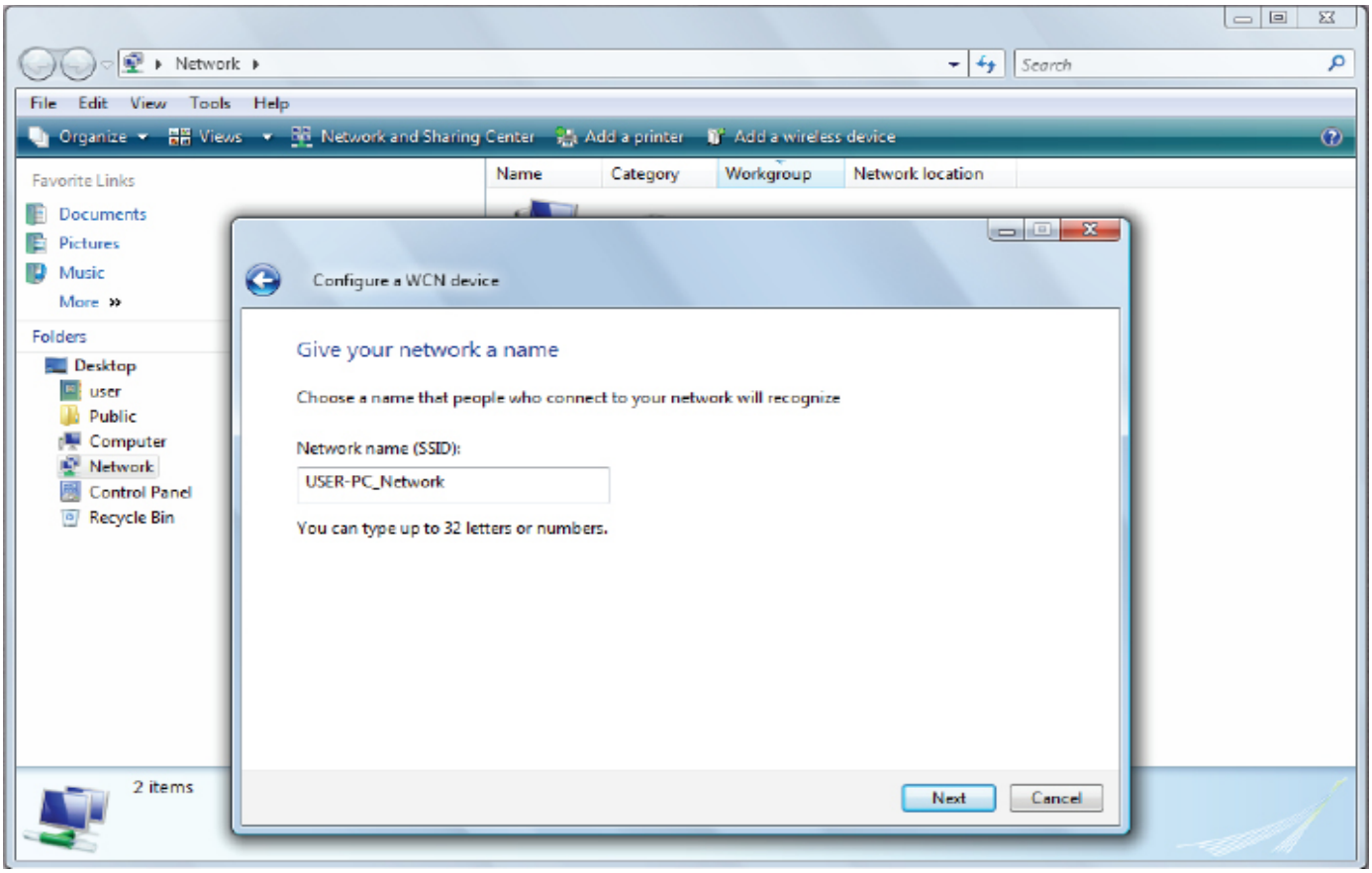
1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Enable WPS service, set the WPS State to Unconfigured and then click Apply.



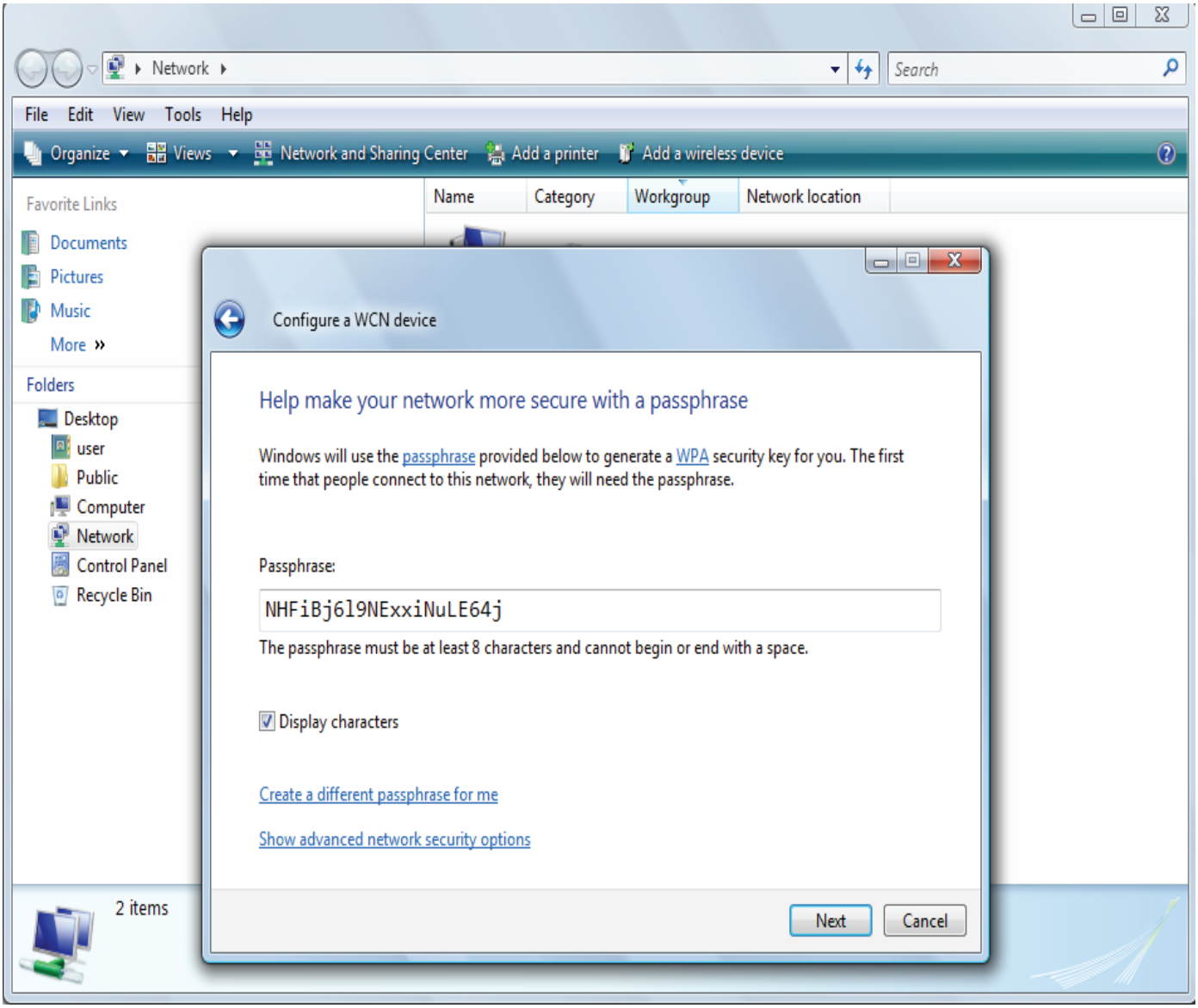
3.In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 7800N icon and enter the AP PIN in the column provided then press Next.



4. Enter the AP SSID then click Next.



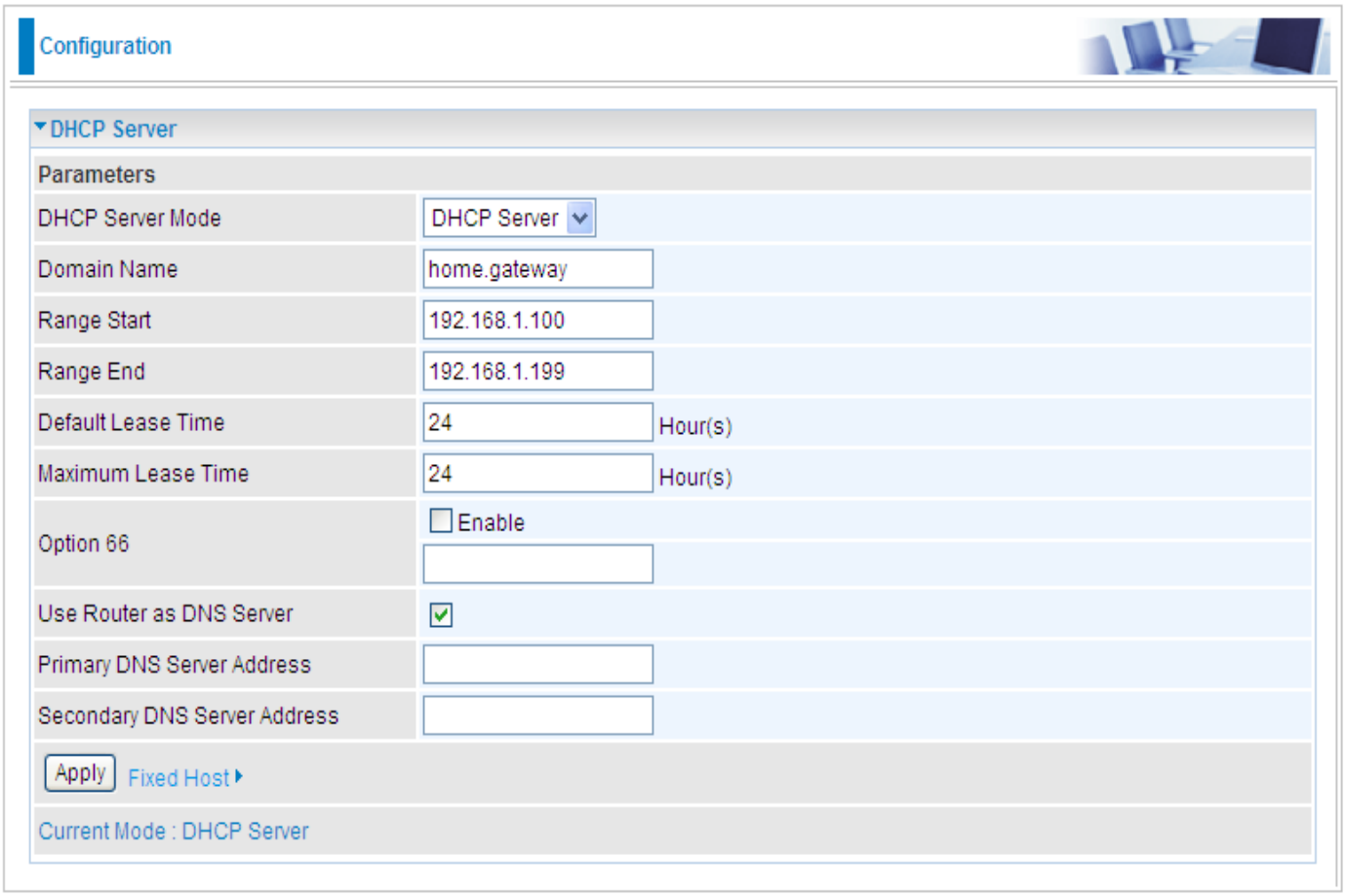
5. Enter the passphrase then click Next.



6. When you have come to this step, you will have comleted the Wi-Fi network setup using the built-in WCN feature in Windows Vista.

DHCP Server

DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device.



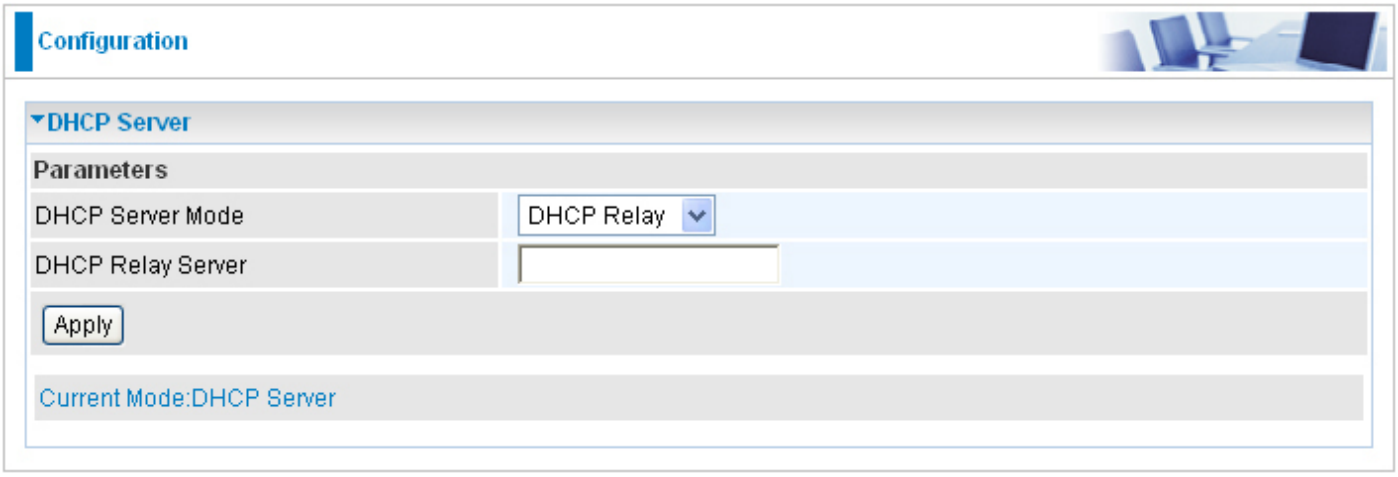
To configure the router's DHCP Server, select **DHCP Server** from the DHCP Server Mode drop-down menu. You can then configure parameters of the DHCP Server including the domain, IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. If you check "Use Router as a DNS Server", the ADSL Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network). Click Apply to enable this function.

Note:

Option 66: This option is used to identify a TFTP server, User must set TFTP server IP address if enable option 66.

Click Apply to enable this fuction.

If you select **DHCP Relay** from the DHCP Server Mode drop-down menu, you must enter the IP address of the DHCP server that assigns an IP address to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click Apply to enable this function.

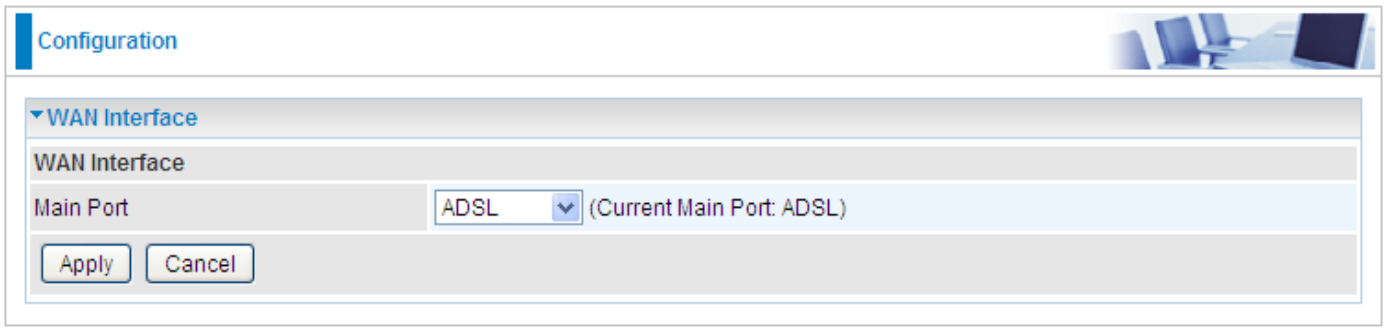


WAN - Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems. There are two items within the WAN section: **WAN Interface, WAN Profile** and **ADSL Mode**.

WAN Interface

WAN Interface (ADSL)



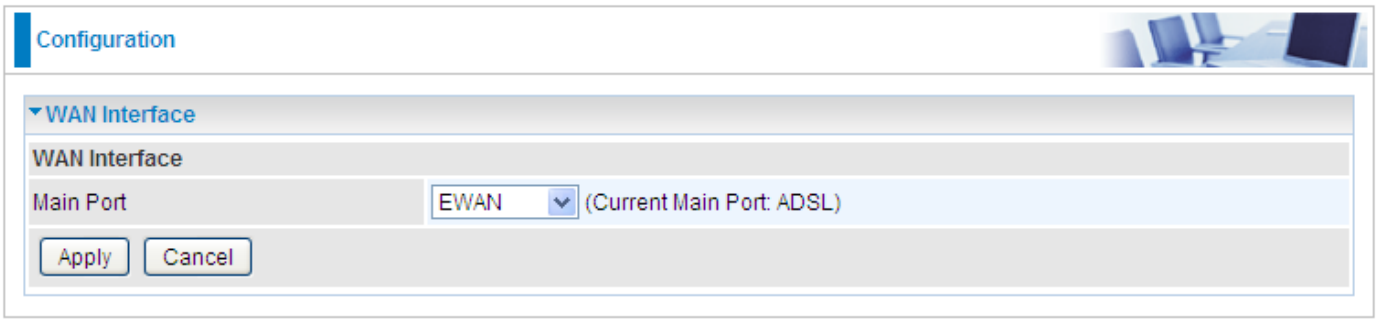
Main Port: Select the main port(the WAN connection mode) from the drop-down menu.

Click **Apply** to confirm the change.

Note:

Current Main Port: indicate the current used main WAN connection mode, default is ADSL.

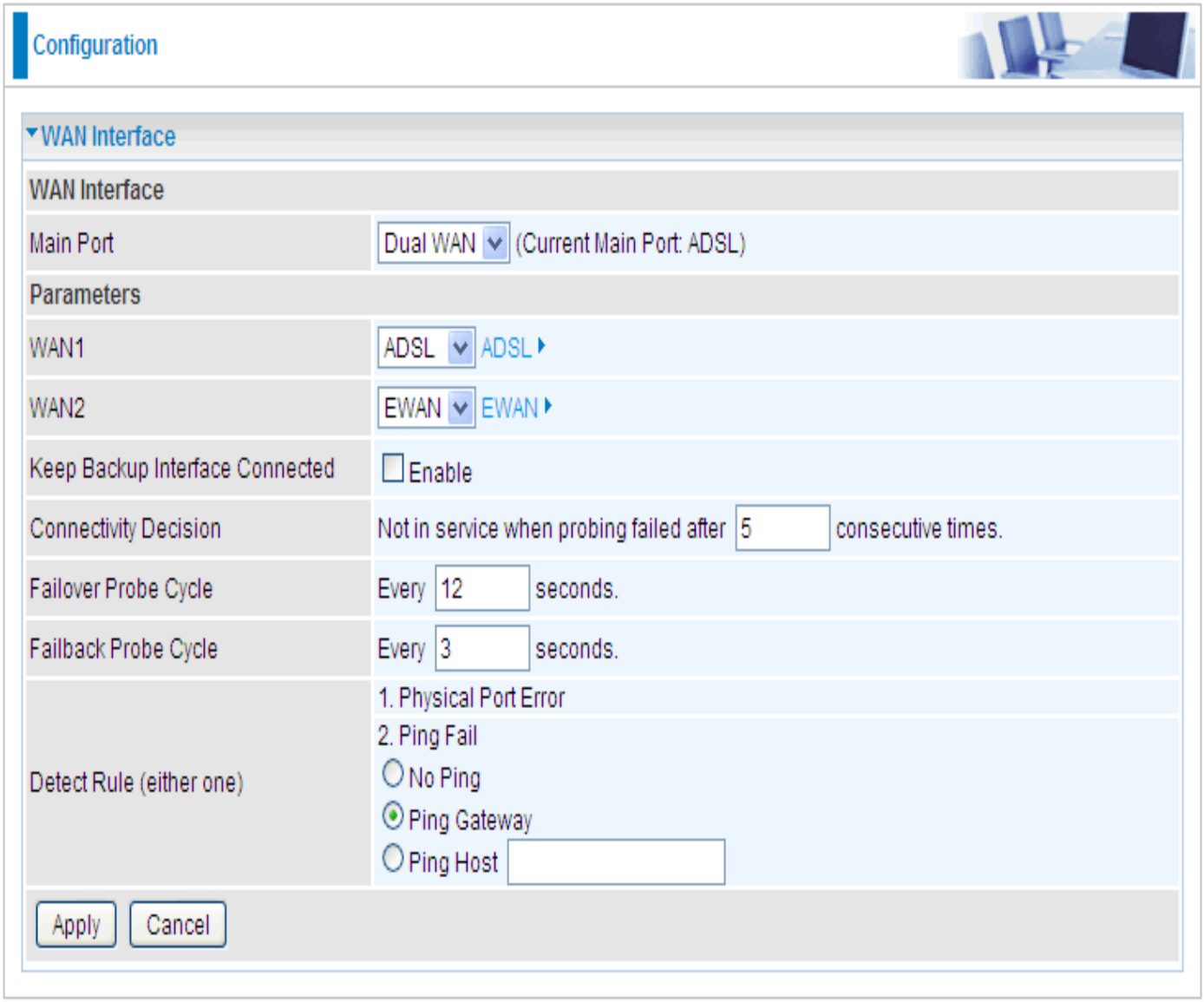
WAN Interface (EWAN)



Main Port: Select the main port from the drop-down menu.

Click **Apply** to confirm the change.

WAN Interface (Dual WAN)



Main Port: Select the main port from the drop-down menu.

WAN1: Choose ADSL or EWAN for WAN1. Click the link to go to WAN Profile page to configure its parameters.asdffddddd

WAN2: Choose one from the remainninng modes. Click the link to go to WAN Profile page to configure its parameters.

Connectivity Decision: Enter the value for the times when probing failed to switch backup port.

Failover Probe Cycle: Set the time duration for the Failover Probe Cycle to determine when the

router will switch to the backup connection (backup port) once the main connection (main port) fails.

Failback Probe Cycle: Set the time duration for the Failback Probe Cycle to determine when the

router will switch back to the main connection (main port) from the backup connection (backup port) once the main connection communicates again.

Note: The time values entered in Failover Probe Cycle and Failback Probe Cycle fields are set for

each probe cycle and decided by Probe Cycle duration multiplied by Connection Decision value(e.g. 60 seconds are multiplied by 12 seconds and 5 consecutive fails).

Detect Rule (either one):

1. Physical Port Error

2. Ping Fail

• **No Ping:** It will not send any ping packet to determine the connection. It means to disable the ping fail detection.

• **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every “Probe Cycle”.

• **Ping Host:** It will send ping packet to specific host and wait response in every “Probe Cycle”. The host must be an IP address.

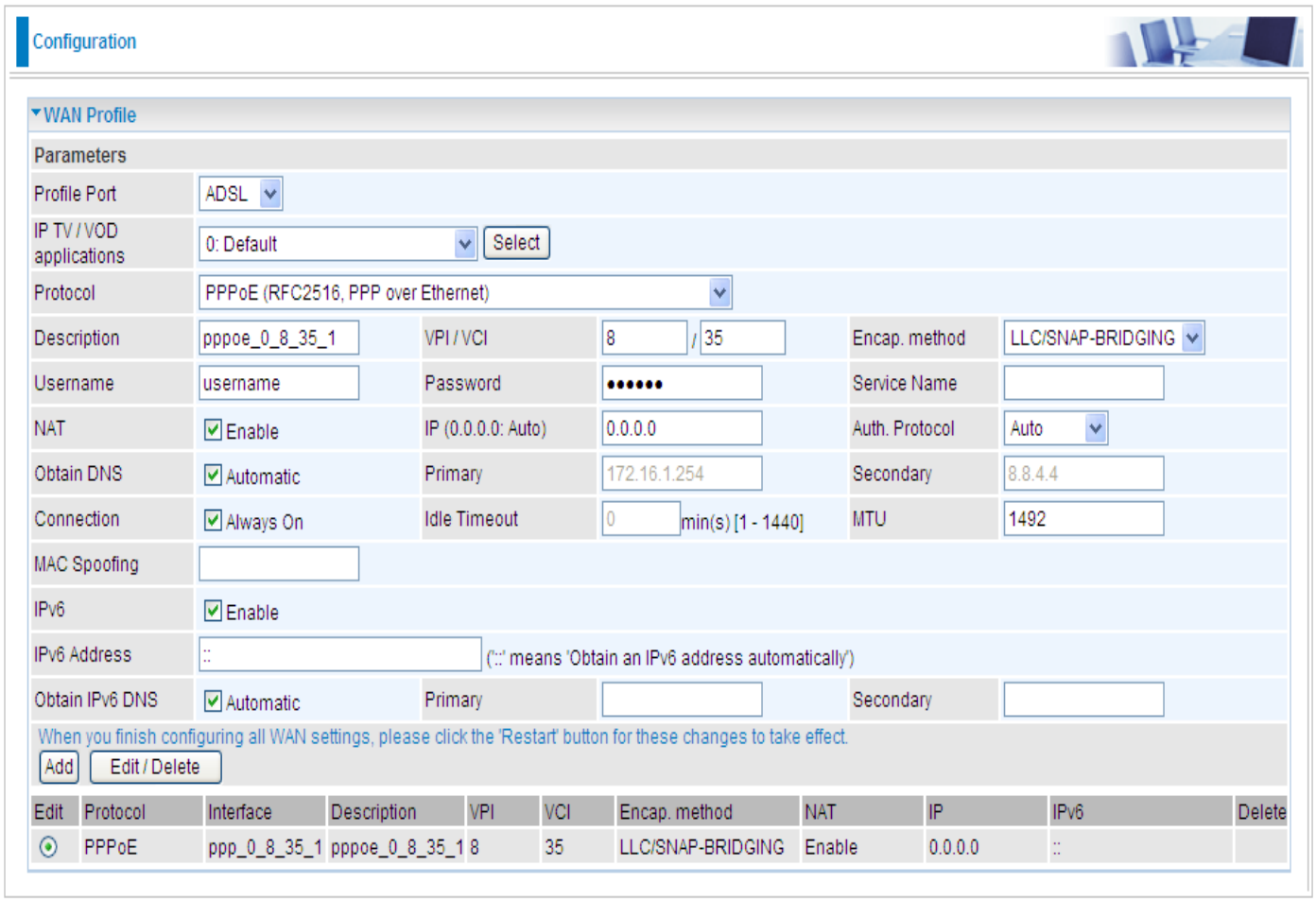
Click **Apply** to confirm the change.

WAN Profile

WAN Profile (ADSL)

PPPoE Connection (ADSL)

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



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

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

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

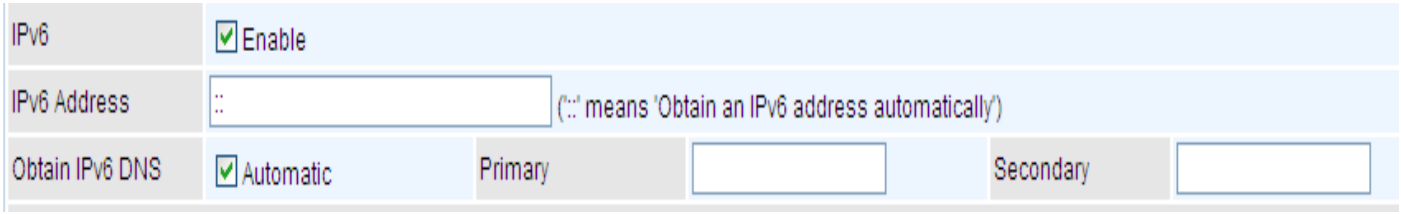
Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



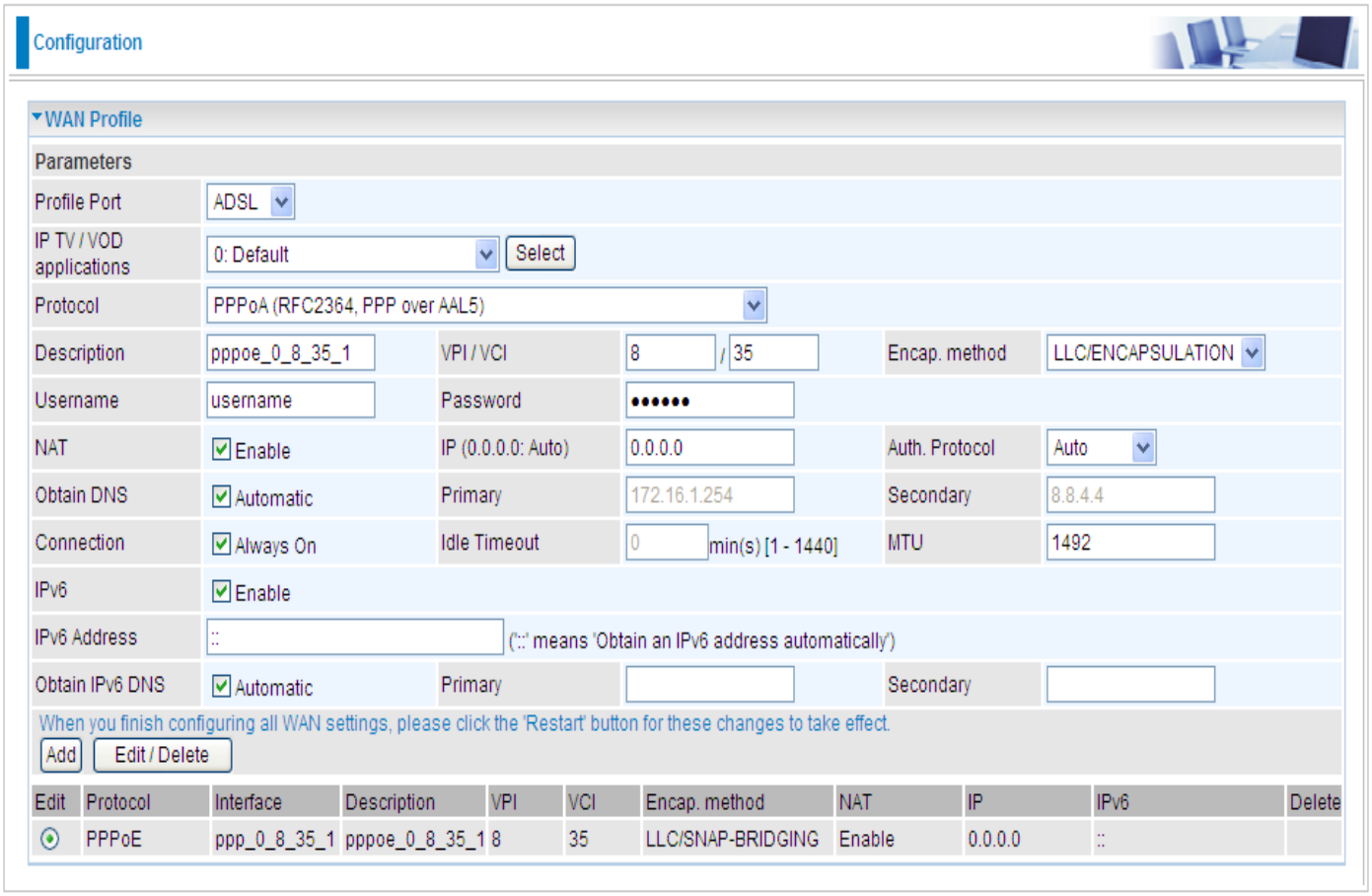
IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ”::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the exact ones in the Primary and secondary fields.

Click Apply to confirm the settings.

PPPoA Connection (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functions in a manner similar to dial-up services using PPP.



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

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

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

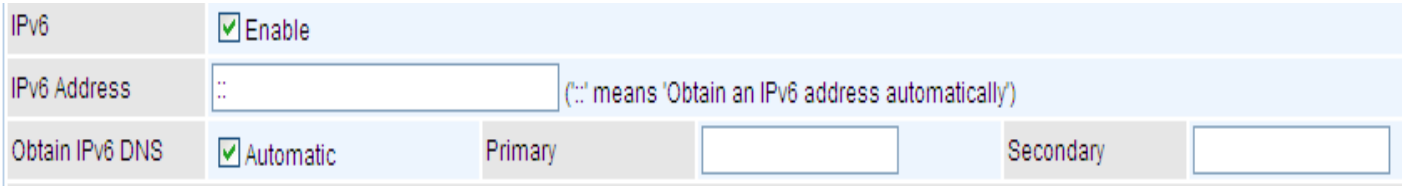
Secondary DNS: Enter the secondary DNS.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.

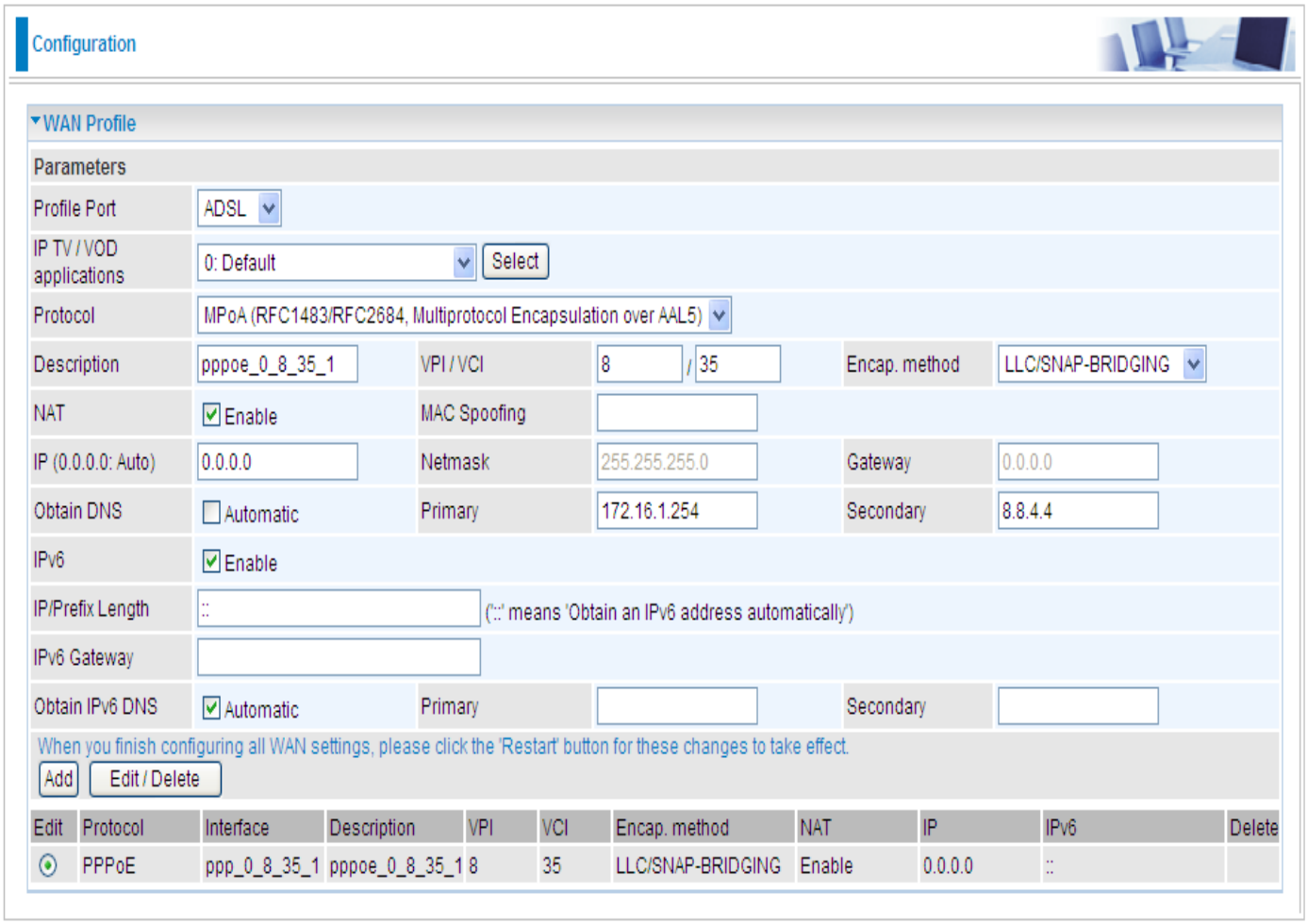


IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ”::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the exact ones in the Primary and secondary fields.

Click Apply to confirm the settings.

MPoA Connection (ADSL)



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

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

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway can be left blank.

Netmask: User can change it to other such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

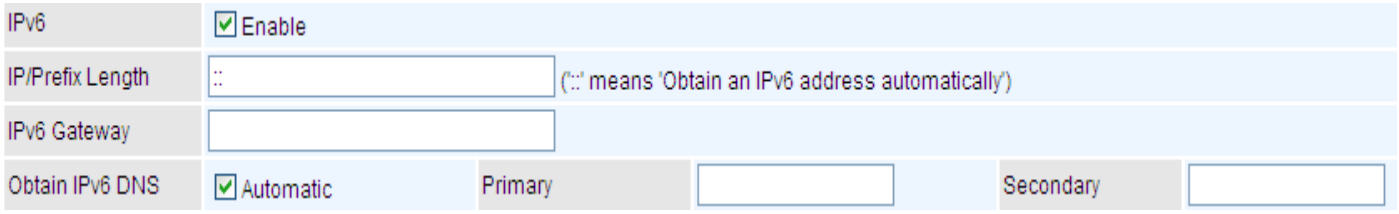
Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are

passed to the DHCP clients along with the IP address and the netmask.

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



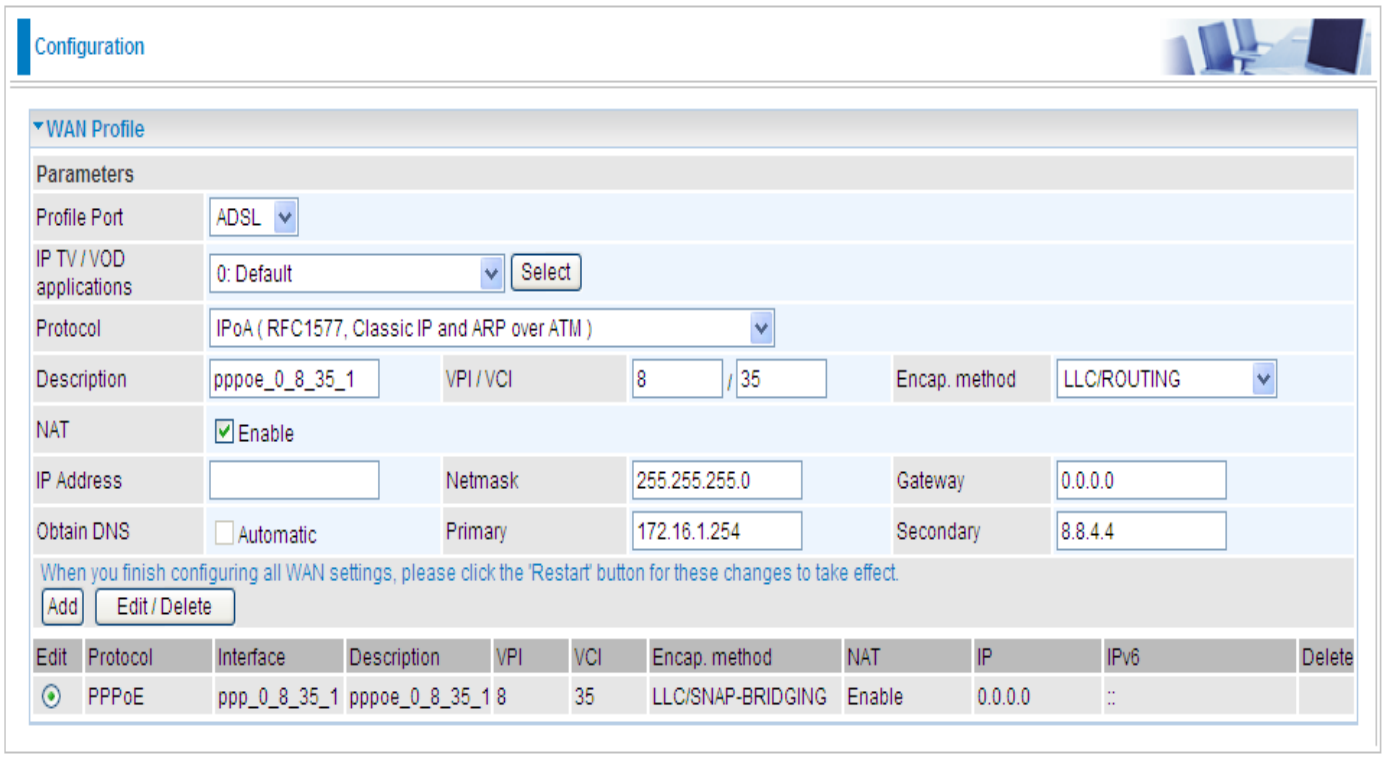
IP/Prefix Length: please type the IP and the prefix length for the IPv6 address from your ISP.

IPv6 Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Click Apply to confirm the settings.

IPoA Connections (ADSL)



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

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

IP Address: Enter your fixed IP address.

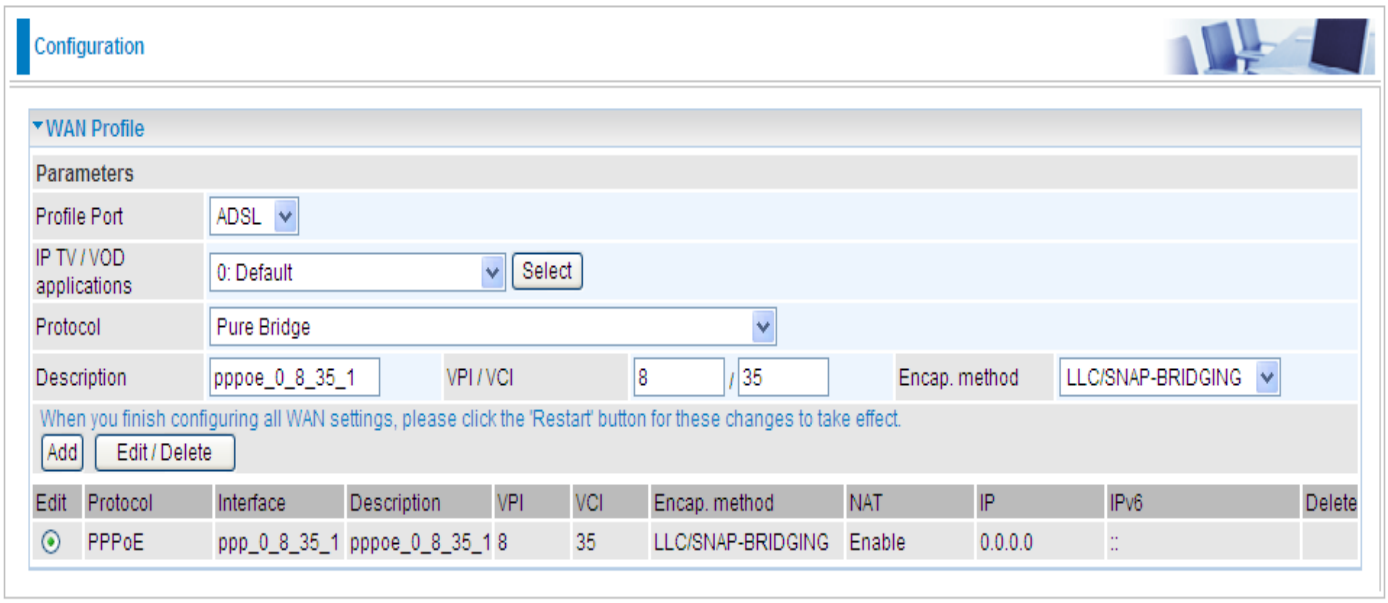
Netmask: User can change it to other such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: Select this check box to activate DNS.

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

Pure Bridge Connections (ADSL)



IP TV / VOD applications: The predefined WAN settings for users. Users can adopt the appropriate one base on need.

Description: A given name for the connection.

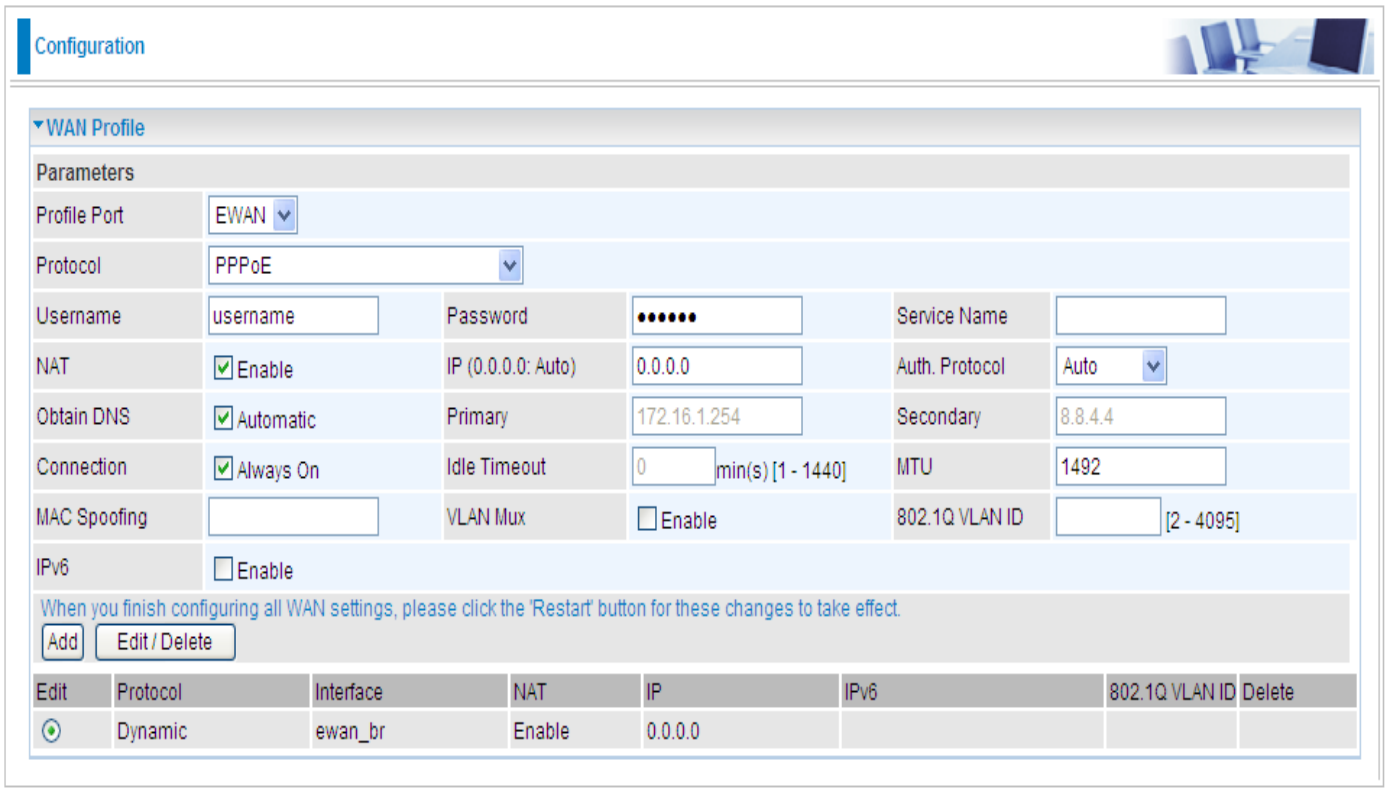
VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

WAN Profile – Main Port (EWAN)

Besides using ADSL to connect to the Internet, BiPAC 7800(N) EWAN port is also an alternative to connect to Cable Modems, VDSL and fiber optic lines. This alternative provides users with faster connection & flexibility to connect to the Internet.

PPPoE (EWAN)



Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

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.

IP (0.0.0.0.Auto): Enter your fixed IP address.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS Automatically: Select this check box to activate DNS.

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

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line

for a predetermined period of time.

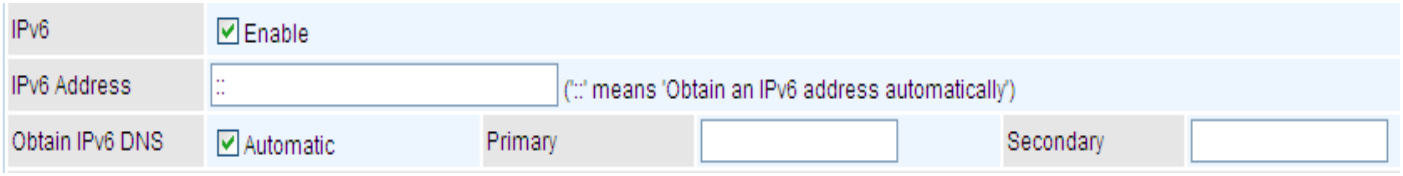
MTU: Control the maximum Ethernet packet size your PC will send.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.

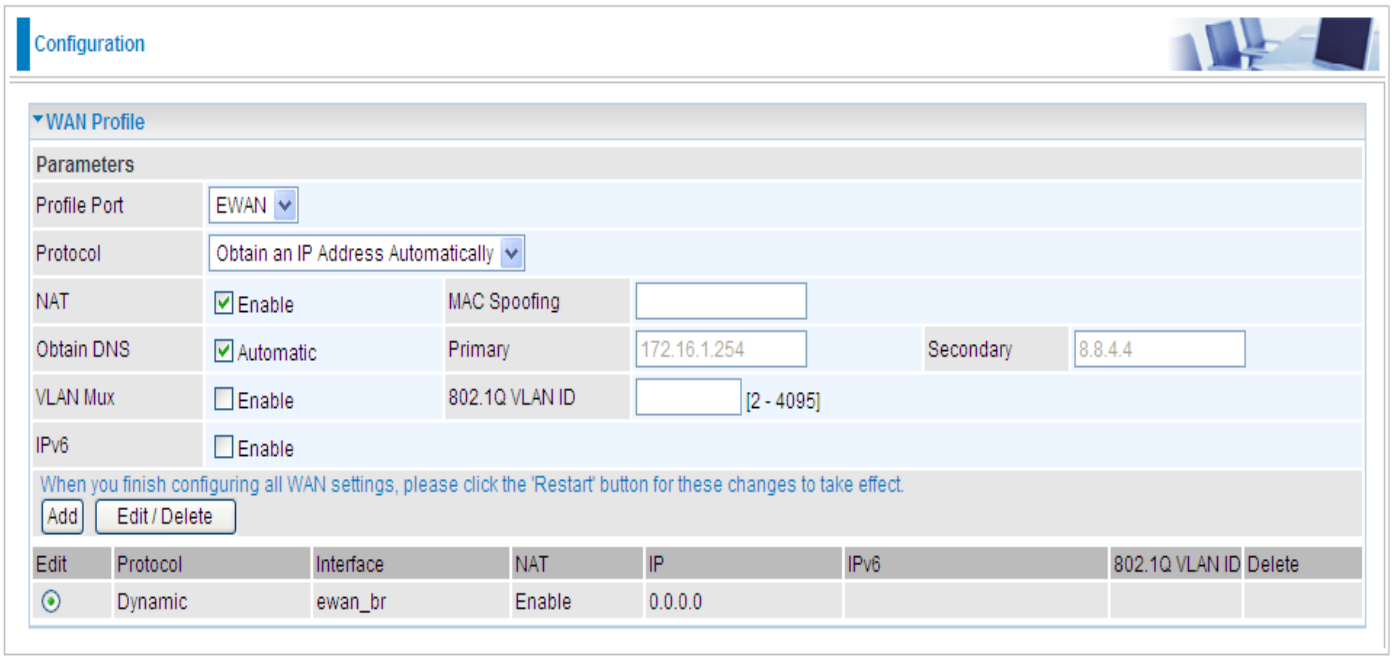


IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Click Apply to confirm the settings.

Obtain an IP Address Automatically (EWAN)



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.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Obtain DNS: Select this check box to activate DNS.

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

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

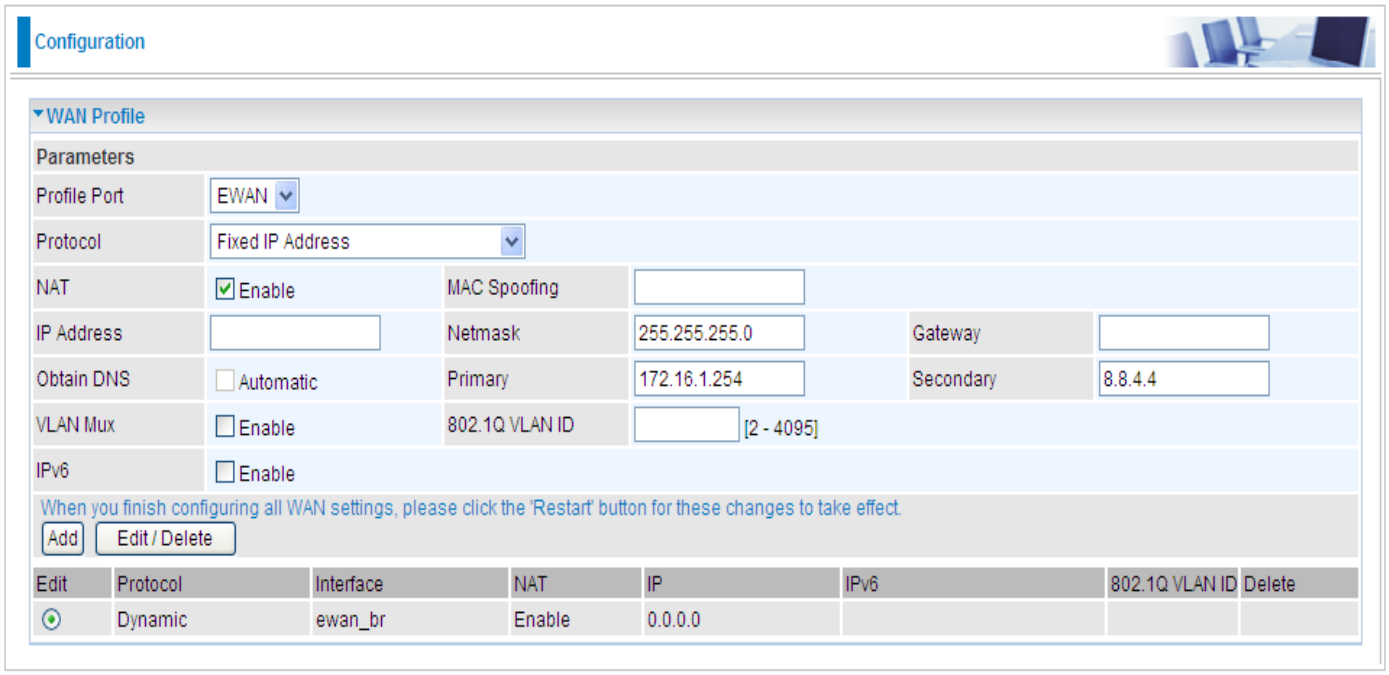
IPv6: Check to enble the function

IPv6 Gateway: Enter the IP address of the default IPv6 gateway.

Obtain IPv6 DNS: check Automatic to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

Click Apply to confirm the settings.

Fixed IP Address (EWAN)



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.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

Gateway: Enter the IP address of the default gateway.

Obtain DNS: Select this check box to activate DNS.

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

VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

IPv6: Check to enble the function.

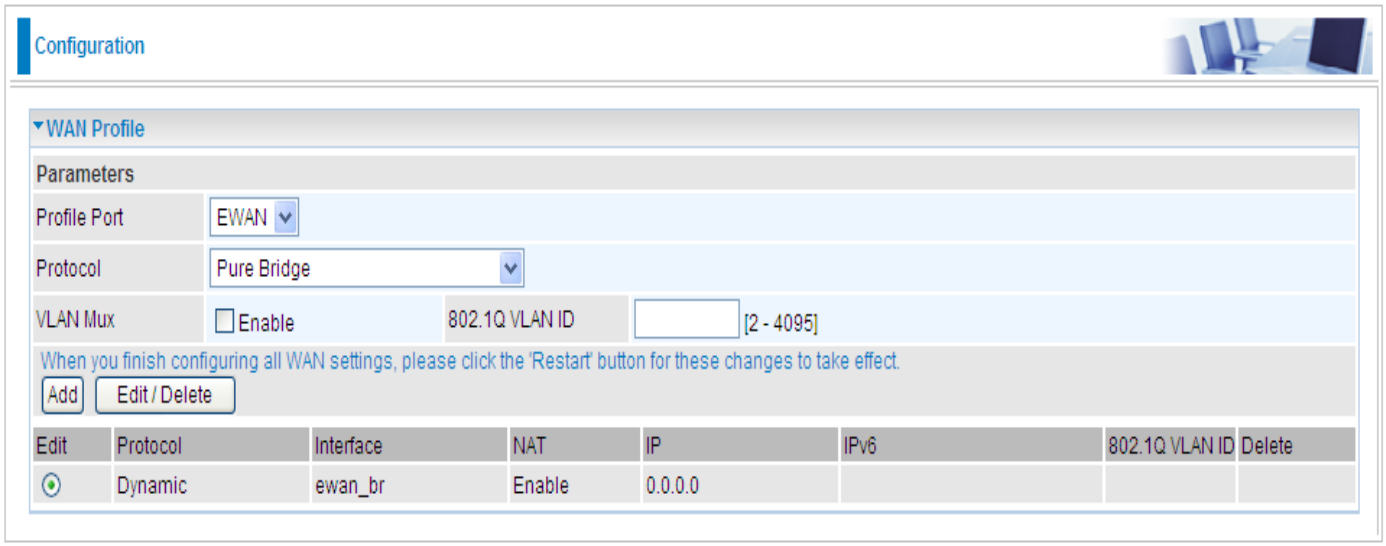
IP/Prefix Length: Enter IP Address and Prefix length.

IPv6 Gateway: Enter the IP address of the default IPv6 gateway.

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

Click Apply to confirm the settings.

Pure Bridge (EWAN)



VLAN Mux: check whether to enable VLAN Mux function.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 2-4095.

Click Apply to confirm the settings.

VLAN MUX Setting

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.

The most commonly used Virtual LAN is defined by 802.1Q tagging protocol, which expended the original Ethernet frame header to include VLAN ID (tag) and priority bits.With the support of network equipments, multiple virtual networks can coexist over the same physical network.

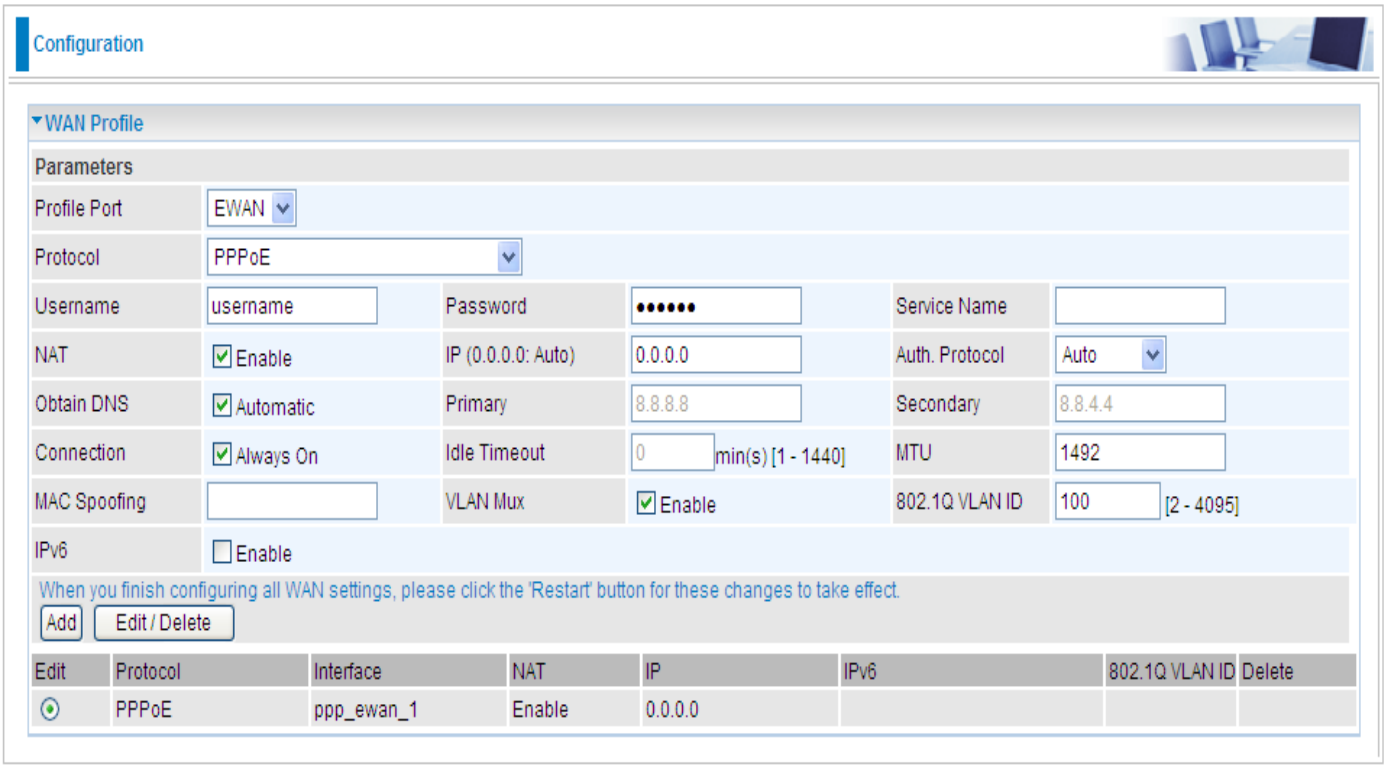
VLAN MUX is a VLAN operation where a VLAN and the user group are one-to-one mapped, a VLAN can be an unique identification for the user group.

Example: IPTV service achieved with VLAN MUX

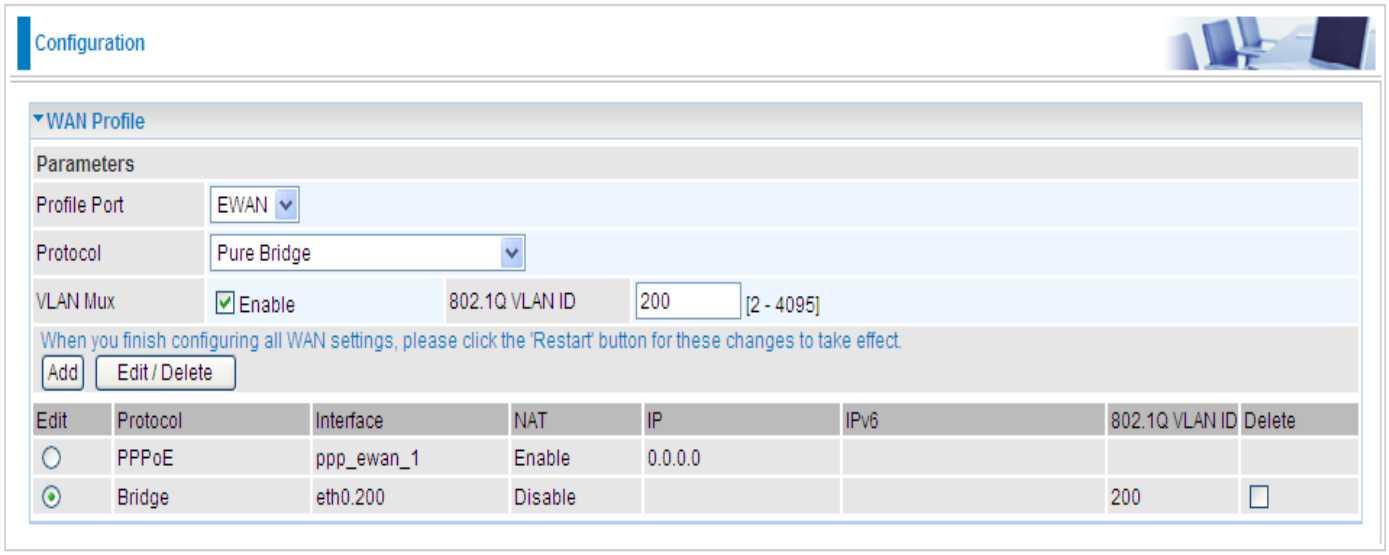
According to your ISP, while the devices in your ISP need VLAN ID information, then VLAN MUX is required to be enabled.

Suppose you want router port 1 for IPTV application, port 2-4 for common application. You want to separate IPTV traffic from common application traffic, you can create two VLANs, thus, VLAN200, for IPTV application, VLAN 100 for common use.

Step 1: Select **Configuration** > **WAN** > **WAN Profile**, in Profile Port field, select **EWAN**. Set PPPoE connection, enter the needed information. Enable VLAN MUX, set 802.1Q VLAN ID 100.

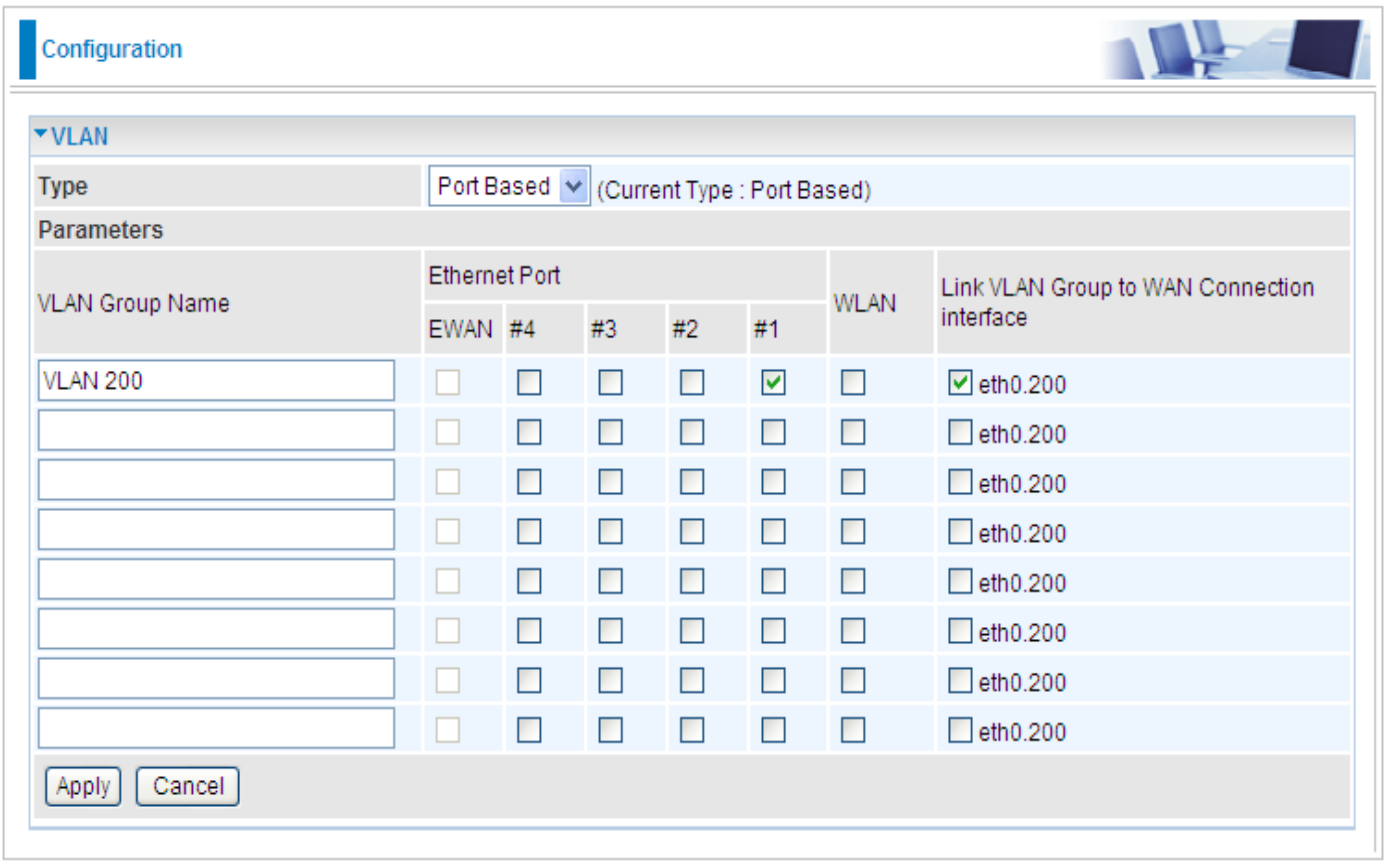


Step 2: Select **Pure Bridge** mode, Enable VLAN MUX, set 802.1Q VLAN ID 200, Click Add.

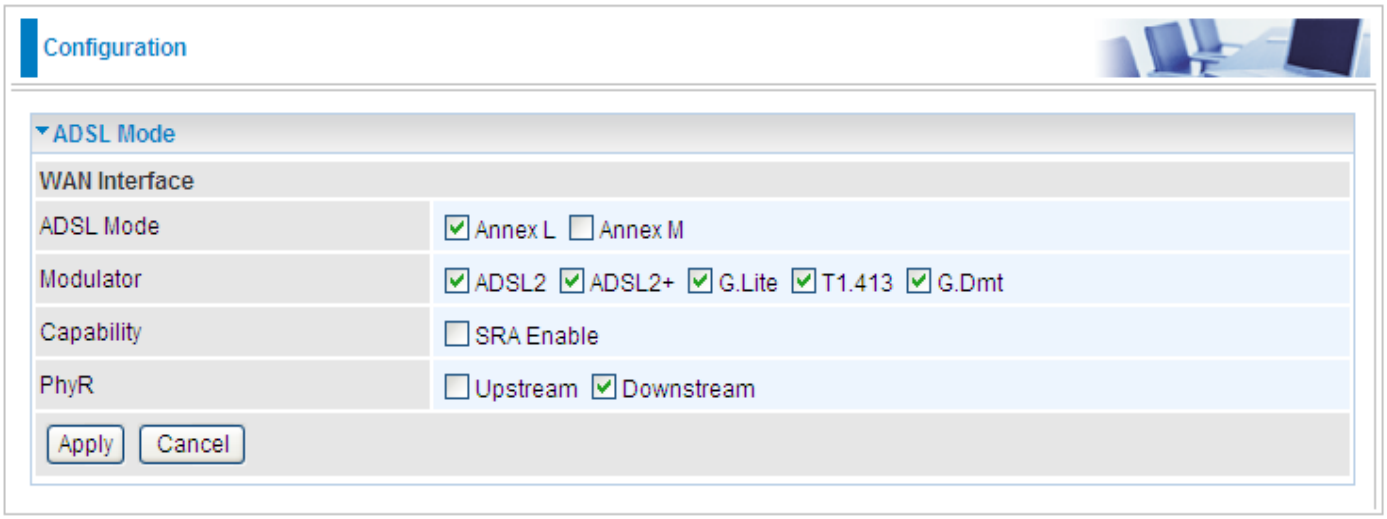


Step 3: Now go to **Configuration** > **Advanced** > **VLAN**, start to set VLAN. Select Port Based VLAN Type, set VLAN Group Name VLAN 200, select port 1 to join in this VLAN group and link this VLAN group to eth0.200 as follows.

Here you have finished your wanted configuration. The port 2-4 and VLAN are automatically perceived as VLAN 100. Thus, you only need to configure VLAN 200 for IPTV application, through VLAN, you can separate the traffic easily and have a wonderful video expericence.



ADSL Mode



ADSL Mode: There are 2 modes “Annex L” and ”Annex M” that user can select for this connection.

Modulator: There are 5 modes “ADSL2”, ”ADSL2+”, “G.Lite:”, “T1.413” and “G.DMT” that user can select for this connection.

SRA: select whether to enable SRA feature. SRA, short for Seamless Rate Adaptation, is a technology used to adapt the rate seamlessly without any influence to the working system, to assure of the quality of the ADSL system.

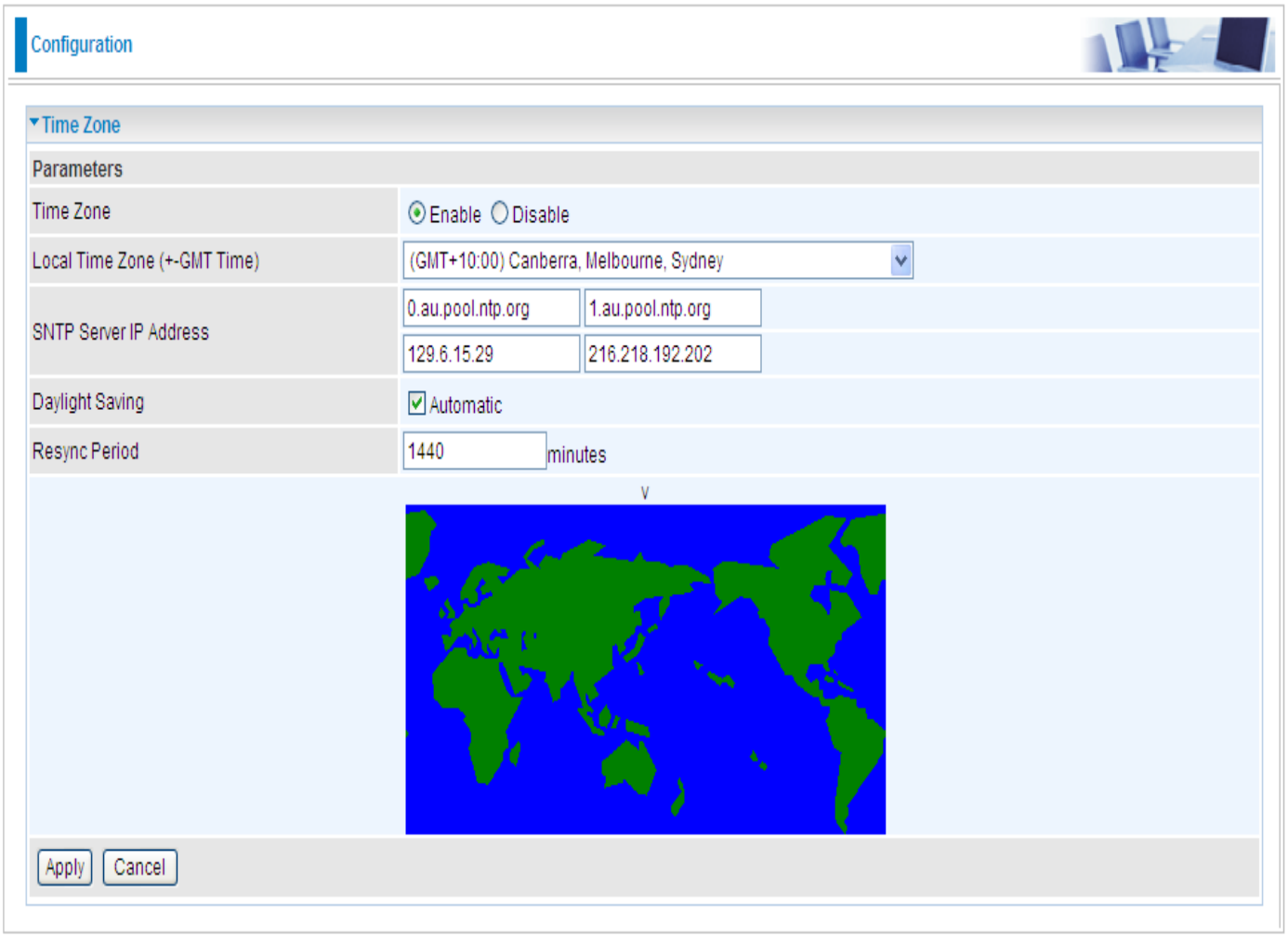
PhyR: An impulse noise protection technology to improve xDLS performance. It was based on your service provider. You can check Upstream and Downstream to improve Upstream or Downstream communication performace.

Click Apply to confirm the change.

System

There are seven items within the System section: **Time Zone, Firmware Upgrade, Backup/ Restore, Restart, User Management, Syslog and Diagnostics Tools.**

Time Zone



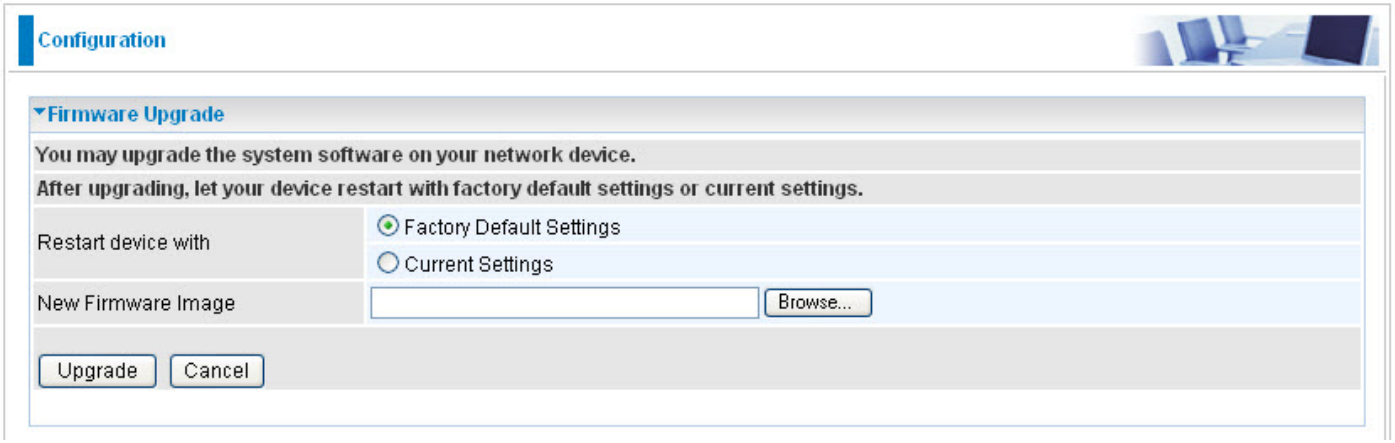
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the most current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP 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.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days. The default value is set at 1440 minutes.

Click Apply to confirm the settings.

Firmware Upgrade

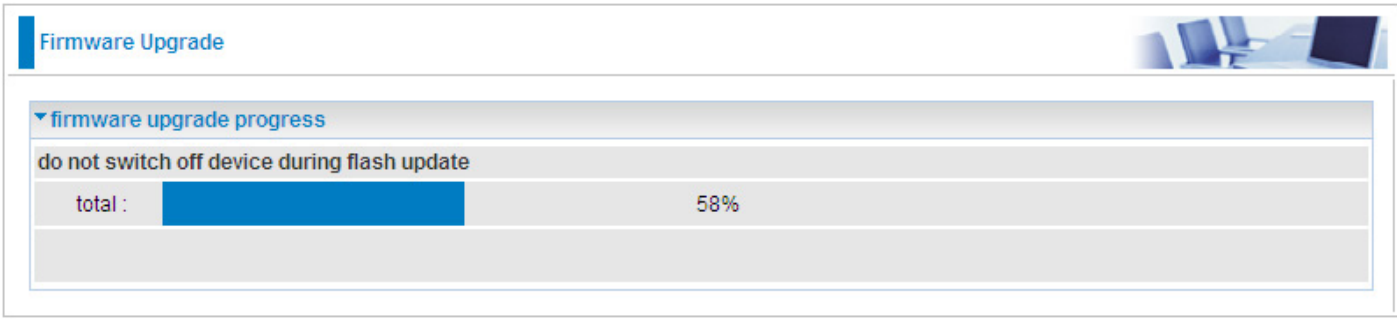
Your router's firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.

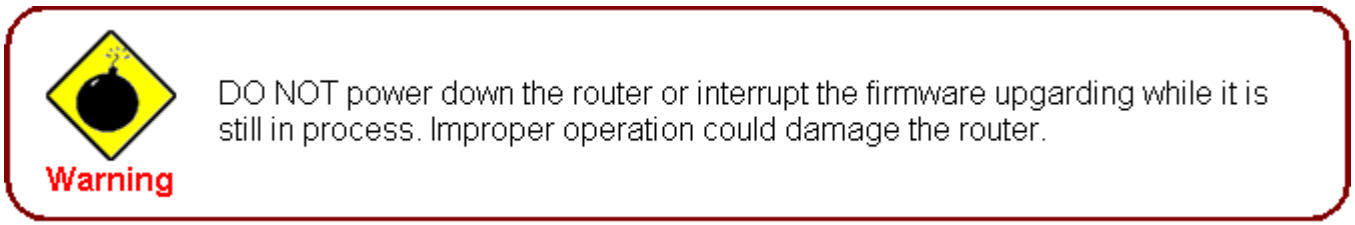


Factory Default Settings: If select this setting, the device will reboot to restore the parameters of all its applications to its default values.

Current Settings: If select this setting, the device will reboot and retain the customized settings of all applications.

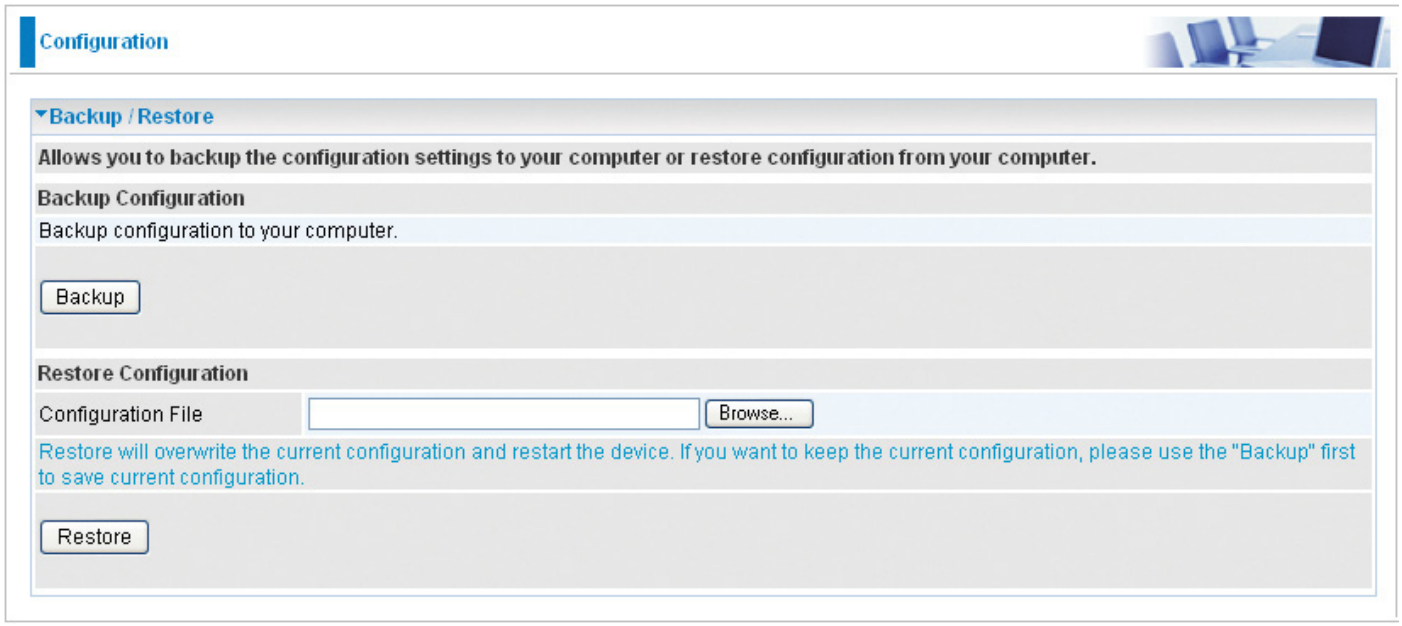
Click on Browse to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware to your router.





Backup / Restore

These functions allow you to save a backup of the current configuration of your router to a defined location on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup in hand in case any mistakes occur. It is advisable that you backup your router configuration before making any changes to your router configuration.



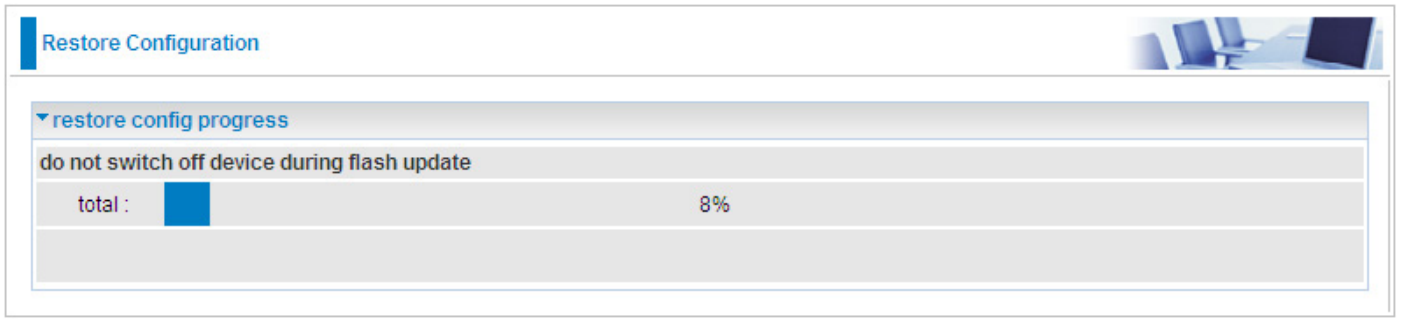
Backup Configuration

Press Backup Settings to select where on your local PC you want to store your setting file. You may also want to change the name of the file when saving if you wish to keep multiple backups.

Restore Configuration

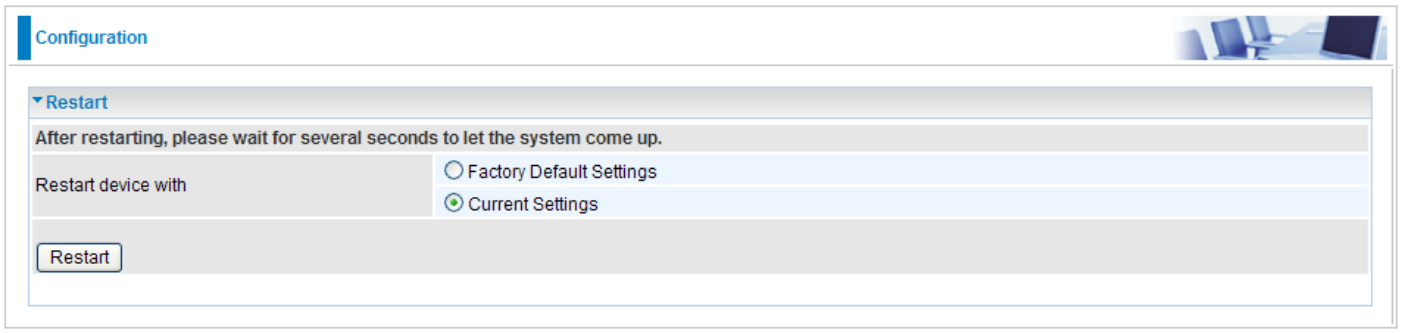
Press Browse to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router firmware. Settings files saved to your PC should not be manually edited in any way.

Select the settings files you wish to use, and press Restore to load the setting into the router. Click Restore to begin restoring the configuration and wait for the router to restart before performing any actions.



Restart

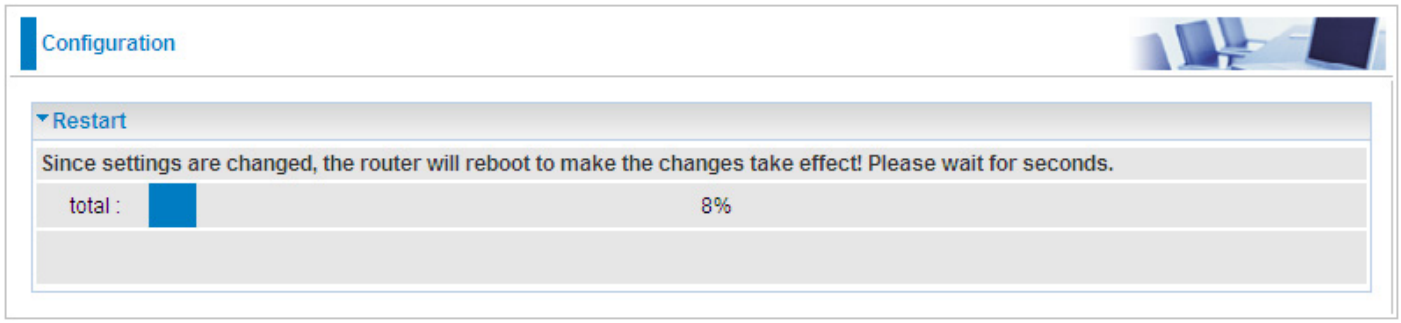
There are 2 options for you to choose from before restarting the your 7800(N) device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.



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.

Click Restart with option Current Settings to reboot your router (and restore your last saved configuration).

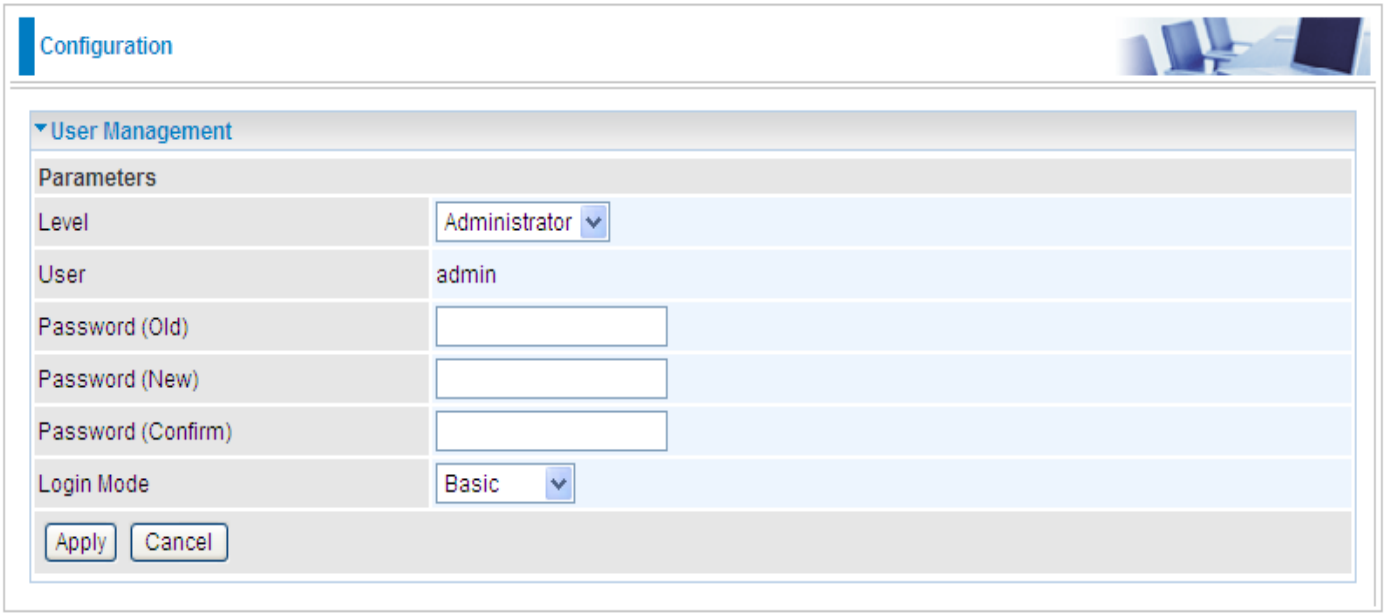
After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.



You may also reset your router to factory settings by holding the small Reset pinhole button more than 1 second on the back of your router.

User Management

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Three user levels are provided here. Each user level there's a default provided password. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.To change your password, simply enter the old password in the Old Password blank. Then enter your new password in the New Password and Confirm Password blanks provided. When this is done, press Apply to save changes.



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

Administrator: the root user, corresponding default username and password are admin and admin respectively.

Advanced: username for the remote user to login, corresponding default username and password are support and support respectively.

Basic: username for the general user, corresponding default username password are user and user respectivley.

User: display the usename.

Password(Old): Enter the old password.

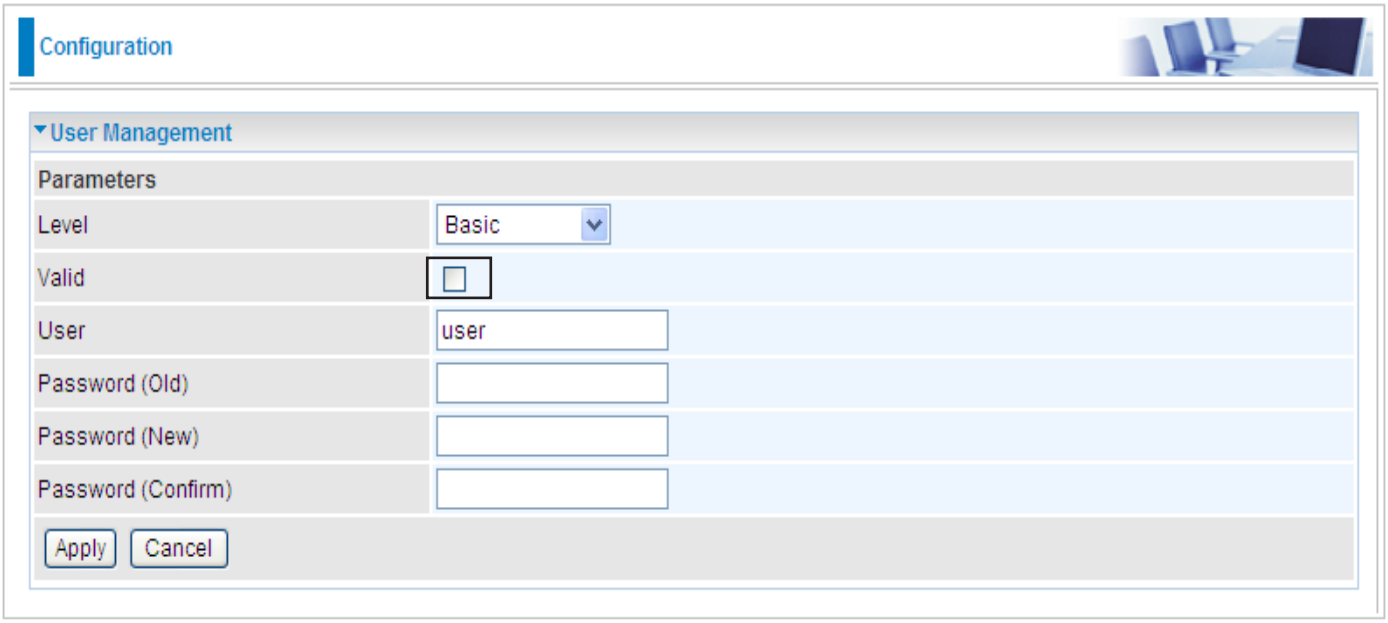
Password(New): Enter the new password.

Password(Confirm): Enter again the new password to confirm.

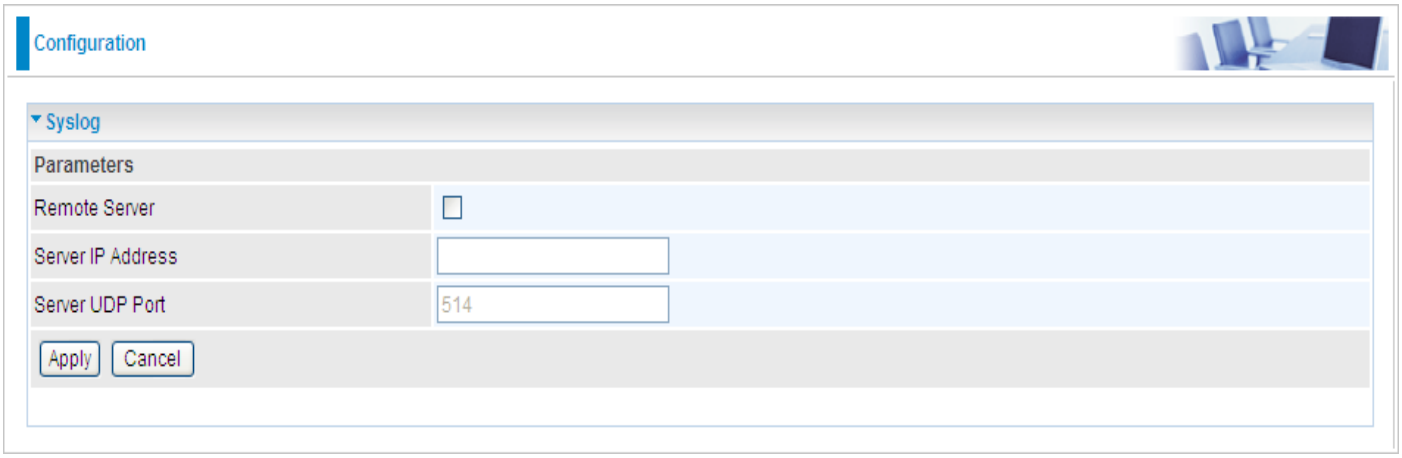
Login Mode: choose to login to which Web GUI configuration page, Basic or Advanced. Basic will lead you to Basic configuration , Advanced will lead you to Advanced configuration.

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

Note: by default the other two users of level Advanced and level Basic, thus user and support, are not available, if you want to use the two accounts, check Valid and set their password. And here username is allowed to change, as follows, usename User in User field can be changed.



Syslog

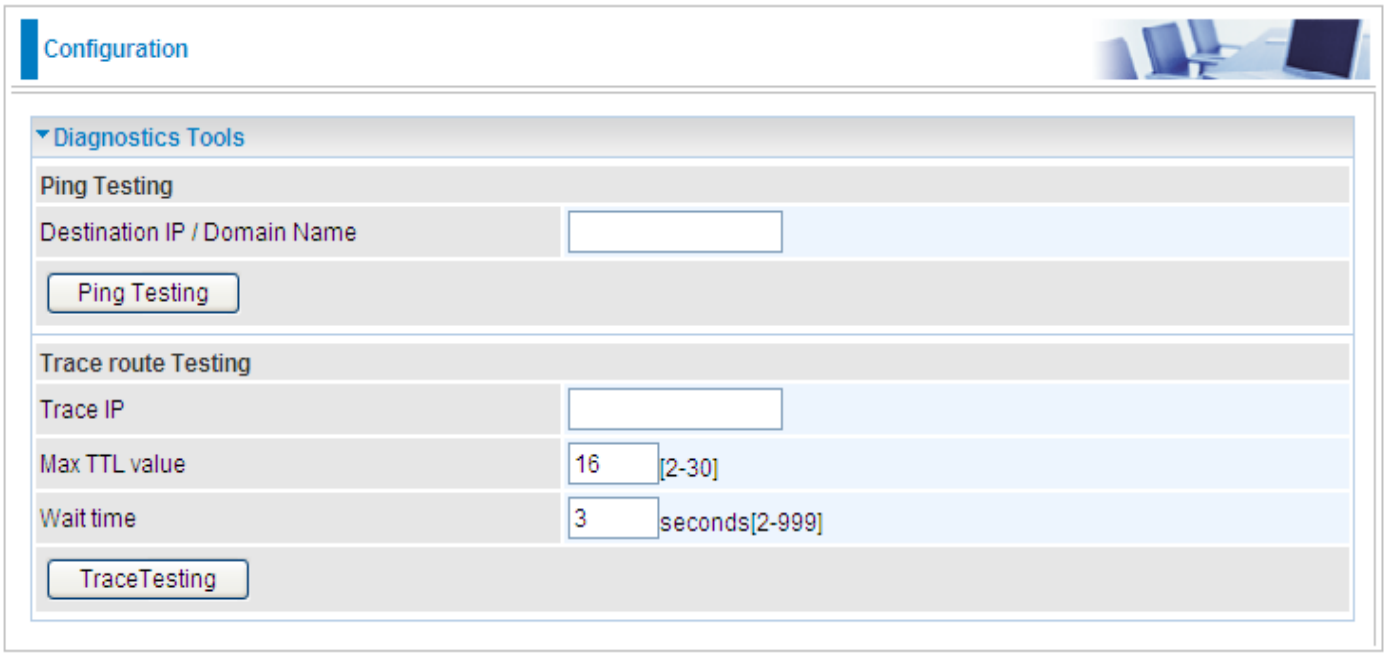


Remote Server: Specify the server that is used to save the device's syslog.

Server IP Address: The IP address of remote server.

Server UDP Port: The UDP Port of remote server.

Diagnostics Tools



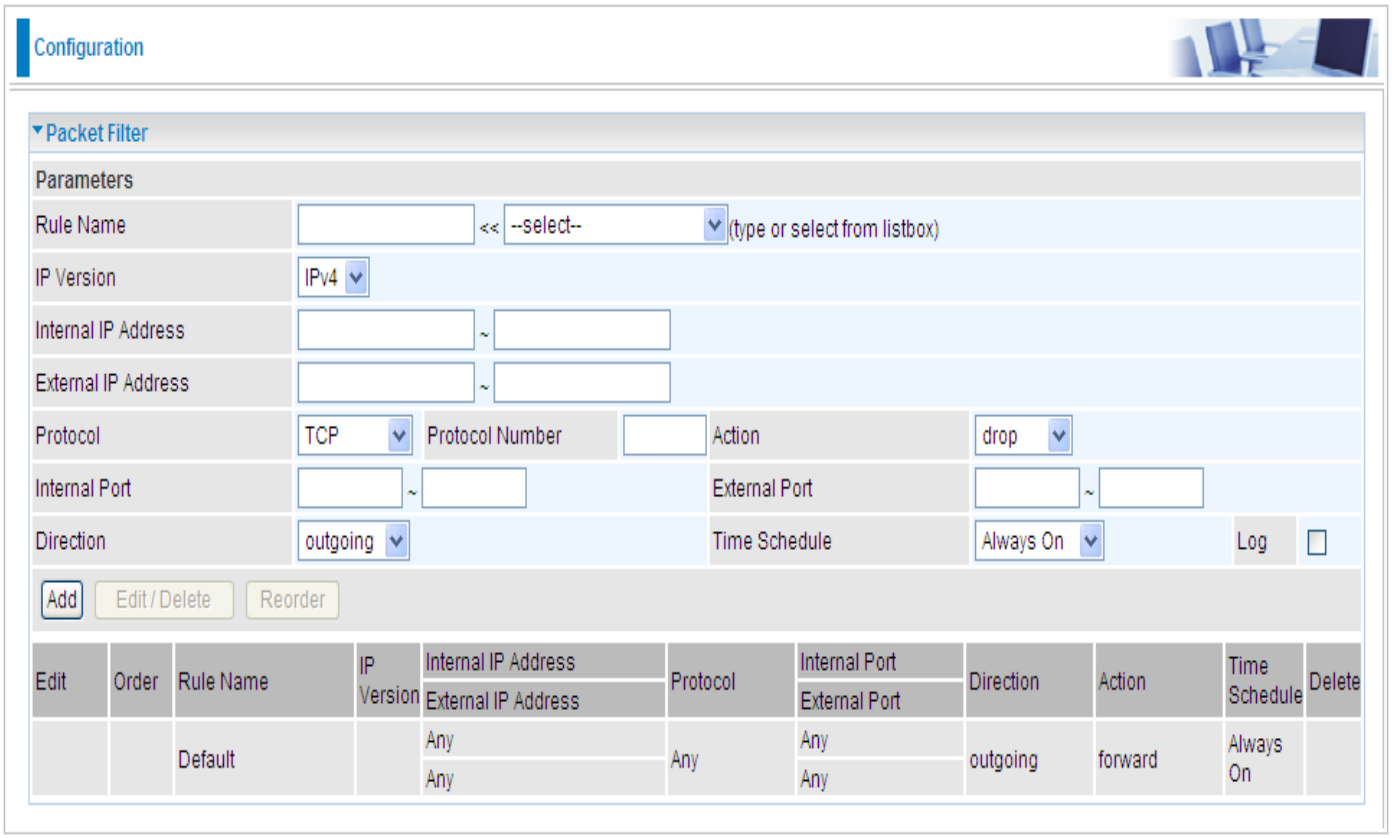
Destination IP / Domain Name: Input the IP or domian name to be tested.

Trace IP: Input IP to be traced.

Firewall

Listed are the items under the Firewall section: **Packet Filter**,**Ethernet MAC Filter, Wireless MAC Filter, Intrusion Detection, Block WAN PING** and **URL Filter.**

Packet Filter



Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. 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.

Rule Name: User defined description for entry identification. The maximum name length is 32 characters, and then can choose an application that they want from the listbox.

IP Version: select either IPv4 or IPv6 base on need.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/rom particular IP address(es). Input the range you want to filter out. If you leave these four fields empty or enter 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, TCP/UDP, RAW, Any) that the rule applies to. Select TCP if you wish to search for the connection-based application service on the remote server using the port number. Or select UDP if you want to search for the connectionless application service on the remote server using the port number. Only when **RAW** is selected, then you can type the protocol number (0-254) to identify the protocol that you want the filter applies to. When **Any** is selected, it means the filter will applies to any protocol.

Protocol Number: type the specific protocol number when **RAW** is selected in the above field.

Action: If a packet matches this filter rule, forward (allows the packets to pass) or drop (disallow the

packets to pass) this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range 1 ~ 65535. It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Select Enable for this option if you will like to capture the logs for this Packet filter policy.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Check the Rule No. you wish to edit, and then click “Edit”.

Delete: Check the Rule No. you wish to delete, and then click “Delete”.

Reorder: Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press “Reorder” to save the new priority.

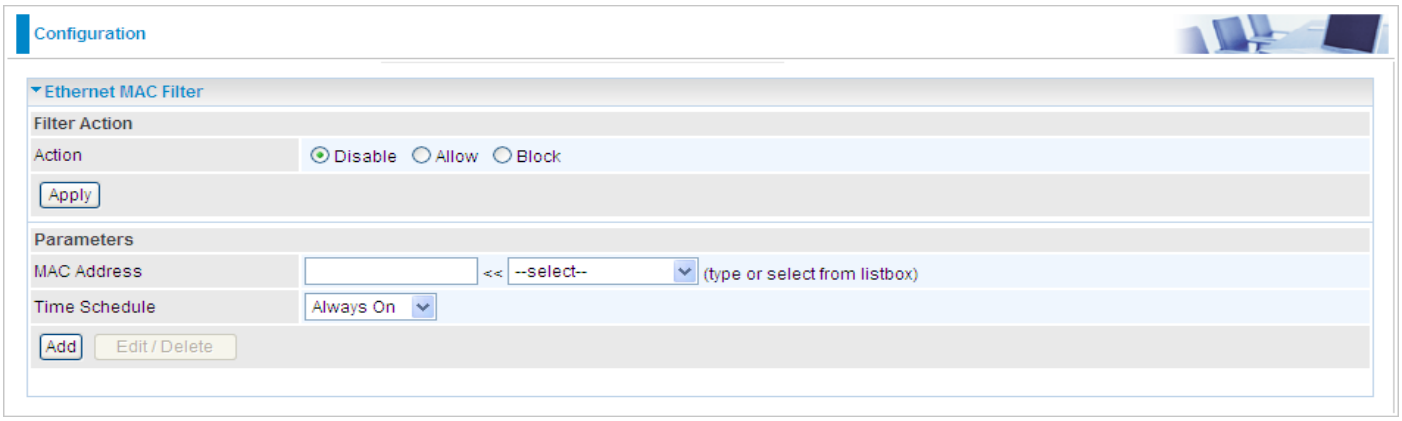
Edit	Order	Rule Name	Internal IP Address External IP Address	Protocol	Internal Port External Port	Direction	Action	Time Schedule	Delete
○	↓	FTP	Any Any	TCP	Any 21 ~ 21	outgoing	drop	Always On	☐
○	↑	HTTP	Any Any	TCP	Any 80 ~ 80	outgoing	drop	Always On	☐
		Default	Any Any	Any	Any Any	outgoing	forward	Always On	

Ethernet MAC Filter

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.

There are no pre-defined MAC address filter rules, you can add the filter rules to you're your requirements.

The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.



Filter Action

Action: Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

Parameters

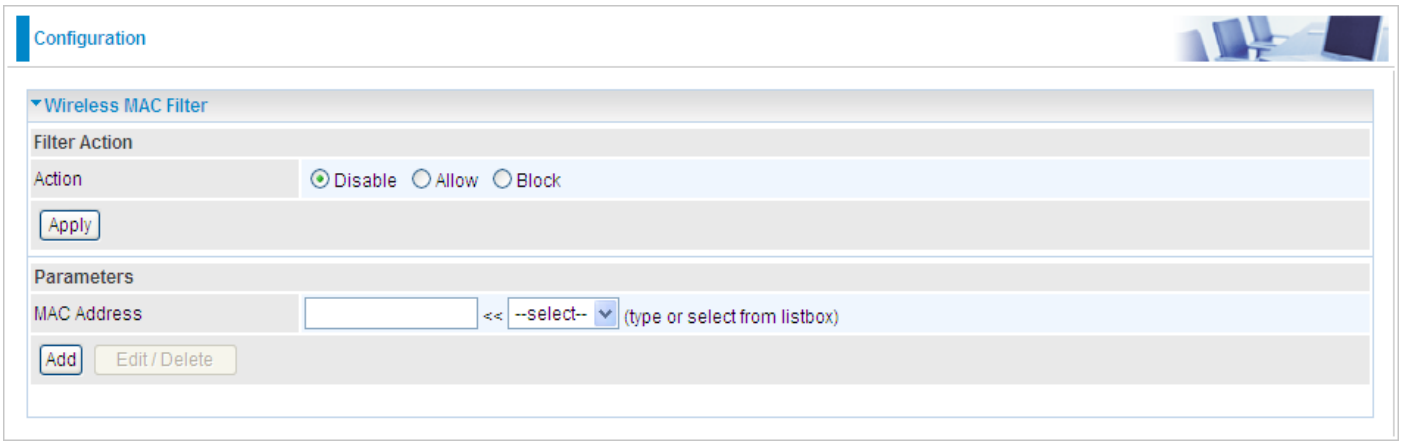
MAC Address: Enter the ethernet MAC addresses you wish to have the filter rule applies.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Wireles MAC Filter

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.

There are no pre-defined MAC address filter rules, you can add the filter rules to you're your requirements.



The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Filter Action

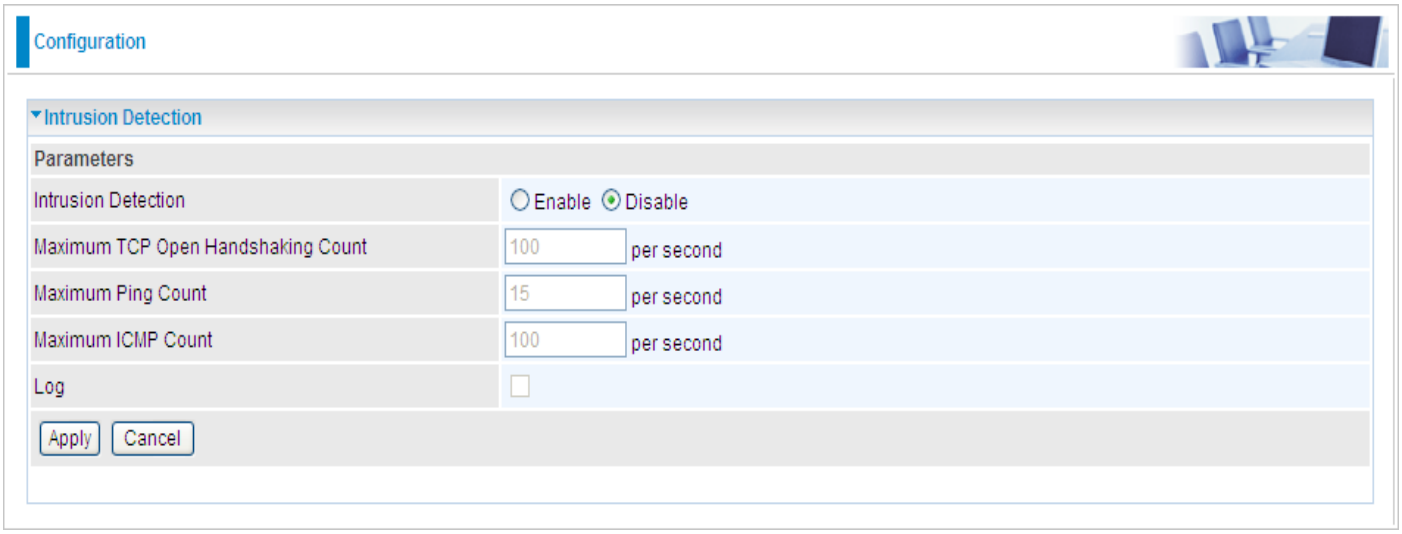
Action: Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

Parameters

MAC Address: Enter the wireless MAC addresses you wish to have the filter rule applies.

Intrusion Detection

The router Intrusion Detection System (IDS) is used to detect hacker's attack and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.



Max TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

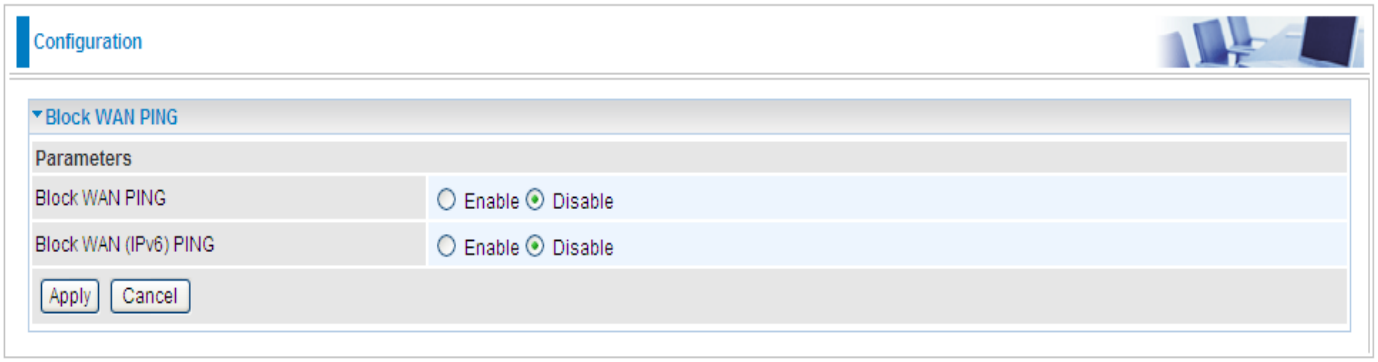
Max PING Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Select Enable for this option if you will like to capture the logs for this Packet filter policy.

Block WAN Ping

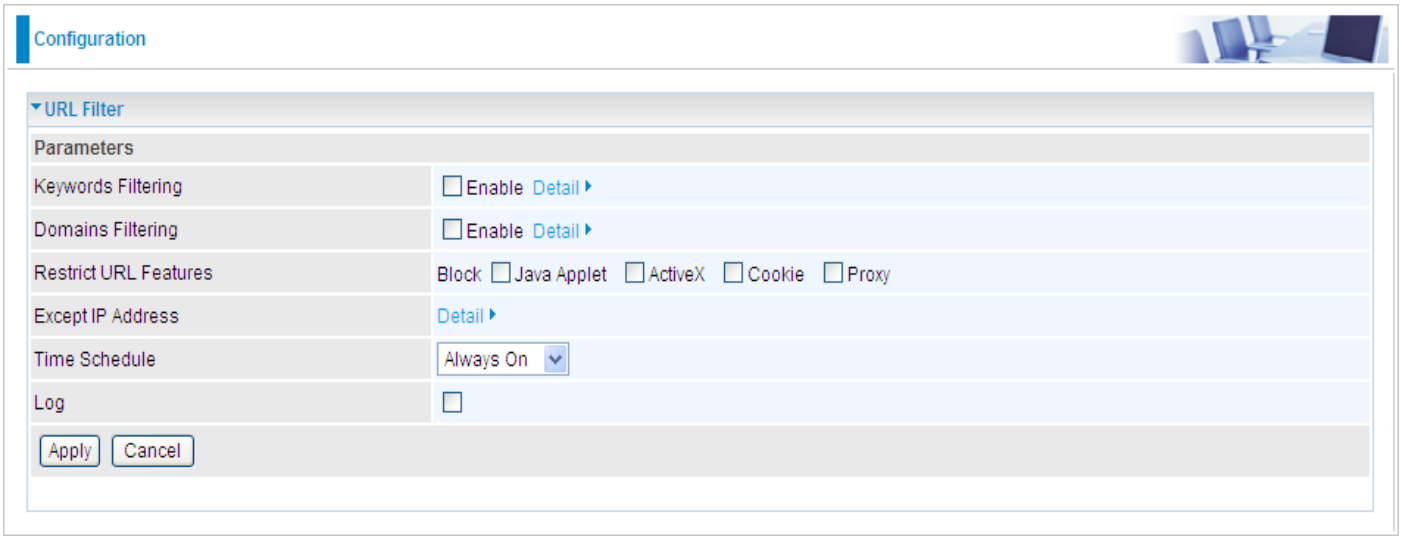
This feature is to be enabled when you want the public WAN IP address on your router not to respond to any ping command.



This feature is disabled by default. To activate the Block WAN PING feature, check the Enable box and then click the Apply button.

URL Filter

URL (Uniform Resource Locator) (e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rule allows you to prevent users on your network from accessing specific websites defined by their URL. There are no predefined URL filter rules, therefore you can add filter rules to meet your requirements.



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.

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).

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.

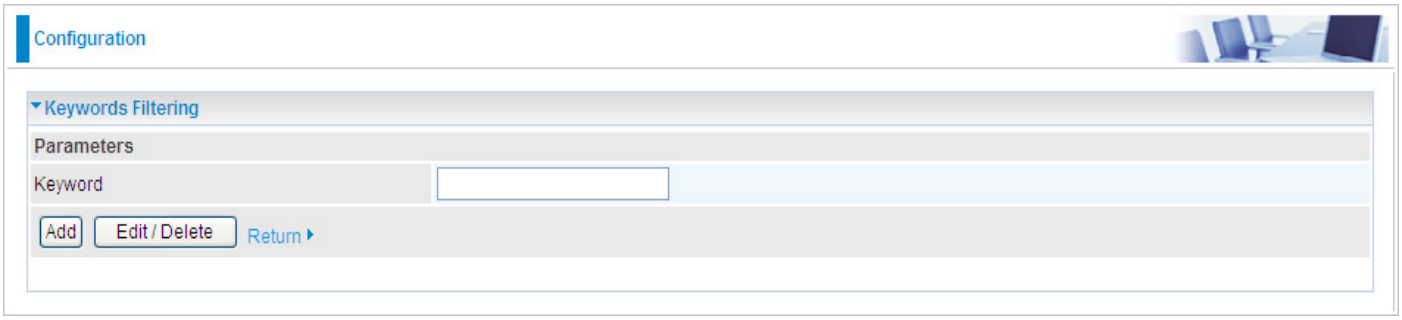
Exception List: You can input a list of IP addresses as the exception list for URL filtering.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy.

Keywords filtering

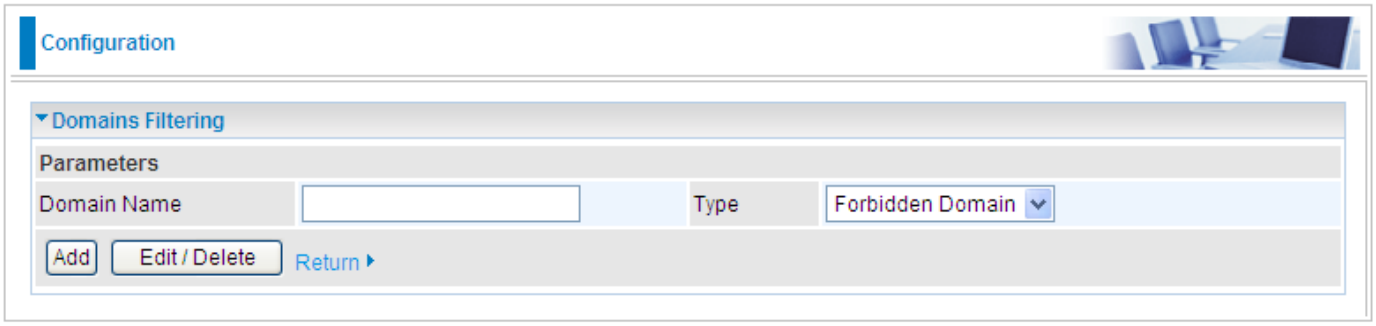
Click the checkbox to enable this feature. To edit the list of filtered keywords, click Details.



Enter a keyword to be filtered and click Apply. Your new keyword will be added to the filtered keyword listing.

Domains Filtering

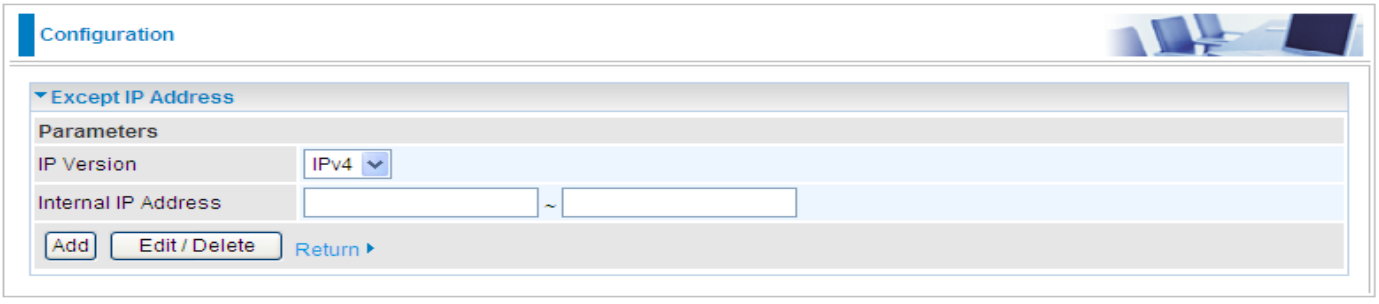
Click the top checkbox to enable this feature. To edit the list of filtered domains, click Details.



Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click Apply. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously.

Except IP Address

You may also designate which IP addresses are to be excluded from these filters by adding them to the Exception List. To do so, click Details.



Select the IP version(IPv4 or IPv6) to identify of which IP version you will enter the IP, then type the except IP address range. 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.

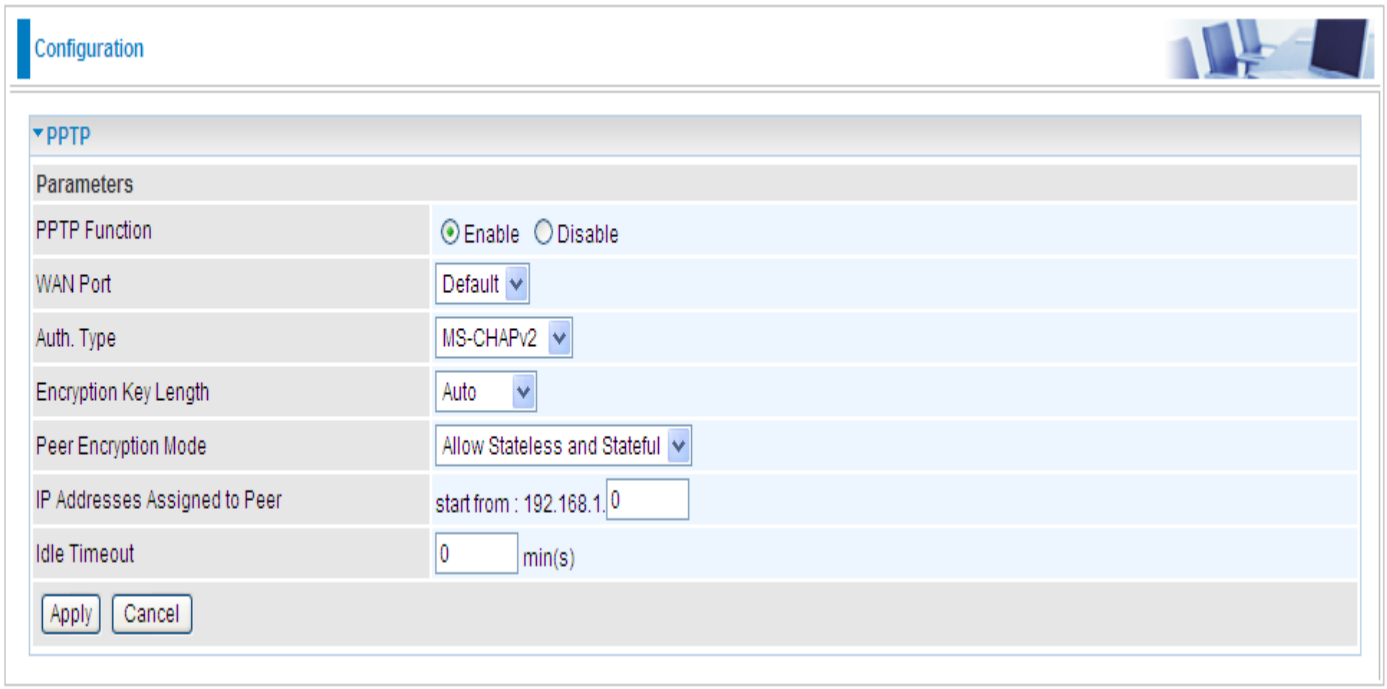
VPN

A virtual private network (VPN) is a computer network that is constructed by using public networks or wires such as Internet to provide remote offices or individual users to get secure access to their organization's network. This network uses encryption and other security mechanisms to ensure that only authorized users are able to participate in the communications and that the data cannot be intercepted. It aims to avoid an expensive system of privately owned or leased lines that can be used by only one organization.

The use of a public network, usually the Internet, to connect securely to a private network, is the basis of a VPN. Companies and organizations will use a VPN to communicate confidentiality over a public network; the VPN can be used to send voice, video or data. It is an excellent option for remote workers and organizations with global offices and partners to share data in private manner.

You can find three items under the VPN section: PPTP, PPTP Account and PPTP Client.

PPTP



PPTP Funtion: Select Enable to activate PPTP Server. Disable to deactivate PPTP Server function

WAN Port: select ADSL means you establish a PPTP VPN base on ADSL port, when you use ADSL for conneting to the internet, you then can this VPN.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap and MS-CHAPv2. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

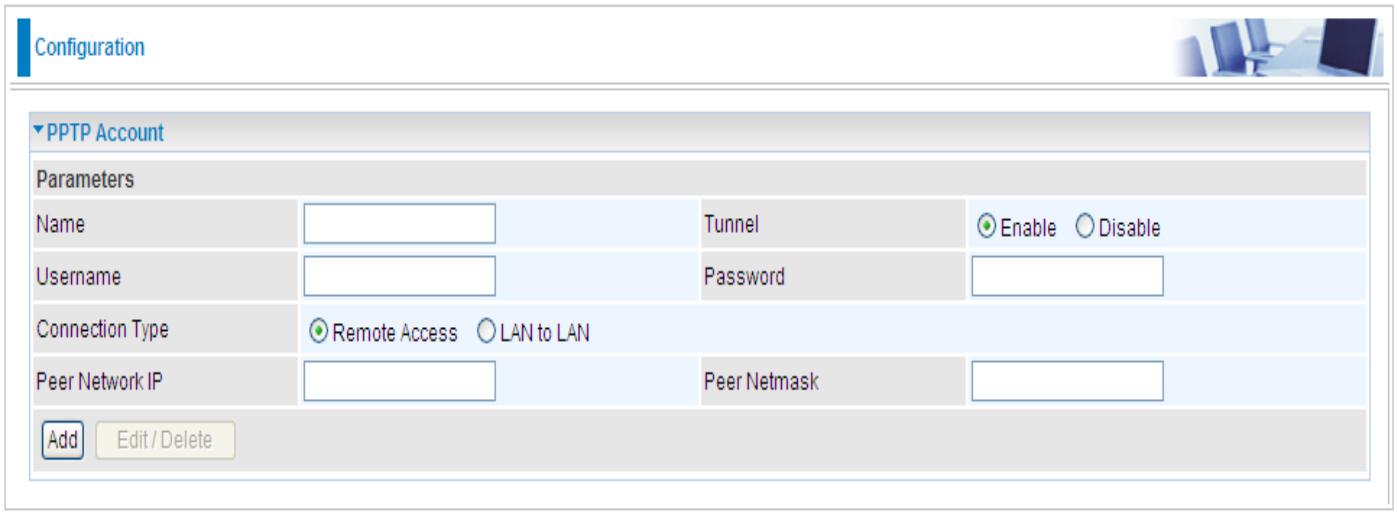
Peer Encryption Mode: You may select Stateful or Stateless mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254

(except BiPAC 7800N's LAN IP address with 192.168.1.254 as BiPAC 7800N's default LAN IP address and IP pool range of DHCP server settings with 100~199 as BiPAC 7800N''s default DHCP IP pool range.)

Idle Timeout: Specify the time for remote peer to be disconnected without any activities, from 0~120.

PPTP Account



Connection Name: A user-defined name for the connection.

Tunnel: Select Enable to activate this tunnel. Select Disable to deactivate this tunnel.

Username: Please input the username for this account.

Password: Please input the password for this account.

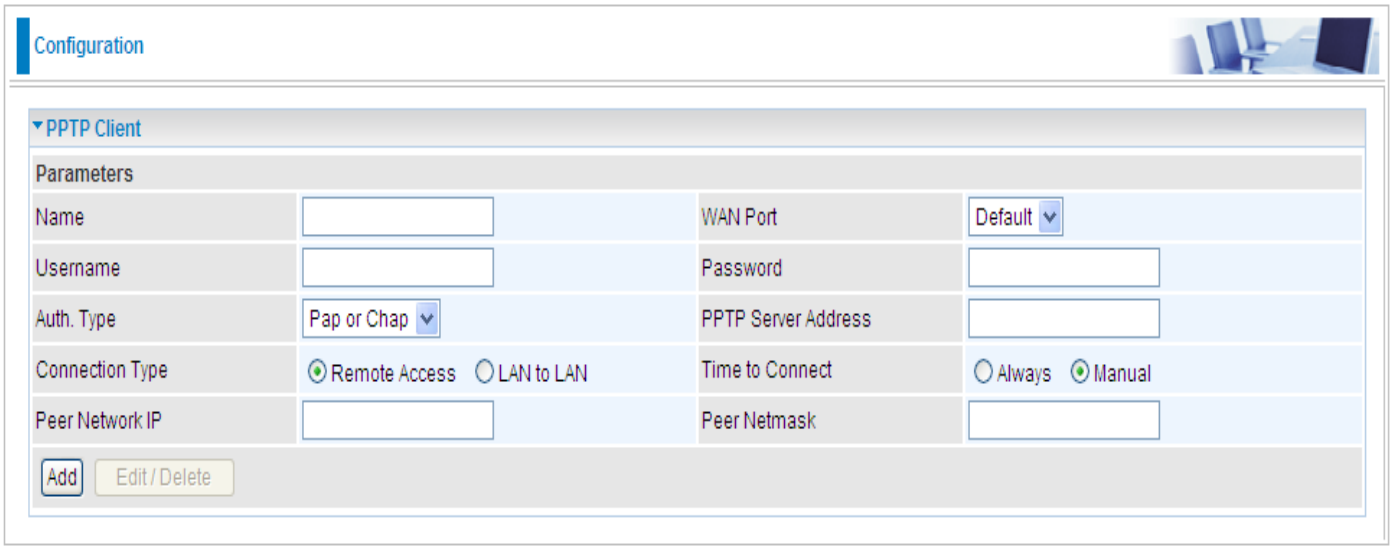
Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

PPTP Client

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.



Name: user-defined name for identification.

WAN Port: select the WAN port the PPTP Client are based on.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

Auth. Type: Default is Auto if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replacedthe client.

PPTP Sever Address: Enter the Server IP Adress or Domain Name.

Connection Type: Remote Access or LAN to LAN.

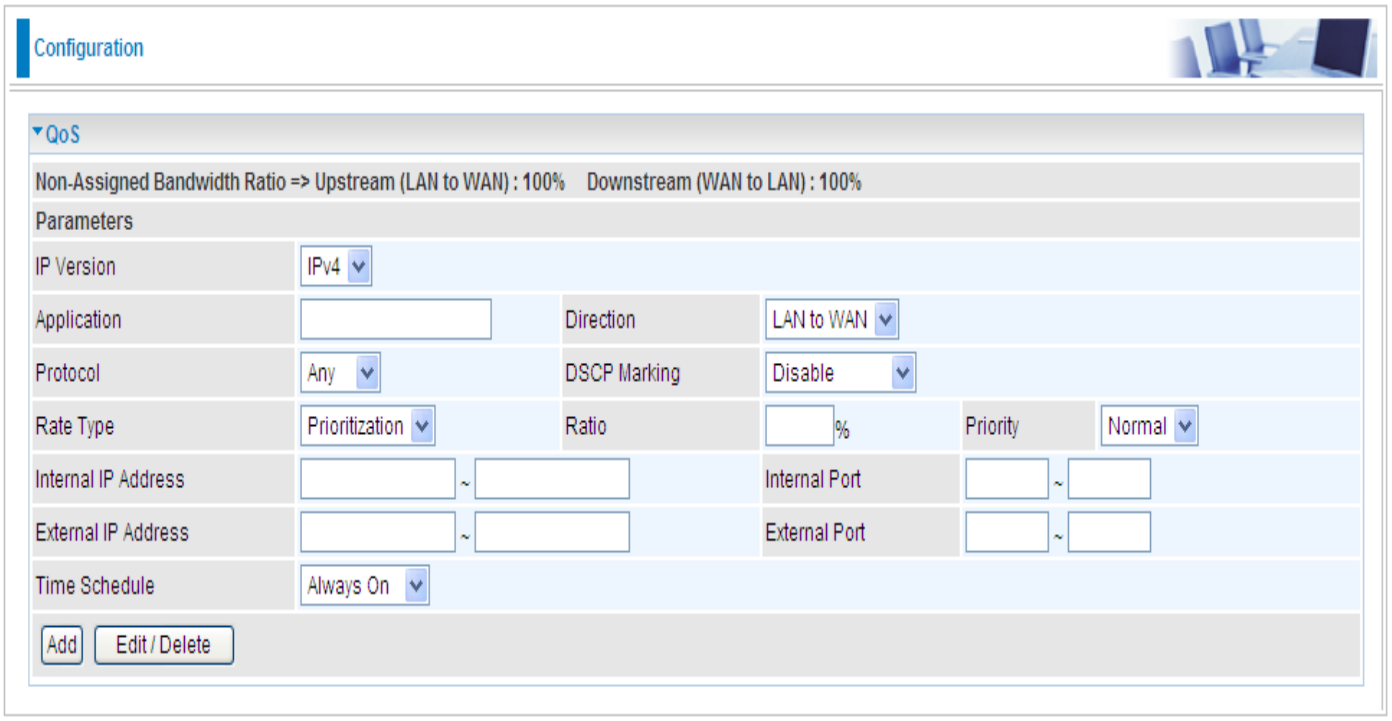
Time to Connect: The connected time could be set as “Aways” or “Manual”.

Peer Network IP: Enter Peer Network IP (when you select LAN to LAN connection type, please set the peer network IP and Netmask.

Peer Netmask: Enter the Peer Netmask.

QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet and/ or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.



IP Version: Select either IPv4 or IPv6 base on need.

Application: Assign a name that identifies the new QoS application rule.

Direction: Shows the direction mode of the QoS application.

- **LAN to WAN:** You want to control the traffic flow from local network to the ouside(Upstream). You can assign the priority for the application or you can limit the rate of the application. Eg: you have a FTP server inside the local network and you want to have a limited controlled by the QoS policy and so you need to add a plicy with LAN to WAN direction setting.
- **WAN to LAN:** Control traffic flow 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.

Rate Type: You can choose Limited or Guaranteed.

- **Limited (Maximum):** specify a limited data rate for this policy. It also is the maximal rate for this pilicy. 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:** to specify the rate type control for the rule to used. If you choose Prioritization for the rule, you parameter Priority would be available, you can set the priority for this rule.

Ratio: The rate percent in contrast to that on WAN interface given to each policy/application with limited rate type.

Priority: The priority given to each policy/application. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.**Internal IP Address:** The private IP in the LAN network.

External IP Address: The IP address on the Internet.

Internal Port: The Port number on the LAN side.

External Port: The Port number on the Remote/WAN side.

Time Schedule: A self defined time period. You may specify a time schedule for your QoS policy. For setup and detail, refer to Time Schedule section.

Note: Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.

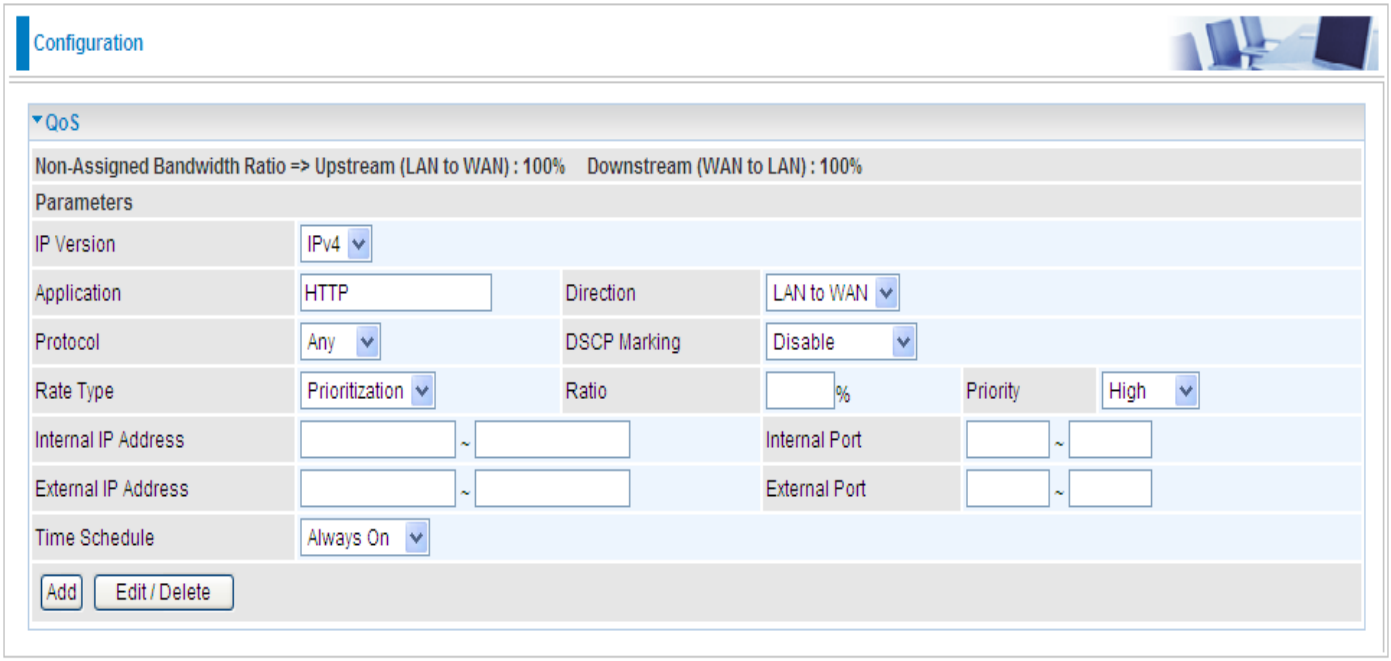
Example 1: Optimize Your Home Network with QoS

If you are actively engaged in using P2P and are afraid of slowing down internet access throughput of other users within your network, you can thus use QoS function to set different priorities for the different applications that members of your network will be using to avoid bandwidth traffic from getting overloaded.

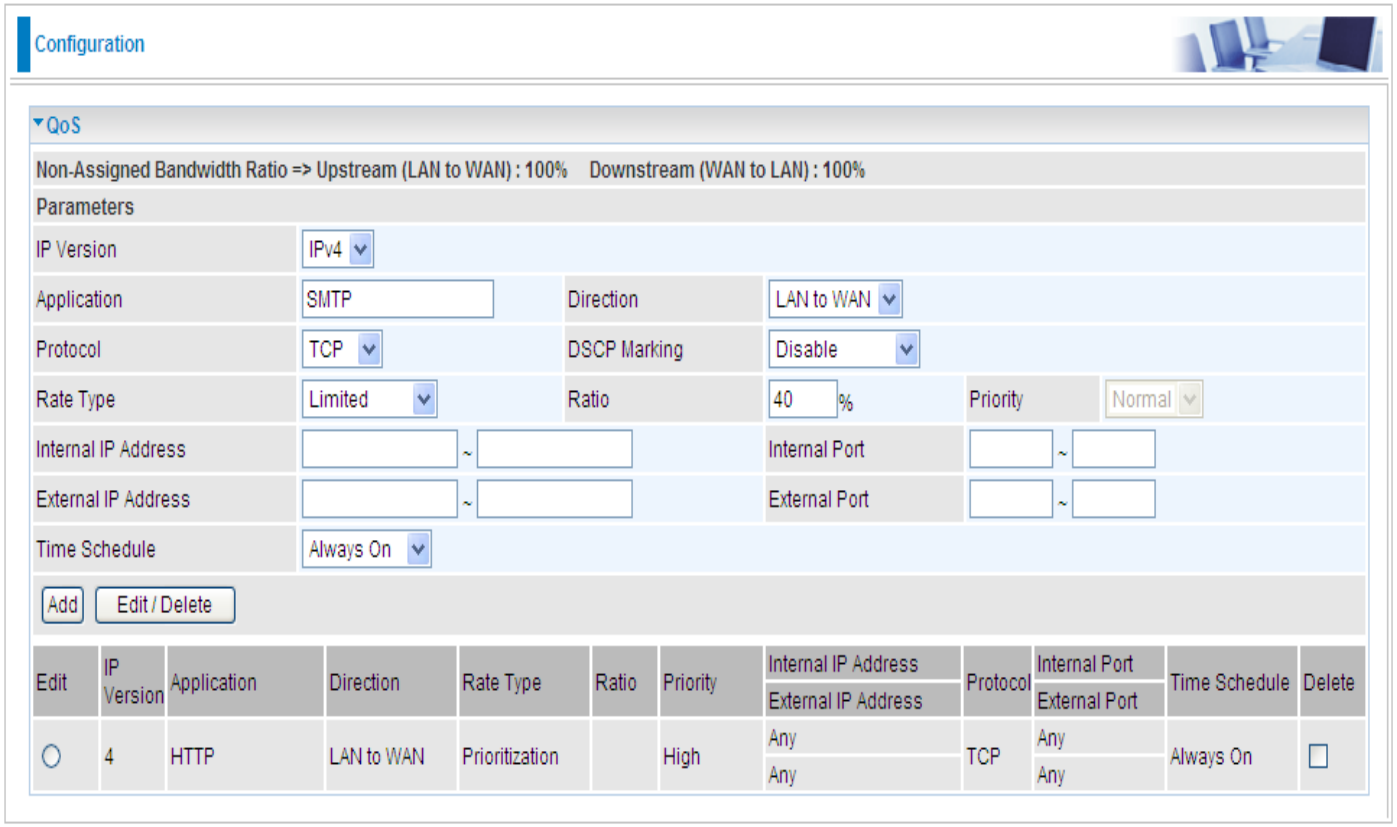
Therefore, in order to assign the priority status of each application, we must first create a new QoS rule for each application.

The figures below show the different settings for assigning a High Priority status to Web Browsing, assigning limited rate for Email send & receive.

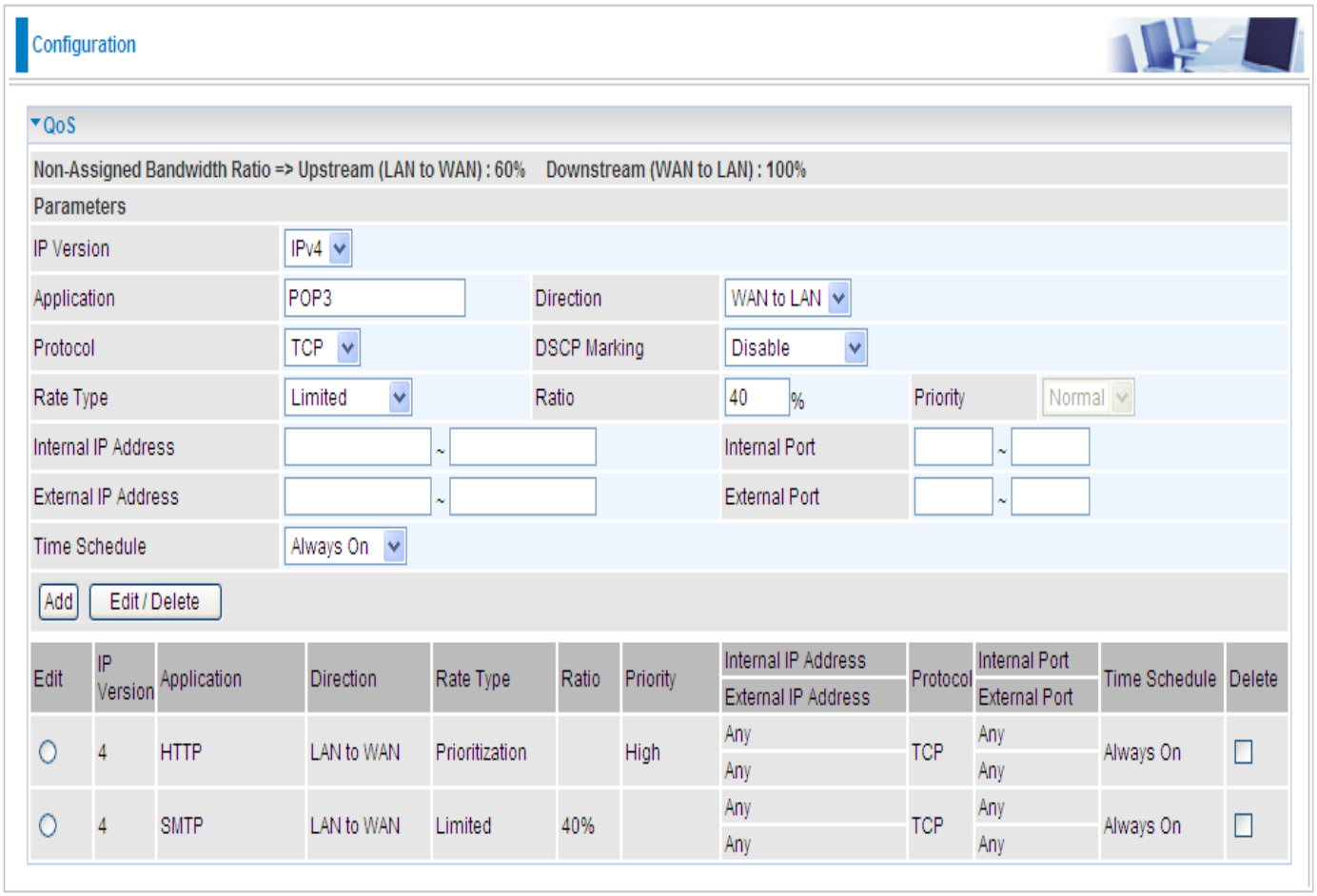
For Web Browsing



For Mail Sending



For Mail Receiving

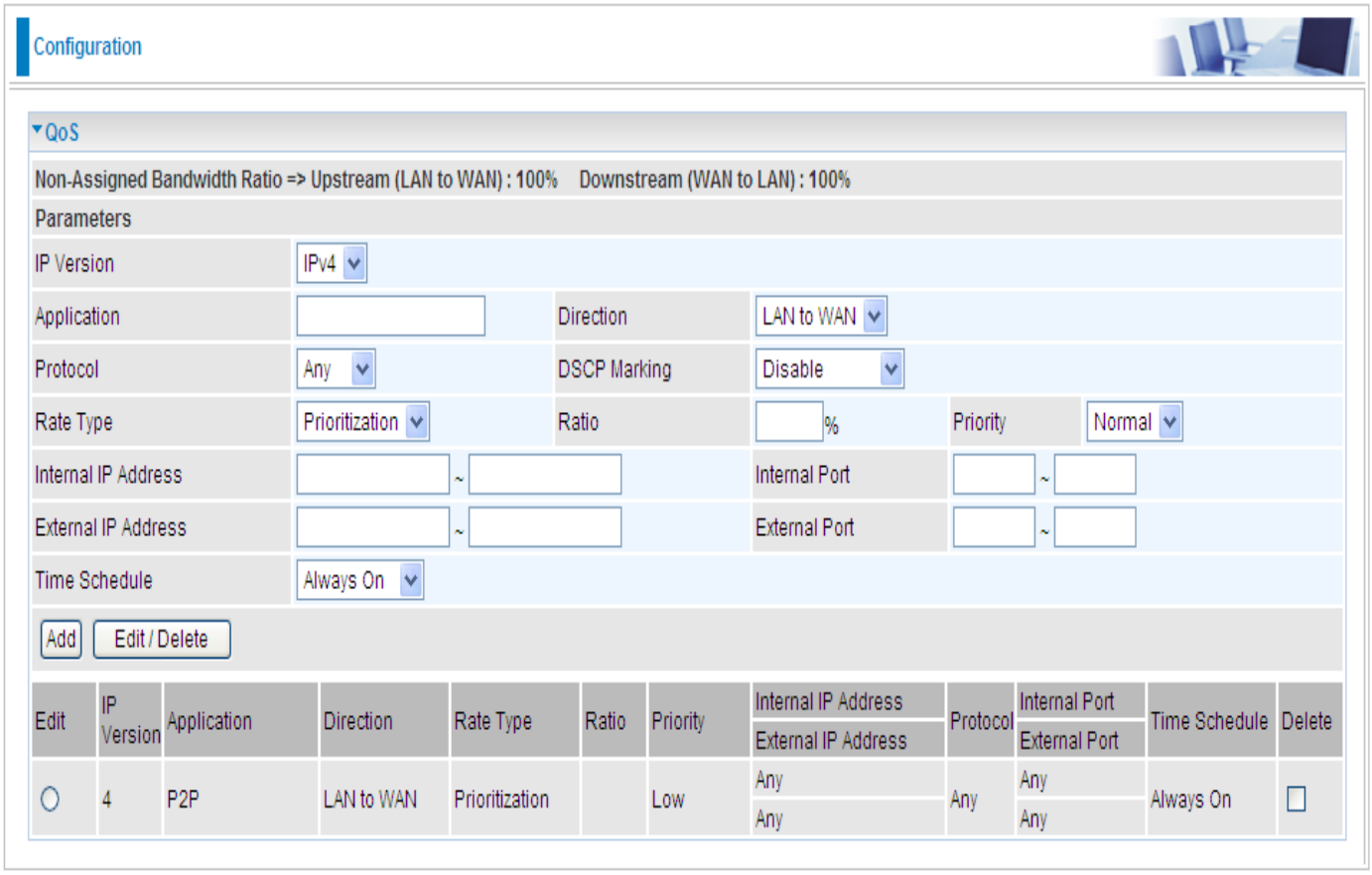


QoS Rules created

Edit	IP Version	Application	Direction	Rate Type	Ratio	Priority	Internal IP Address / External IP Address	Protocol	Internal Port / External Port	Time Schedule	Delete
○	4	HTTP	LAN to WAN	Prioritization		High	Any / Any	TCP	Any / Any	Always On	☐
○	4	SMTP	LAN to WAN	Limited	40%		Any / Any	TCP	Any / Any	Always On	☐
○	4	POP3	WAN to LAN	Limited	40%		Any / Any	TCP	Any / Any	Always On	☐

Example 2: Optimize Your Home Network with QoS

If you are only using a specific PC for the P2P application, you can create a rule that has a low priority. In this way, P2P application will not congest the data transmission rate when there are other applications present.



Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

In TCP 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.

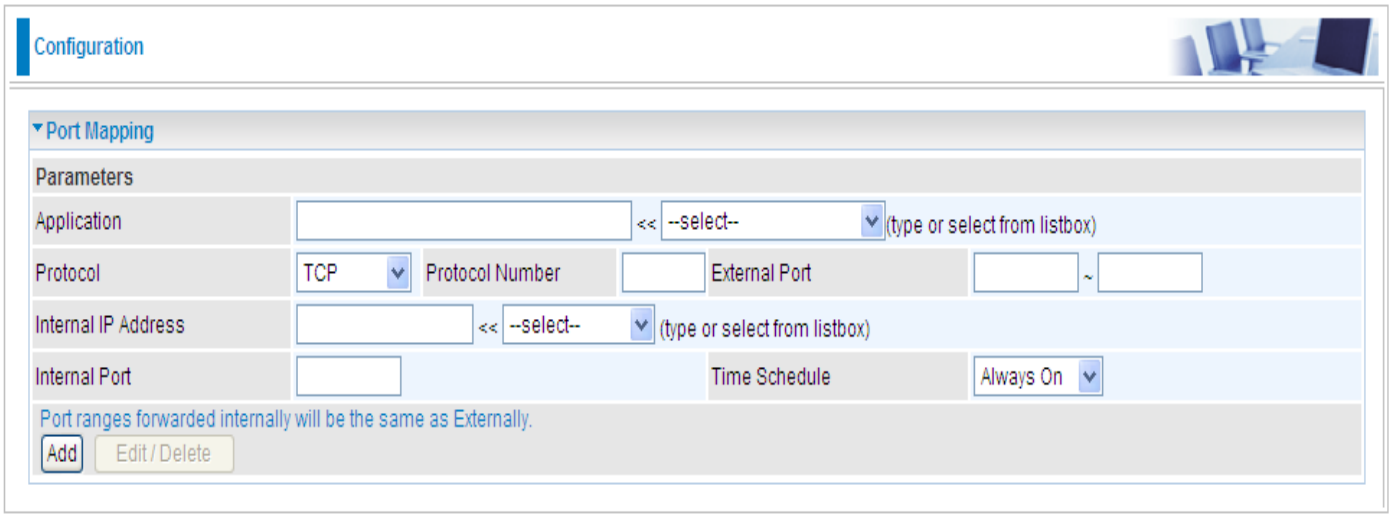
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: **http://www.iana.org/assignments/port-numbers**

Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	TElnet
25	TCP	SMTP (simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	Real Audio

Port Mapping



Application: Select the service you wish to configure.

Protocol: A protocol is automatically applied when an Application is selected from the listbox or you may select a protocol type which you want. But when **RAW** is selected, you must set the protocol number to identify the protocol that the application utilzie.

Protocol Number: when RAW is selected in Protocol field, then type the specific protocol number (1~254) here.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Add: Click to add a new virtual server rule. Click again and the next figure appears.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the Edit/Delete button to apply the changes.

Delete: To remove a port mapping application, check the Remove box of the selected application then click the Edit/Delete button.

Time Schedule: A self defined time period. You may specify a time schedule for your port mapping. For setup and detail, refer to Time Schedule section.

Since NAT acts as a “natural” Internet firewall, your router protects your network from accessed by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request the router for a specified port is received, it is forwarded to the corresponding internal server.

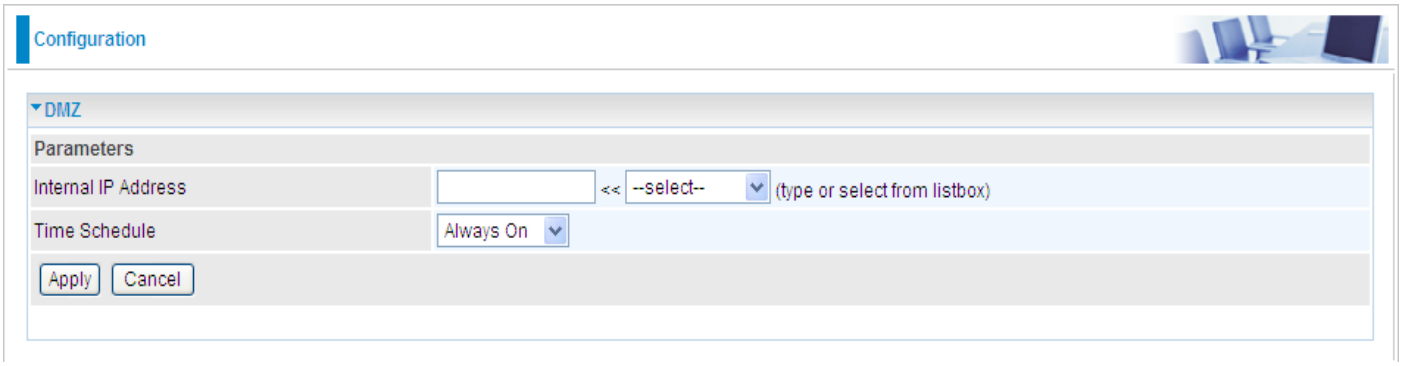
For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
○	FTP	TCP	21	192.168.1.25	21	Always On	☐
○	HTTP	TCP	80	192.168.1.2	80	TimeSlot2	☐

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by a particular application. Most applications use TCP or UDP, however you may also specify other protocols using the drop-down Protocol menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ

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 that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host. When this is done, press Apply to save the changes.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP 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.

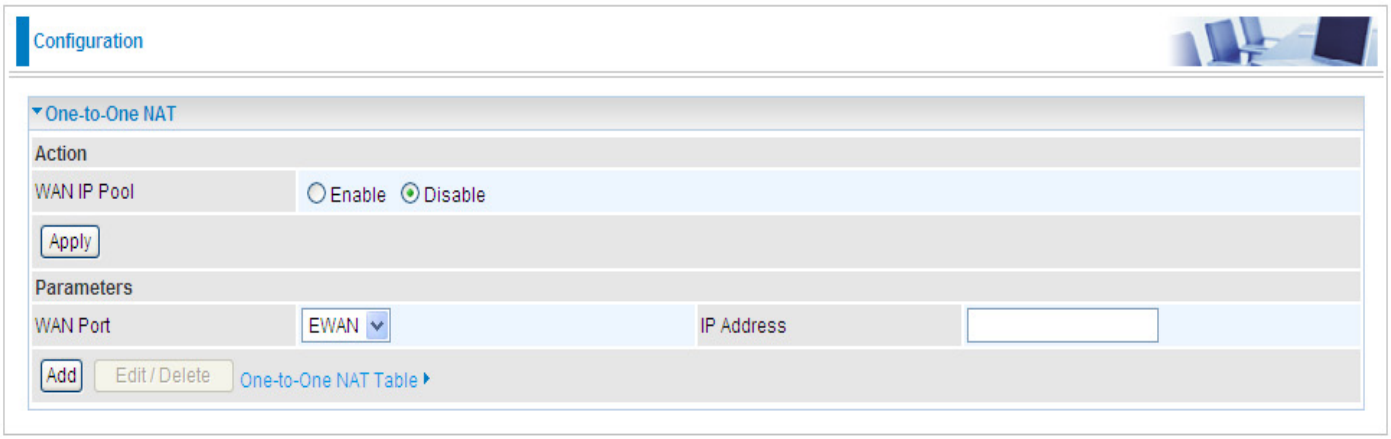
NOTE:

Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore adviced to use specific Virtual Server entries just for those ports that your applications require.

One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address.

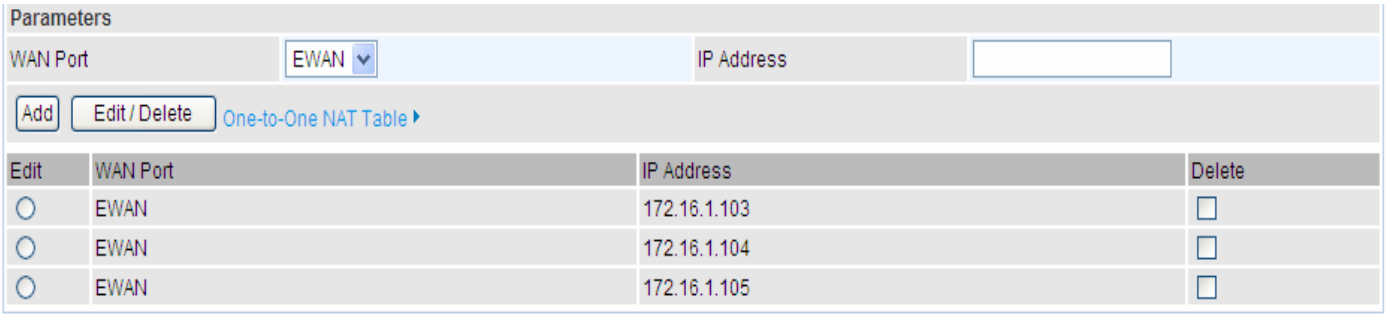
If you have multiple public/WAN IP address from your ISP, you are eligible for One-to-One NAT to utilize these IP addresses.



WAN IP Pool: select Enable to activate the feature and Click Apply to submit your configuration.

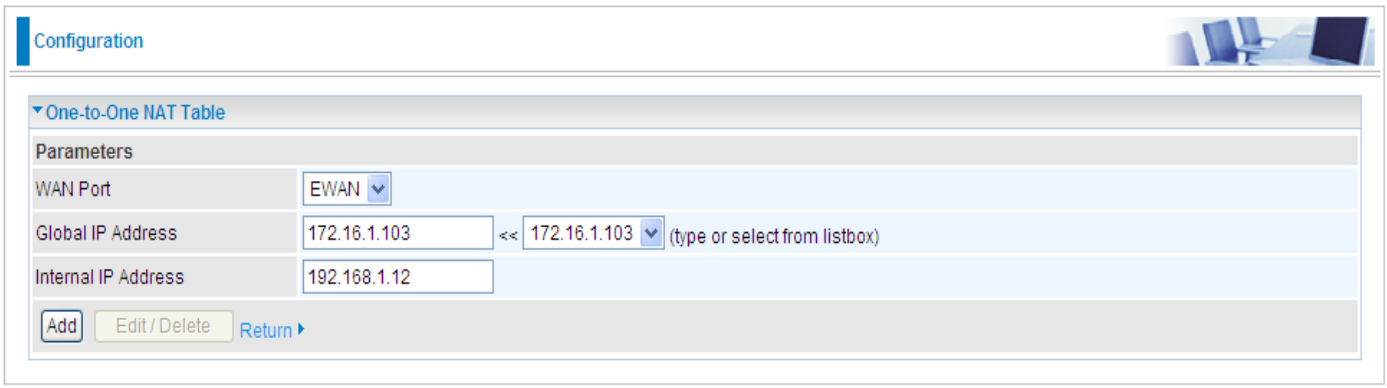
WAN Port: choose the WAN port you are going to configure multiple IPs for One-to-One NAT. for example, you have three available public IPs from 172.16.1.103-172.16.1.105 (internal test for instance), you can add these IPs respectively to the following IP Address field.

IP Address: Type each available WAN IPs to this field and Click Add to add respectively to show as below.



Then Click 

to go on distributing the WAN IP to the specific local IP.

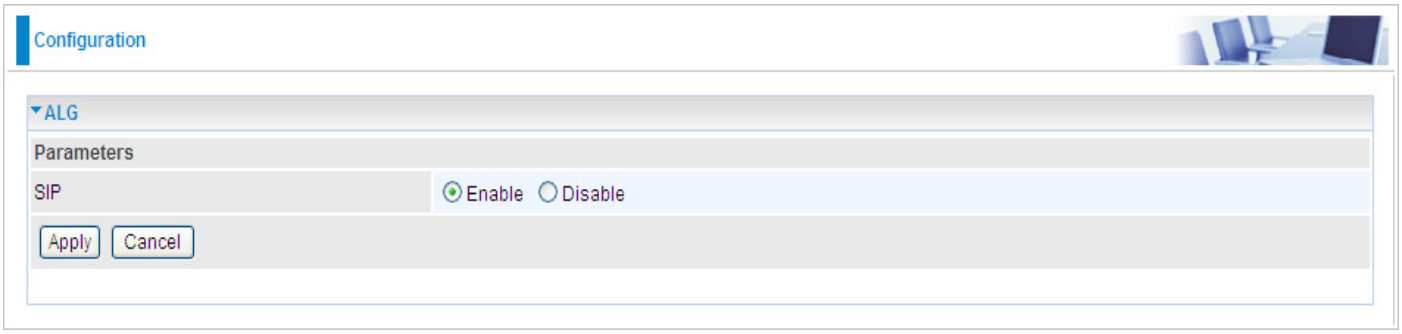


Global IP Address: the set WAN IP, you can type manually or select if you have add to the list before.

Internal IP Address: set the concrete local IP you want to map to the WAN IP.

ALG

Controls enable or disable various protocols over application layer.



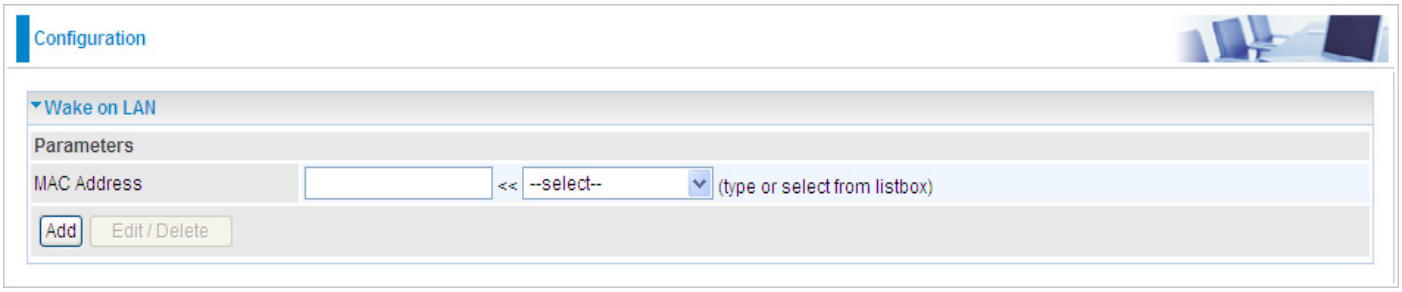
For example, SIP ALG:

Enable: When SIP phone need ALG to pass through the NAT.

Disable: When SIP phone included NAT-Traversal algorithm. Turn off the SIP ALG.

Wake on LAN

This feature provides greater flexibility for users to turn on / boot the computer of the network from a remotely site.



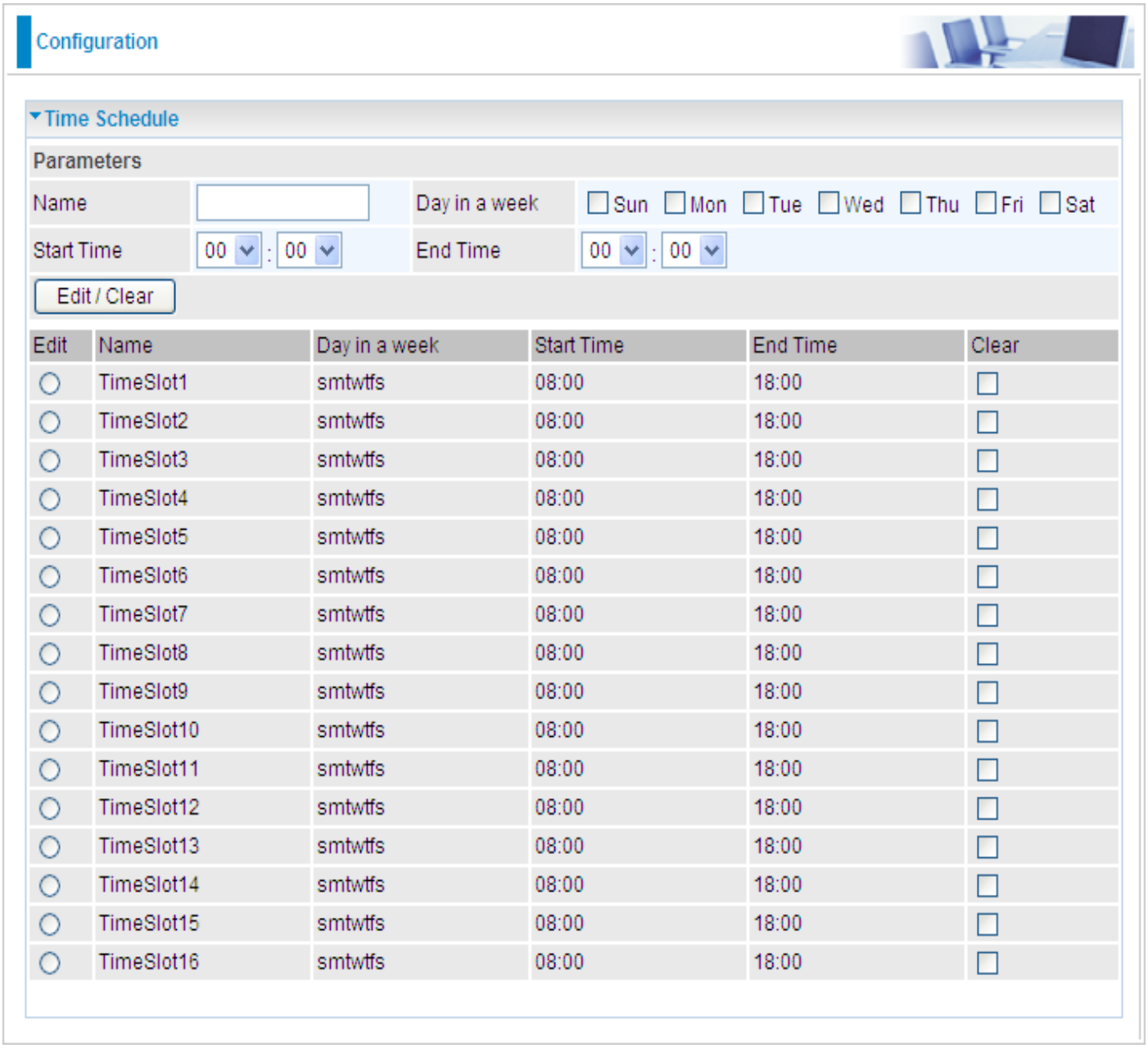
MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the Select drop down menu on the right.

: You can select the MAC from this list.

Time Schedule

The Time Schedule supports up to 16 time slots 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 allow the use of the Internet by users or applications.

Time Schedule correlates closely with router 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. Refer to Time Zone for details. Your router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.



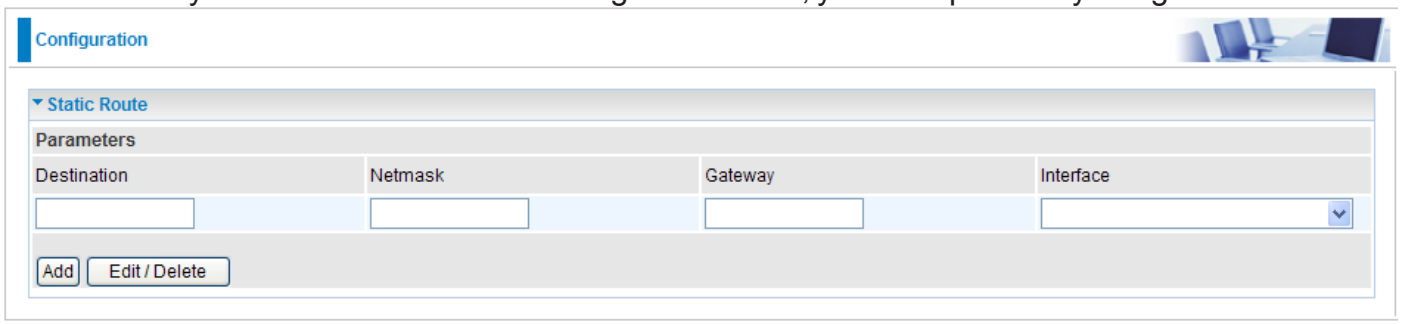
Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the Advanced section: **Static Route**, **Static ARP**, **Static DNS**, **Dynamic DNS**, **VLAN**, **Device Management**, **IGMP**, **MLD**, **SNMP Access Control**, **Remote Access** and **Web Access Control**.

Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination



where the traffic will be routed to.

Destination: Enter the destination IP where the traffic is to be forwarded.

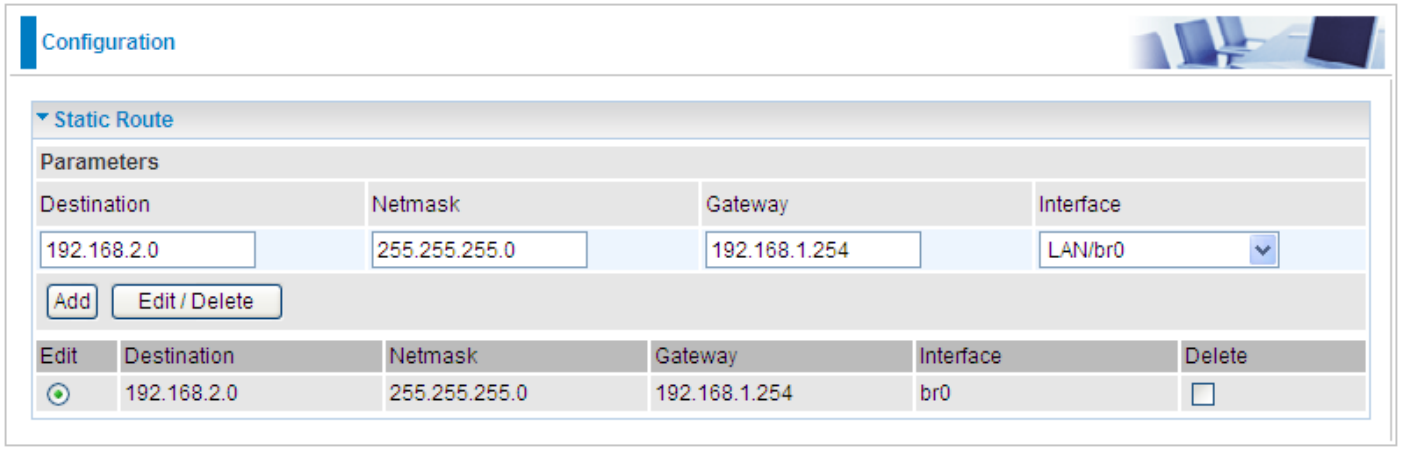
Netmask: Enter the netmask of the destination.

Gateway: Enter the gateway address for the traffic.

Interface: Select an appropriate interface for the new routing rule from the drop down menu.

Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected application, then after

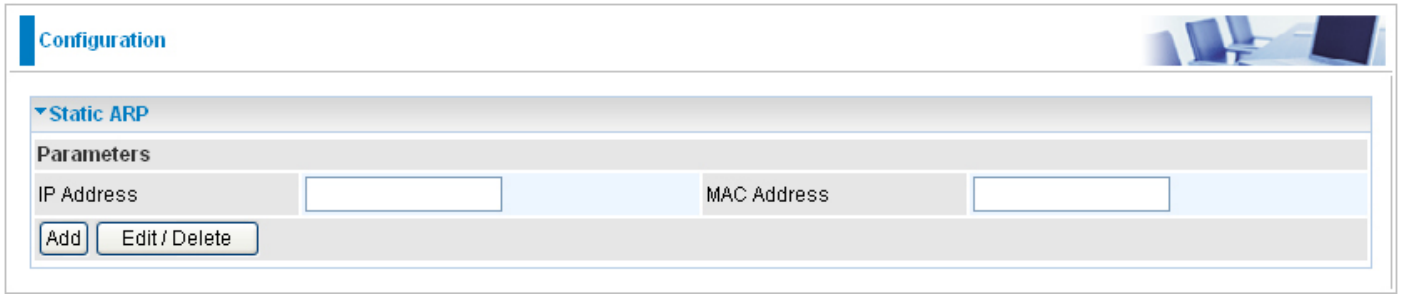


changing the parameters click the "Edit/Delete" button to apply the changes.

Delete: To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

Static ARP

This feature allows you to map the layer-2 MAC (Media Access Control) address that corresponds to the layer-3 IP address of the device.

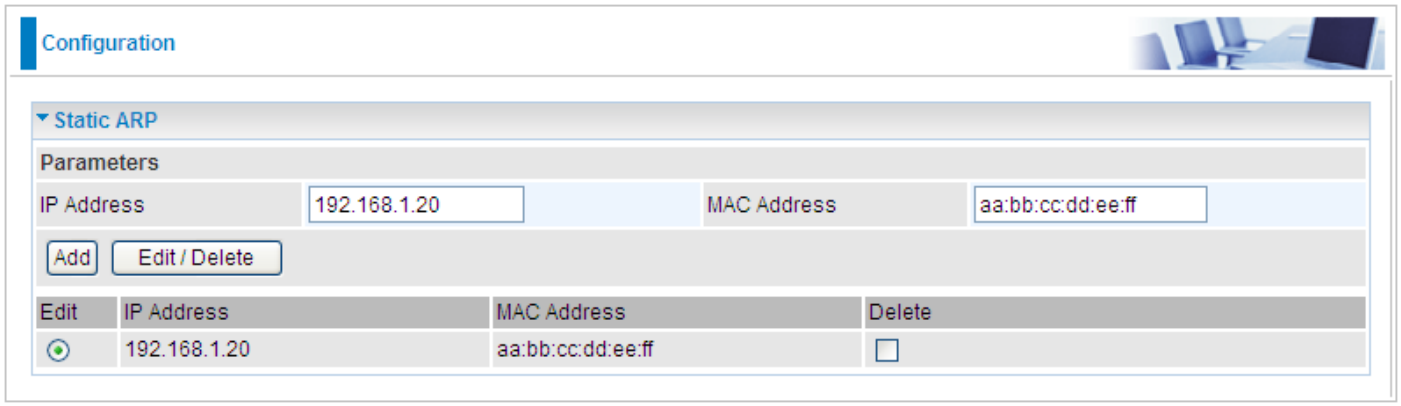


IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.



Delete: To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com translates to the addresses 192.0.32.10 (IPv4).

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 for the ISP's DNS server.

Host Name: type the domain name for the specific IP.

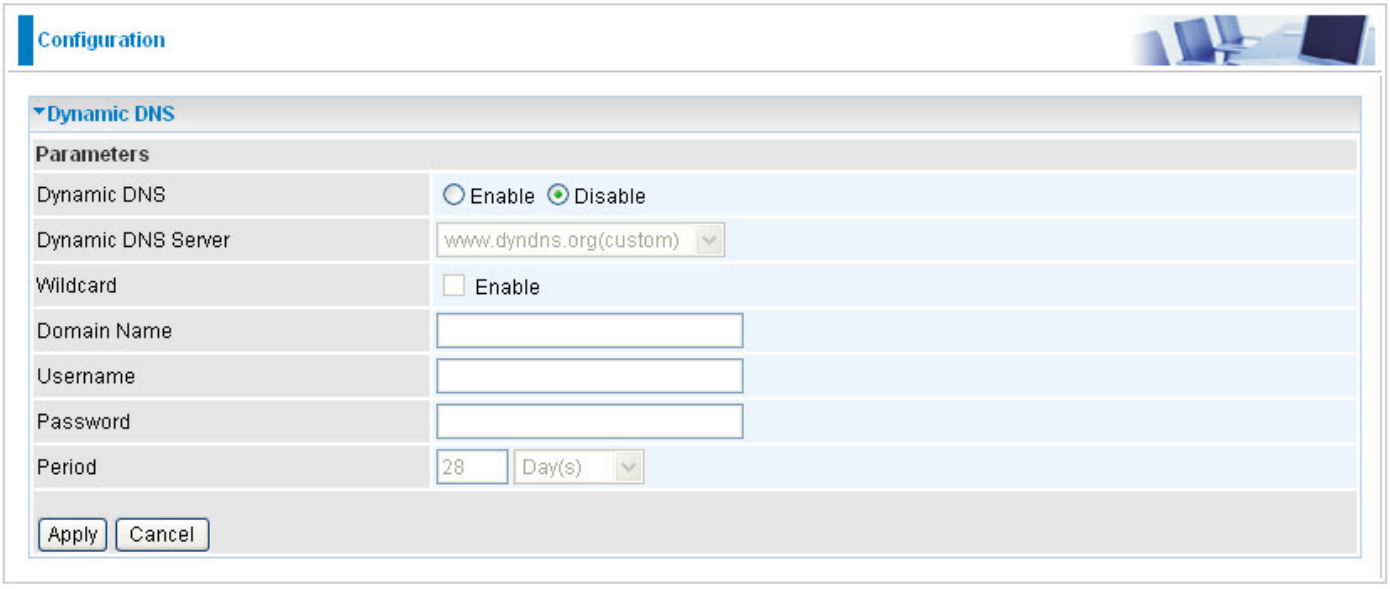
IP Address: type the IP address.

Click Add to add the static DNS item.

Dynamic DNS

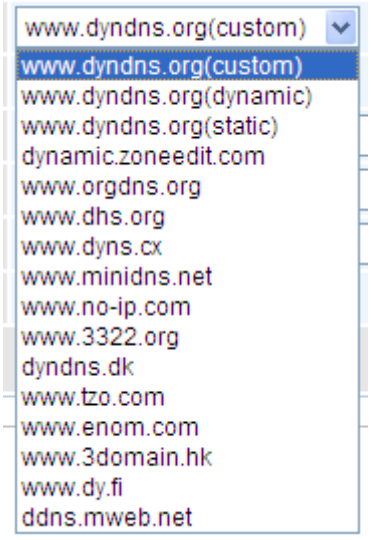
The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful when hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

You need to first register and establish an account with the Dynamic DNS provider using their website, for example **http://www.dyndns.org/**.



Dynamic DNS: Default is disabled. Check Enable to enable the Dynamic DNS function and the following fields will be activated and required.

Dynamic DNS Server: Select the DDNS service you have registered an account with.



Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

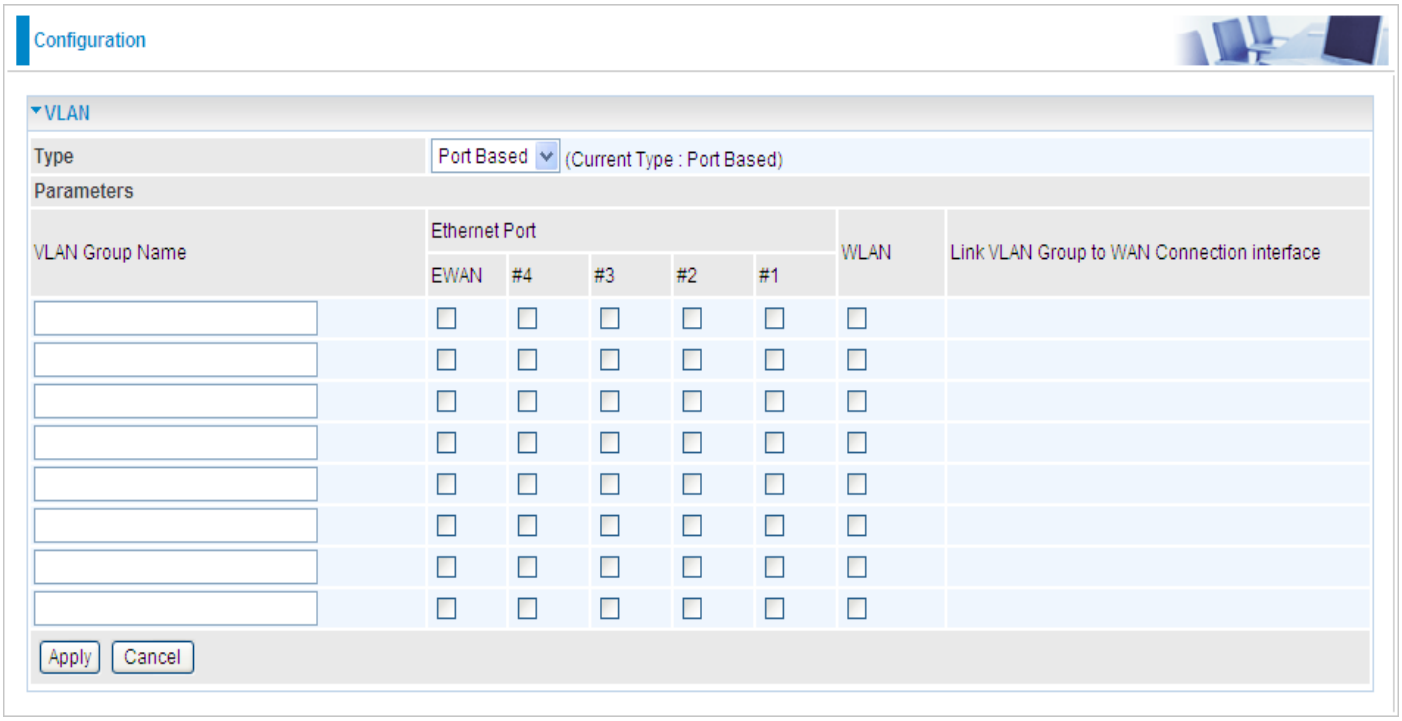
Domain Name, **Username** and **Password:** Enter your registered domain name and your username and password for this service.

Period: Enter the length of the period in the blank, you can set the period unit in day, hour or minute.

Click Apply to confirm the settings.

VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.

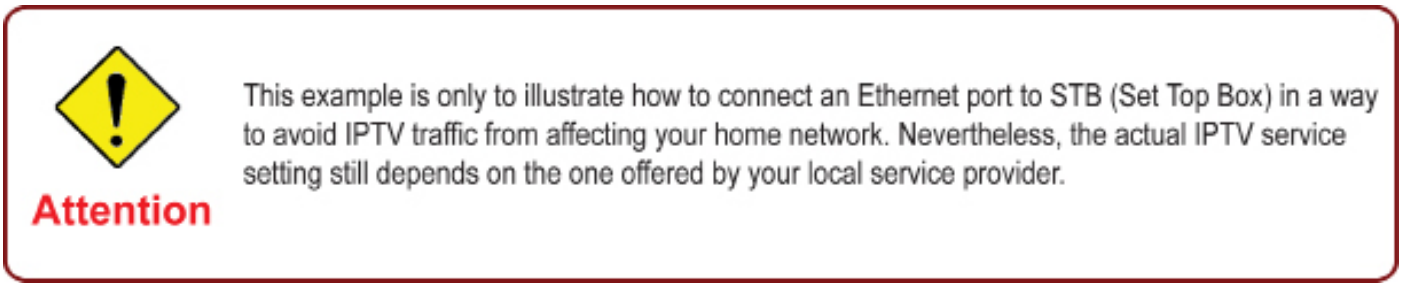


Type: Select the VLAN type from the drop-down menu. There are three options: Port Based, Tag Based and Disable.

Then enter the parameters in the fields of the table.

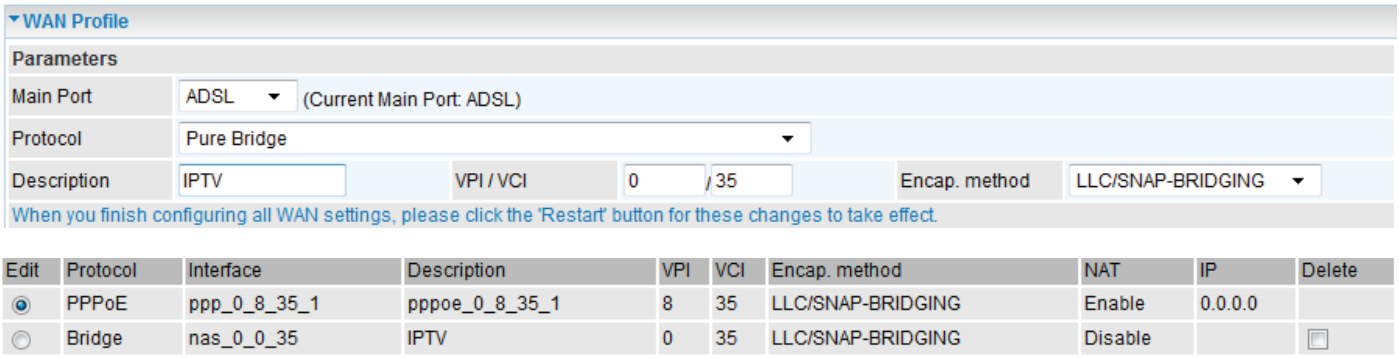
Click Apply to confirm the settings.

Example: IPTV Service Setting



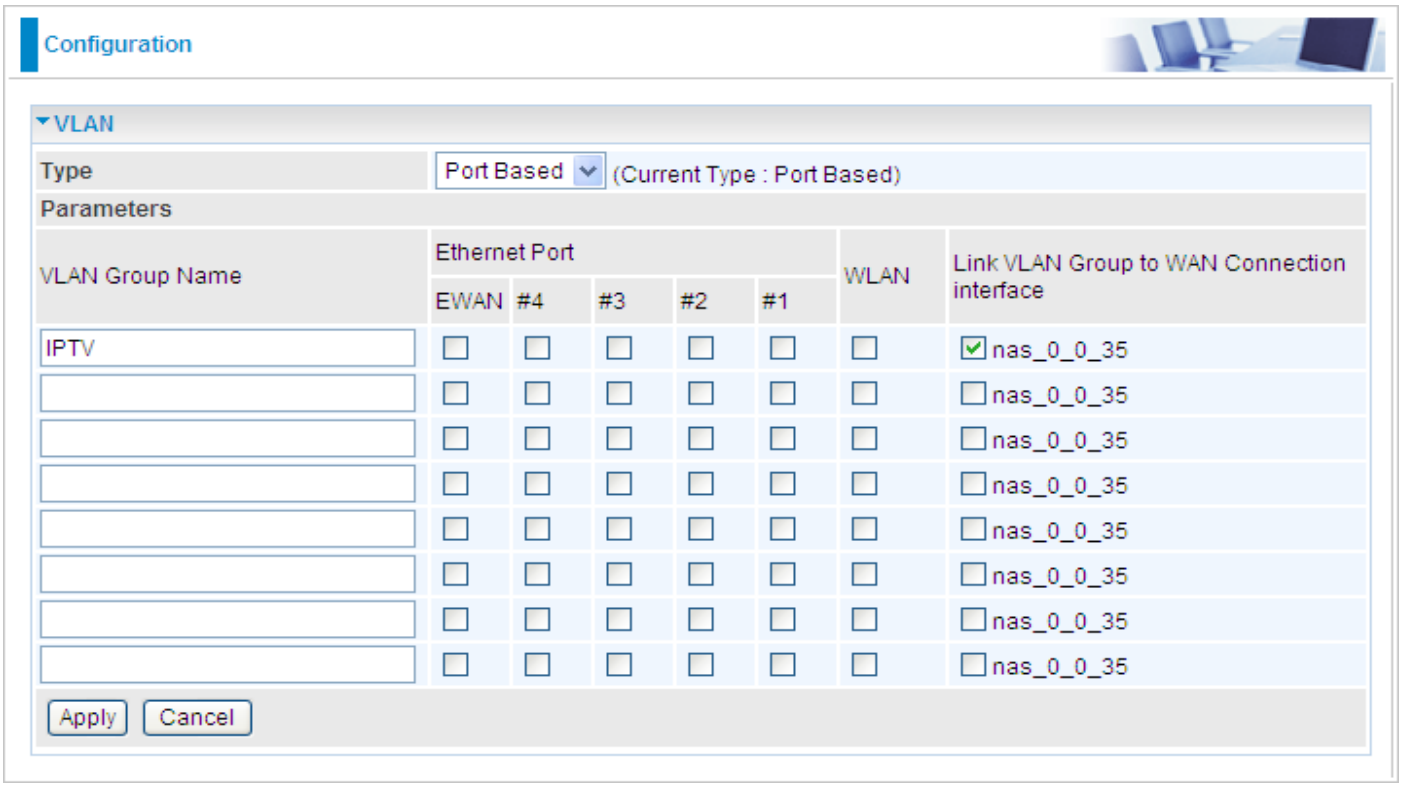
Go to Advanced mode > Configuration > WAN > WAN Profile. Add a new WAN profile using the Pure Bridge protocol. Information should be provided by your local service provider.

Note: Description name should not contain any space.



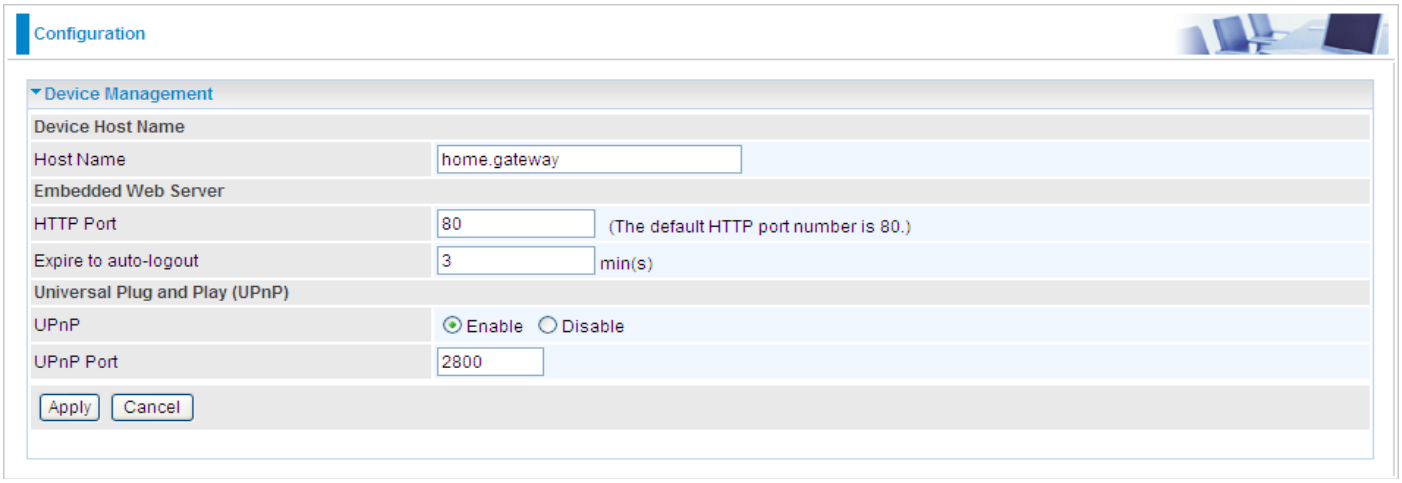
Then go to Advanced mode > Configuration > Advanced > VLAN. Then configure a port that will use the IPTV application. The example below is a setting that illustrates that only Ethernet port #4 can connect to STB and use IPTV.

Note: The VLAN setting illustrated bridges both WAN Profile and the Ethernet Port 4 so that the Ethernet port can connect to STB and get the IP directly from the IPTV Service Network. Thus, Ethernet port 4 can no longer be used for internet access and WEB management.



Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Device Host Name

Host Name: Assign it a name.

Note: The Host Name must have more than a word. These two words should be connected

with a '.' period inbetween.

Example:

Host Name: homegateway ==> Incorrect

Host Name: home.gateway or my.home.gateway ==> Correct)

Embedded Web Server

HTTP Port: This is the port number that the router embedded web server (for web-based configuration) will use. The default value is the standard HTTP port 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address for logon and access the router web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a duration for the system to log the user out of the configuration session automatically.

For Example:

User A changes the HTTP port number to 100, specifies their own IP address as 192.168.1.55 and sets the logout time as 100 seconds. The router will only allow User A to access the Web GUI from the IP address 192.168.1.55 by typing http://192.168.1.254:100 in their web browser. Nevertheless, after 100 seconds the device will automatically log User A out of the system.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with the feature to control data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems. By letting the application

control the required settings and removing the need for the user to control the advanced configuration of their device will make tasks such as port forwarding become easier.

Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UpnP feature. Windows 2000 does not support UPnP.

Disable: Check to inactivate the router's UPnP functionality.

Enable: Check to activate the router's UPnP functionality.

UPnP Port: Default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports that have been used, you are allowed to change the port number.

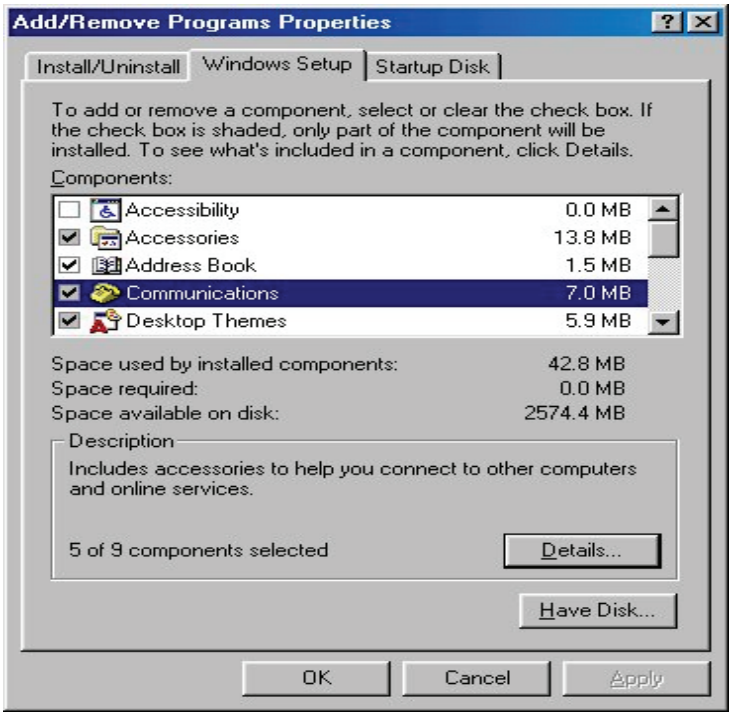
Click Apply to confirm the settings.

Installing UPnP in Windows Example

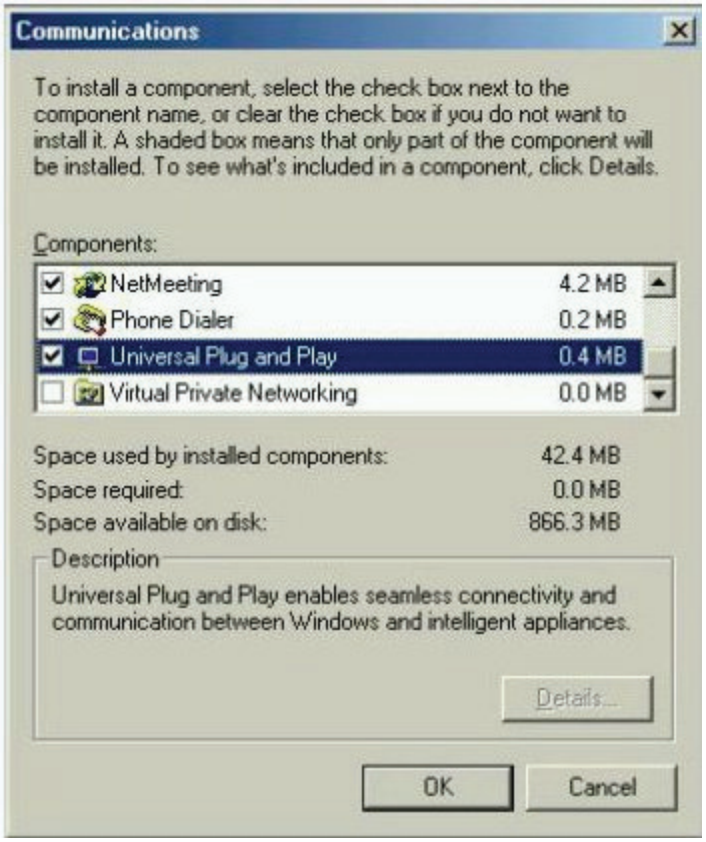
Follow the steps below to install the UPnP in Windows Me.

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.

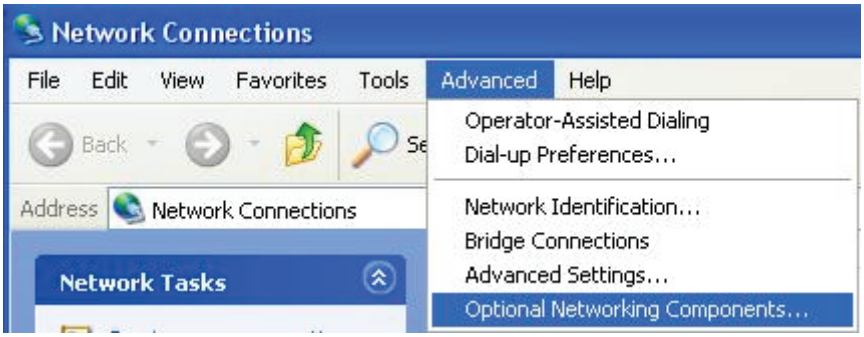
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

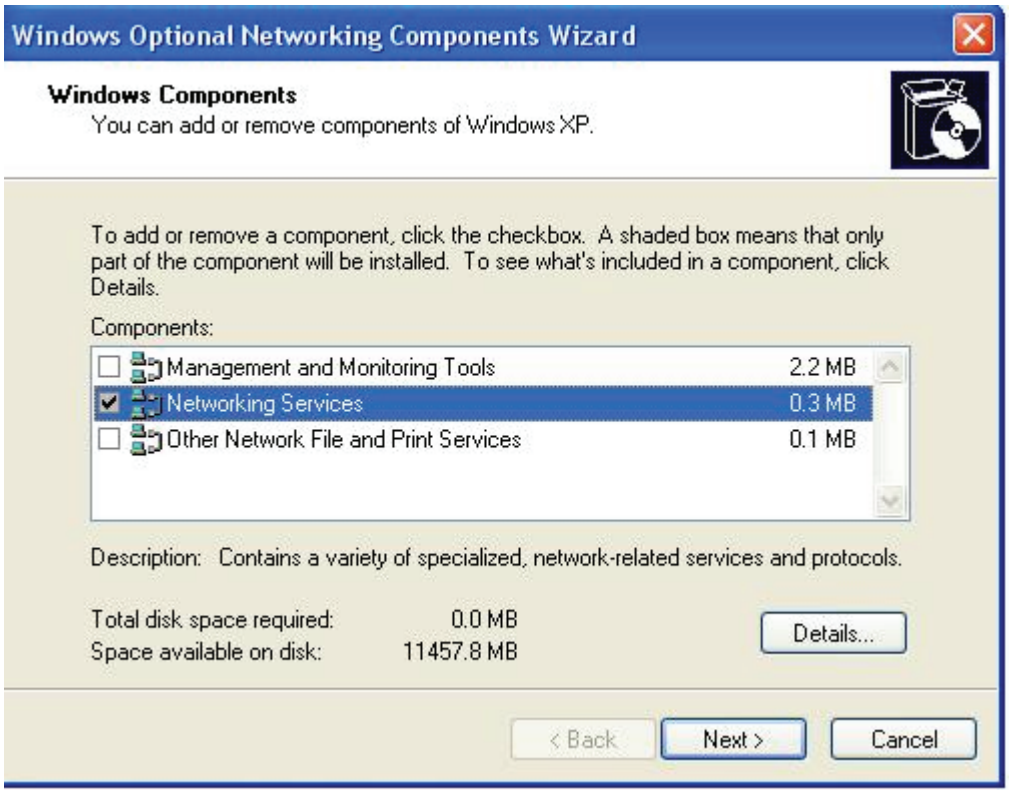
Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….

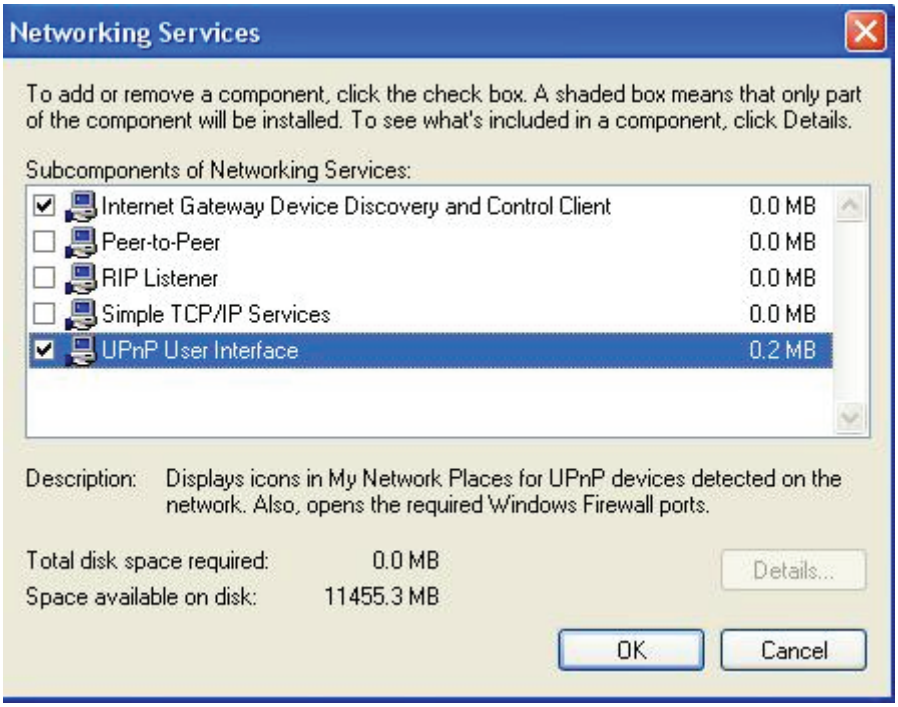


Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



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.



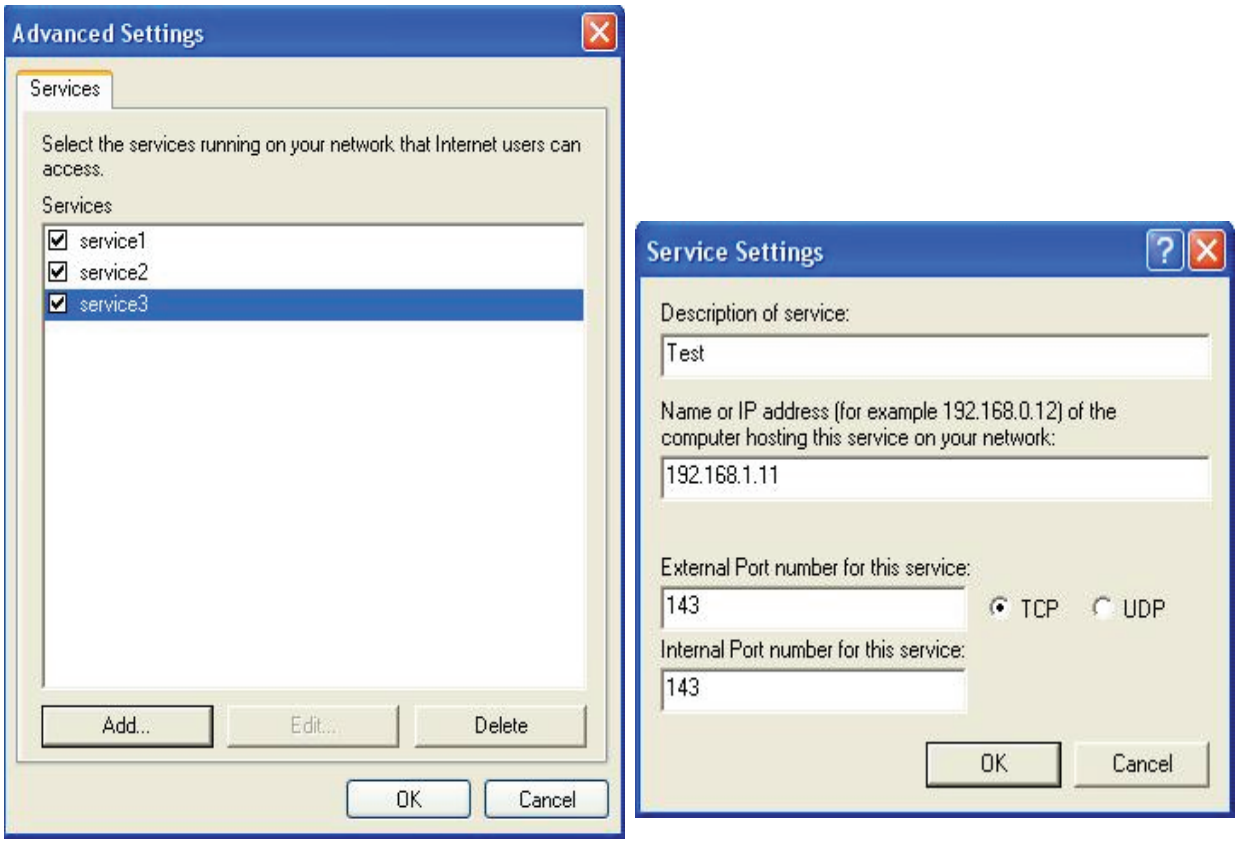
Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

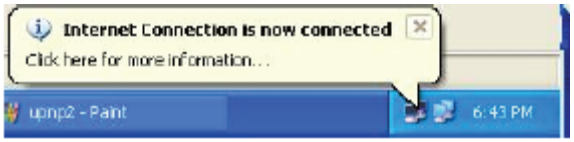
Step 2: Right-click the icon and select Properties.

Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

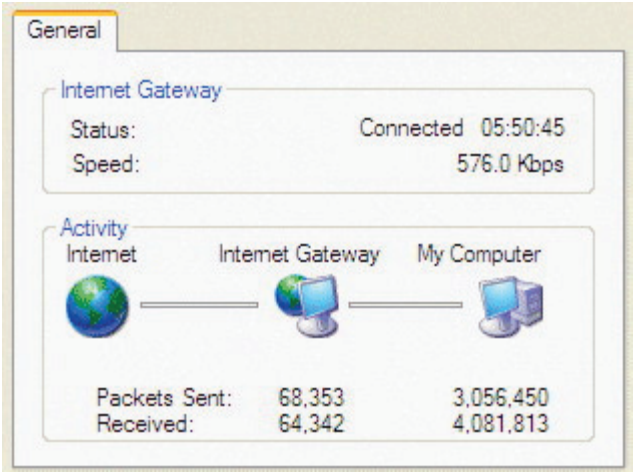
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



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

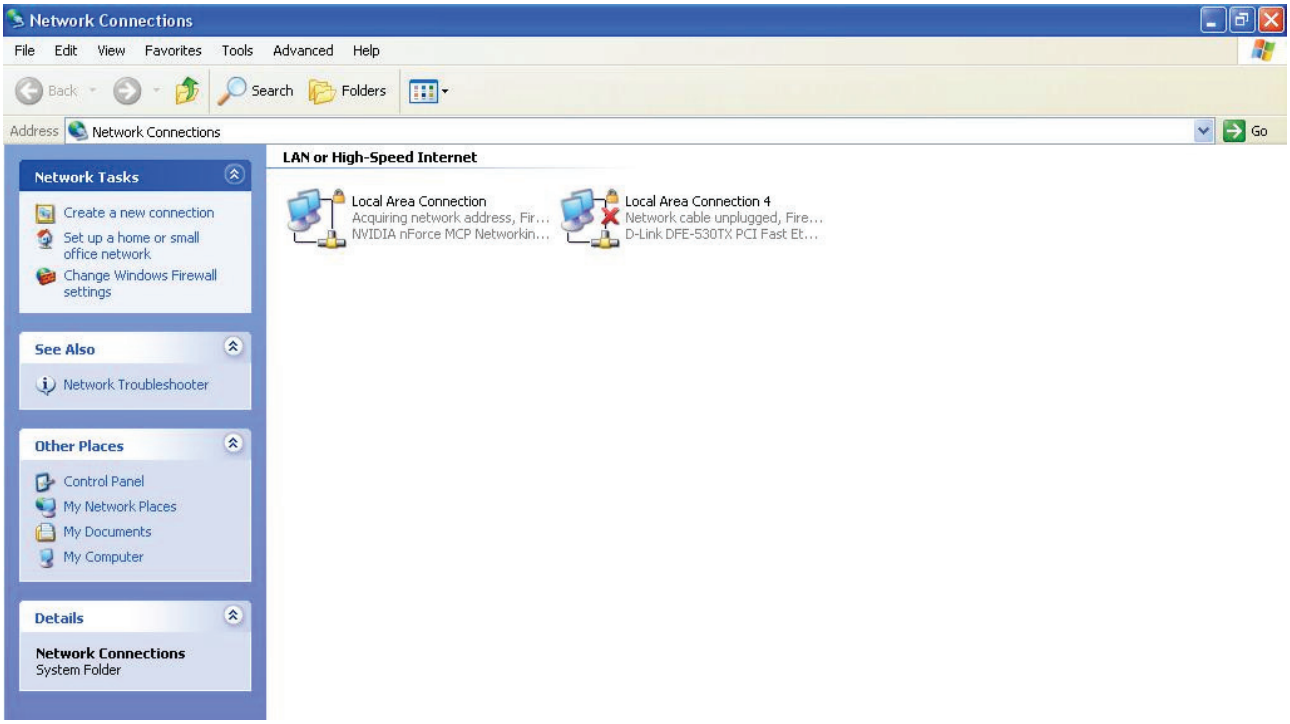
With UPnP, you can access web-based configuration for the BiPAC 7800(N) without first finding out the IP address of the router. This helps if you do not know the router's IP address.

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.



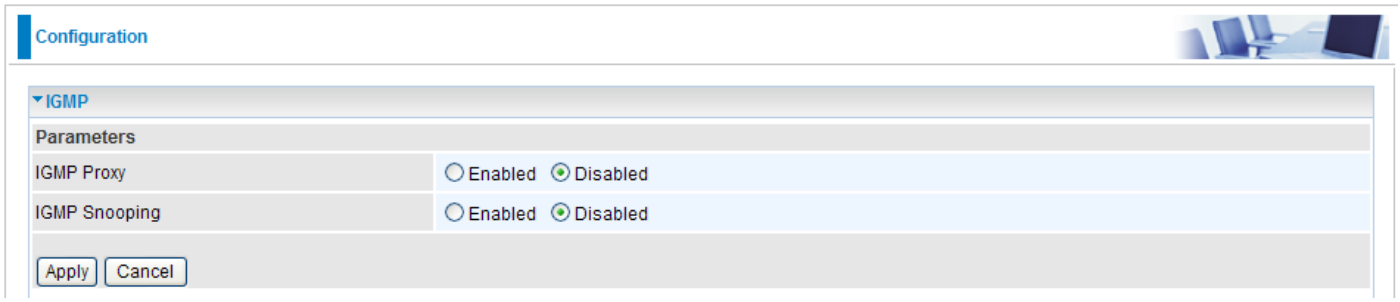
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 7800(N) and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7800(N) and select Properties. A properties window displays basic information about the BiPAC 7800(N).

IGMP

IGMP, known as Internet Group Management Protocol, is used to manage hosts from multicast group.



IGMP Proxy: IGMP proxy enables the system to issue IGMP host messages on behalf of the hosts that the system has discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.

IGMP Snooping: Allows a layer 2 switch to manage the transmission of any incoming IGMP multicast packet groups between the host and the router. Default is set to Disable.

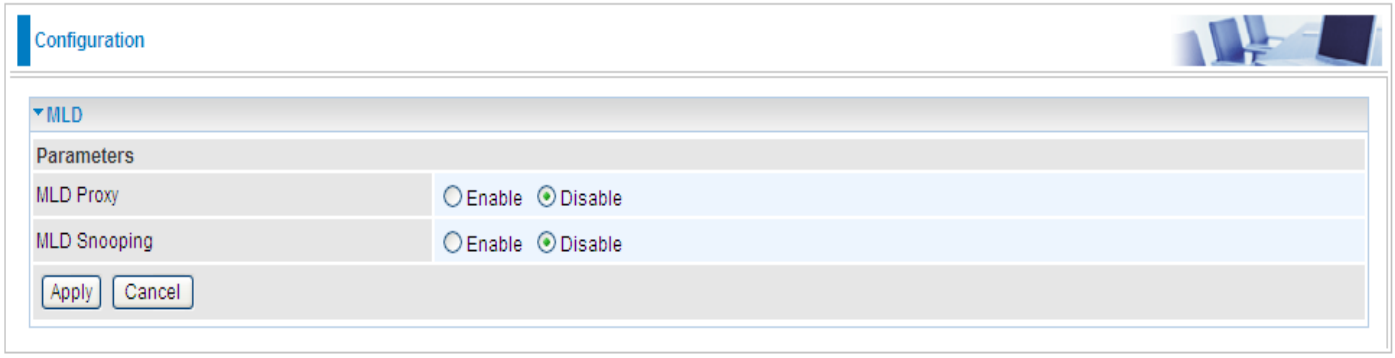
Click Apply to confirm the settings.

Example:

When IGMP snooping is enabled, the feature will analyze all incoming IGMP packets between the hosts that are connected to the switch and the multicast routers in the network. When the layer 2 switch receives an IGMP report from a host requesting for a given multicast group, the switch will add the host's port number to the multicast list for that multicast group to be forwarded to. And, when the layer 2 switch has detected that an IGMP has left, it will remove the host's port from the table entry.

MLD

Multicast Listener Discovery (MLD) enables you to manage subnet multicast membership for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. Multicast traffic is sent to a single address but is processed by multiple hosts. Hosts listening on a specific multicast address make up a multicast group, and they receive and process traffic sent to the group address.



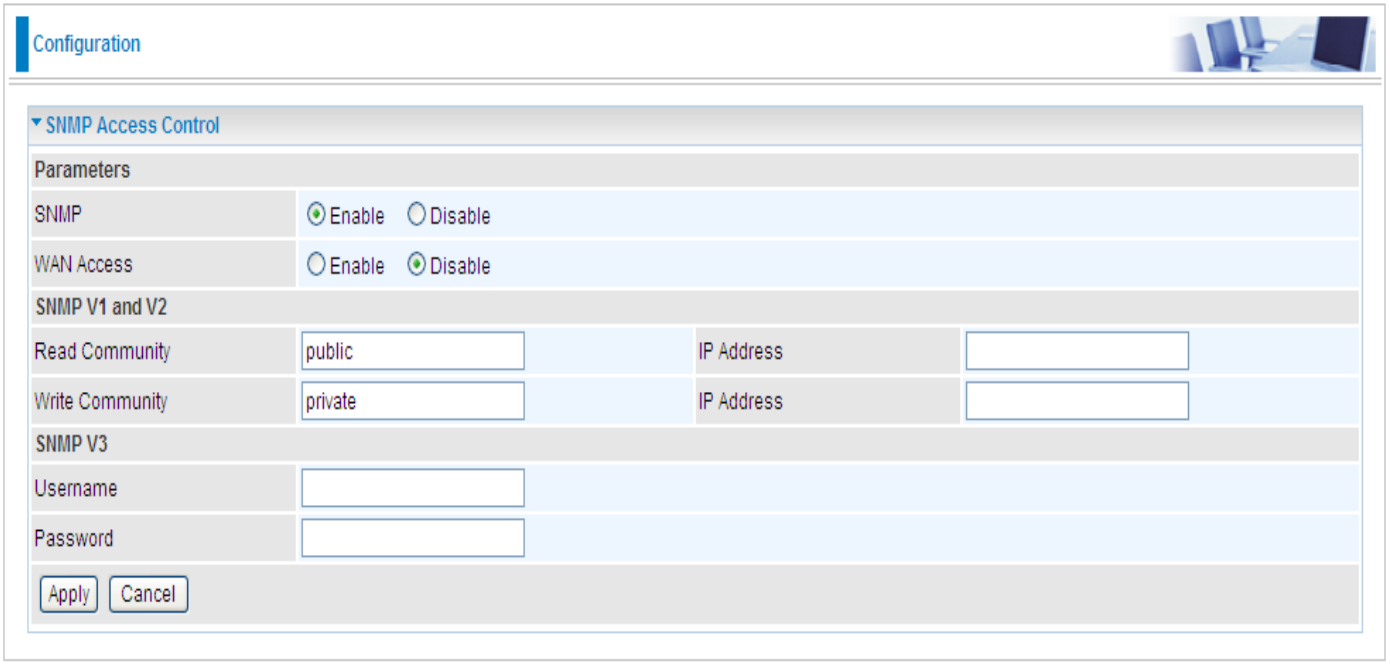
SNMP Access Control

SNMP, short for Simple Network Management Protocol, is an "Internet-standard protocol " for managing devices on Ip networks. It is mostly used in network management system to monito network-attached devices for conditions that warrant administrative atention.

SNMP exposes management data in the form of variables on the management system, which describes the system configuration. These variables can then be queried (and sometimes set) by managing appications.

There are three versions: version 1, 2, 3.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.



SNMP: Click "Enable" to activate the SNMP function.

WAN Access: Check "Enable" if you want users in WAN side have right to access this SNMP feature.

SNMP V1 and V2:

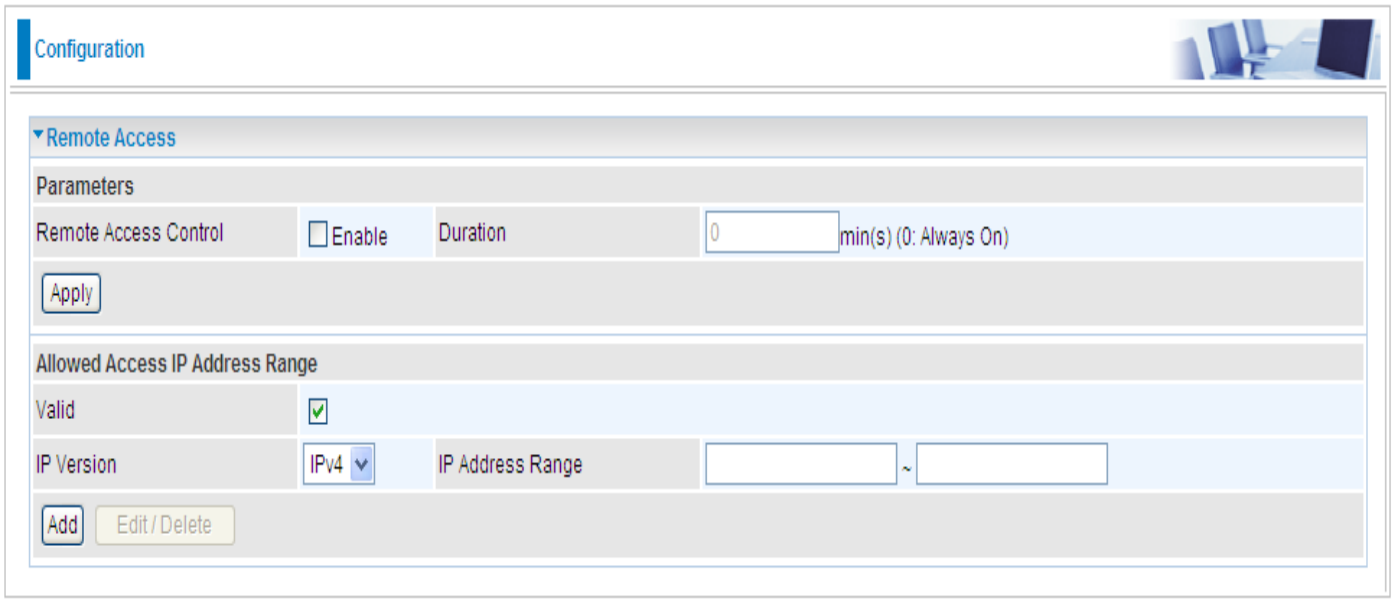
Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

SNMP V3:

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

Remote Access



Remote Access Control: Select Enable to allow management access from remote side (mostly from internet).

"Allowed Access IP Address Range" was used to restrict which IP address has the ritght to remotely access the device using either Telnet , SSH, web GUI or other terminal management system.

Valid: means to enable the IP address Range limitation.

IP Version: select either IPv4 or IPv6, this is used to indendify the allowed IP.

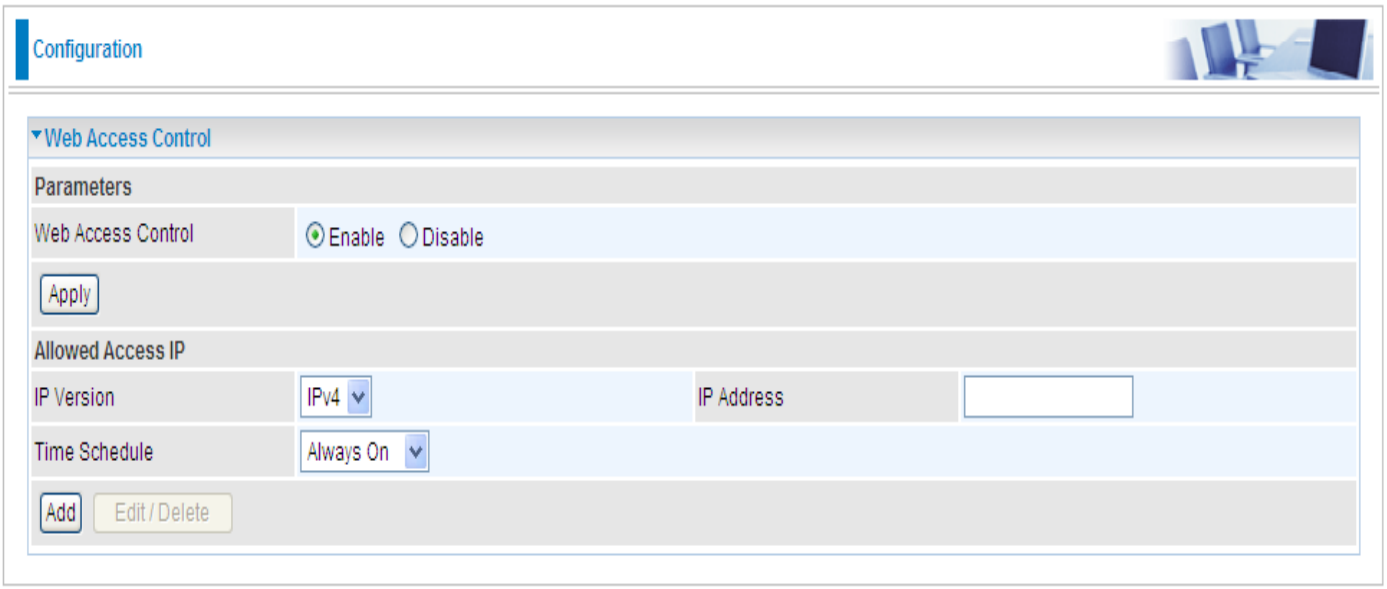
IP Address Range: specifys the IP address Range.

Click **Apply** to confirm Remote Access Control setting.

Click **Add** to add a IP Range to allow remote access.

Web Access Control

Web access control is to only entitle authorized IPs to access the router's configuration webpage.



Web Access Control: Select "Enable" to allow the management of Web control.

Allowed Access IP: Enter the IP Address allowed.

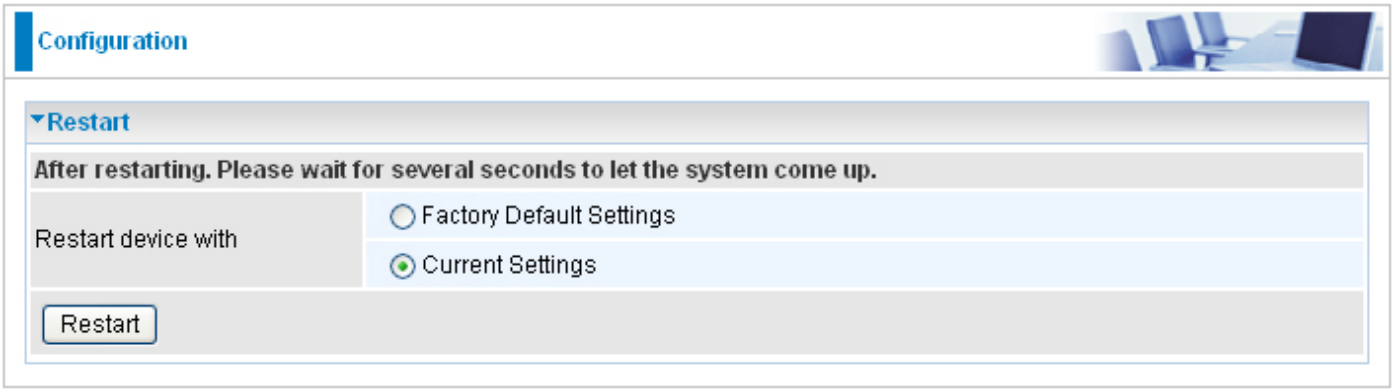
Time Schedule: Choose the time scheduled for this fuction to take effect.

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "Save Config" and click "Apply" to write your new configuration to FLASH.

Restart

Click “Restart” with option Current Settings to reboot your router (and restore your last saved configuration).



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.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on	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 Billion for technical support.
You have forgotten your login username or password	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the reset button for more than 5 seconds.

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your prouct.

Contact Billion

Worldwide:

http://www.billion.com